Experiences of Online Threats Among Younger Adults in the Kingdom of Saudi Arabia and the United Kingdom

Najla Ghanim Aldaraani

PhD

University of York
Computer Science

June 2025

Abstract

This programme of research explored how younger adults (aged 40 or younger) in the Kingdom of Saudi Arabia (KSA) and the United Kingdom (UK) experience, detect and respond to online security threats. Through online studies, two using an innovative diary method, the research investigated the online threats younger people in the two countries encounter, their concerns about these threats, the cues they use to identify threats and how they respond to them.

The first study involved a scenario-based online survey designed using the MITRE ATT&CK framework and the Cyber Kill Chain model to present 12 realistic online threat scenarios to participants. Participants were asked whether they had encountered threats like these scenarios and to report their concerns, detection strategies, and responses to them. The results highlighted attacks from seemingly trusted sources as a top threat in both countries. However, malware and data theft were more frequently reported among KSA participants compared to those in the UK.

To explore these experiences in greater depth, a 30-day online diary study was conducted with 16 participants from KSA. Participants recorded their encounters with online threats through a short questionnaire sent to them daily. Phishing was the most common threat encountered. A substantial proportion of threats could not be fully classified due to the limited information provided. Detection cues reported by participants were systematically coded using a modified version of the NIST Phish Scale, expanded to include cues applicable to a wider range of threat sources beyond email (e.g. voice calls and social media). Language and content cues were the most frequently reported cues of threats, followed by technical indicators and prior knowledge of encountered threats.

A second diary study was conducted in the UK with 45 participants over 7- and 14-day periods. Insights from the KSA study, particularly regarding the ambiguity of open-ended responses and decreased participant engagement over the long study duration, informed the design of this study. Consequently, the UK study was shorter, had more participants and used a more structured approach, incorporating mainly closed-ended questions. The modified Phish Scale cues were used as a set of options to select from. Phishing and spear phishing were the most frequently reported threats. Technical indicators such as suspicious links and email addresses were the most frequent cues used by British participants.

The studies also investigated the influence of individual differences among participants, such as levels of security knowledge, security behaviour intentions (measured by the SeBIS scale), unrealistic optimism, risk-taking, and thinking orientation.

This thesis contributes new empirical evidence on how younger adults experience, detect, and respond to online threats across two distinct cultural contexts (UK and KSA). Its principal contribution lies in methodological innovation: combining surveys with the novel application of diary methods to capture real-world encounters. This approach generated rich insights into behaviours that are often overlooked in lab-based studies.

Table of Contents

List of Tables

List of Figures

Glossary of Key Terms

- Online security: Online security is the practice of protecting individuals, devices, networks, and data from online threats. This is achieved by implementing technological solutions, policies, and user behaviours that prevent unauthorised access, damage, or cyberattacks. This study considers both technical measures (e.g. antivirus software, two-factor authentication) and human actions (e.g. threat recognition, password management).
- Online threat: situations or incidents, such as phishing, malware, and identity theft, aimed at compromising the confidentiality, integrity, or availability of individuals' digital assets or personal data through online channels. In this thesis, "online threats" specifically refers to those encountered by younger adults during their everyday online activities
- Individual user: An individual user refers to a single person using digital devices or services, such as the younger adults in this study.
- Younger adults: often referred to as "digital natives", individuals aged 18 to 40 who have grown up immersed in digital technologies such as the internet, smartphones, and social media.

Acknowledgments

In the name of Allah, all praise and thanks be to Him, at the beginning and the end.

This journey has involved growth, challenges, and special moments, all thanks to the amazing support and encouragement I have received.

My deepest gratitude goes to my supervisor, Prof. Helen Petrie. Your clear and continuous guidance, from the beginning of my PhD to the final moment, along with your encouragement, helped me reach this important milestone.

I also thank my co-supervisor, Dr. Siamak Shahandashti, whose knowledge of cybersecurity greatly improved my research. Thank you for being available, sharing your expertise, and guiding me when I needed help.

To my beloved mother, your belief in me and your strength have inspired me deeply. You have always been my guiding light, and I dedicate this achievement to your memory.

To my father, thank you for motivating me and for believing in my potential. Your support gave me the strength to keep going.

To my loving husband, Dr. Amer Alshahrani, your presence, patience, and constant encouragement have been my anchor. I could not have completed this journey without you.

To my wonderful children, Ruba, Abdulaziz, and Abdulrahman, thank you for your patience and understanding. Your support made each challenge easier and every success even more special.

Thank you to my brothers and sisters for being a source of encouragement and support. Your presence in my life has made a great difference.

Author Declaration

I declare that this thesis is a presentation of original work and I am the sole author. This work has not previously been presented for a degree or other qualification at this University or elsewhere. All sources are acknowledged as references.

List of Publications:

1. Aldaraani, N., Petrie, H., & Shahandashti, S. F. (2022, July). Online security attack experience and worries of young adults in the United Kingdom. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 300-309). Cham: Springer International Publishing.
2. Aldaraani, N., Petrie, H., & Shahandashti, S. F. (2023, July). Online security attack experience and worries of young adults in the Kingdom of Saudi Arabia. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 364-376). Cham: Springer Nature Switzerland.
3. Aldaraani, N., Petrie, H., & Shahandashti, S. F. (2024, July). A Diary Study to Understand Young Saudi Adult Users' Experiences of Online Security Threats. In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 47-60). Cham: Springer Nature Switzerland.

Chapter 1 Introduction

Online security threats have become a pervasive and constant concern for individuals, businesses, and organisations. Rapidly advancing technology and the increasing use of internet-enabled devices have led to a constantly evolving cybersecurity landscape, characterised by new threats and vulnerabilities.

Cybercriminals are constantly advancing their methods, refining their tactics, techniques, and procedures, and now operate as structured, well-resourced entities. Many are motivated primarily by financial gain, and their attacks have become more targeted, persistent, and difficult to detect (Santos et al., 2025). Consequently, businesses, governments, institutions and individuals have experienced a consistent rise in the damage caused by cyberattacks. According to recent estimates, the global economic cost of cybercrime, mainly affecting organisations and industries such as manufacturing, finance, and insurance, was projected to reach USD 9.22 trillion by 2024 and escalate to USD 13.82 trillion by 2028 (Petrosyan, 2025). While such figures illustrate the overall magnitude of the global cyber threat, the present thesis focuses on its consequences for individuals. In the UK alone, recent research by the Office of Communications (OfCom, 2023) found that 87% of adult internet users reported encountering content they believed to be a scam or fraud, and around 21% of individual victims of cyberattacks lost £1,000 or more. While global economic estimates of cybercrime often focus on organisational impacts, these findings highlight that individuals also face significant risk and harm.

High-profile incidents have often brought these challenges to public attention. To illustrate the scale and persistence of cybersecurity threats over the past decade, Table 1.1 summarises a range of high-profile incidents between 2016 and 2025 that have affected governments, businesses, and individuals worldwide.

In October 2016 (Example 1), the Dyn DNS service was hit by a large-scale distributed denial-of-service (DDoS) attack that disrupted access to major global platforms, including Twitter, Netflix, and PayPal. The attack used the Mirai malware, which hijacked thousands of internet-connected home devices such as cameras and routers to flood Dyn's servers with traffic (BBC News, 2016). In the same year, Ukraine experienced a cyberattack (Example 2) on its power grid that cut one-fifth of Kyiv's electricity consumption. Investigations revealed that malware was used to target protective relays, disrupting the physical infrastructure of the grid. Analysts noted that the attack was designed not only to cause short-term disruption but also to inflict potentially long-term damage to the electricity system (BBC News, 2017).

One of the most high-profile examples in the Middle East was the Shamoon malware attack on Saudi Aramco. The first occurrence of the incident was in 2012, which erased data from tens of thousands of computers (Alelyani & GR, 2018). The re-emergence of the malware followed this in 2017 (Shamoon 2, Example 3), which again targeted energy companies and government agencies in the Gulf region through destructive malware and spear-phishing campaigns (Malware News, 2017; The New York Times, 2018).

Table 1.1: Examples of high profile security threats 2016–2025.

No.	Year	Type of threat	Threat name	Main target	Reference(s)
1	2016	DDoS via IoT Botnet	Dyn Cyberattack	Access to Twitter, Netflix, PayPal, PlayStation, and other platforms	BBC News (2016)
2	2016	Malware	Kyiv Power Grid Attack (Industroyer malware)	Ukraine electricity grid	BBC News (2017)
3	2017	Malware/Spear Phishing	Shamoon 2	Saudi Aramco and Government agencies in KSA	Malware News (2017) The New York Times (2018)
4	2017	Ransomware	Uber data breach	Personal data of 57 million customers and drivers in the USA were stolen. Uber paid USD 100,000 for the hackers to delete and destroy the data.	The Guardian (2017) CSIS (2025)
5	2018	Ransomware	Unknown	Leominster Public School District in the USA paid USD 10,000 in Bitcoin to hackers to unlock school's system.	Verdict Encrypt (n.d.)
6	2019	Data breach	Facebook data breach	Personal data of 500+ million users publicly exposed	BBC News (2019) Rabitti et al. (2024)
7	2020	Data leak in dark web	Zoom Credentials Leak	Over 500,000 Zoom users' accounts exposed on the dark web	Rabitti et al. (2024)
8	2020	Phishing	Covid-19 Vaccine Cold Chain Campaign	Organisations linked to Gavi's Cold Chain Equipment Optimisation Platform (CCEOP), including organisation such as WHO, UNICEF, World Bank, across six countries	Corera (2020)
9	2021	Ransomware	Colonial Pipeline Attack (DarkSide)	US fuel pipeline (45% of East Coast fuel supply)	Russon (2021)
10	2022	Phishing and Data Theft	Lapsus$ Group Campaigns	Microsoft, Nvidia, and Samsung	O'Connor (2022)
11	2023	Ransomware	British Library Cyberattack	British Library	ICO (2025)
12	2024	Service Disruption and Data Breach	Transport for London (TfL) Cyberattack	Transport for London customers and services	Edwards (2024)
13	2025	Ransomware	Marks & Spencer (M&S) Cyberattack	UK retailer M&S	Butler (2025)
14	2025	Ransomware	Collins Aerospace Cyberattack	Major European airports (Brussels, Dublin, Berlin, Heathrow), flight cancellations and delays	Rahman-Jones (2025)

In November 2017, Uber disclosed that it had paid hackers $100,000 to delete the stolen data of 57 million customers and drivers, which included names, phone numbers, email addresses, and vehicle license plate numbers (Example 4). Investigations later revealed that the breach occurred when attackers gained access to Uber's Amazon Web Services account using stolen login credentials (The Guardian, 2017).

In 2018, the Leominster Public School District in the United States became the victim of a ransomware attack that encrypted access to its computer systems (Example 5). The attackers demanded payment in Bitcoin, and the district ultimately paid USD 10,000 to regain access to its files (Verdict Encrypt, n.d.).

In 2019, the breach of Facebook exposed personal data from more than 500 million users (Example 6), leaving them vulnerable to identity theft, phishing, and financial fraud (BBC News, 2019). The following year, over half a million Zoom users' credentials were discovered on the dark web (Example 7) after a security breach (Rabitti et al., 2024).

In 2020, a phishing campaign known as the Covid-19 Vaccine Cold Chain Campaign targeted organisations involved in vaccine distribution across six countries (Example 8). The attacks focused on partners linked to Gavi's Cold Chain Equipment Optimisation Platform (CCEOP), including the WHO, UNICEF, and the World Bank, aiming to collect information about systems used for vaccine storage and delivery during the pandemic (Corera, 2020).

In 2021, the Colonial Pipeline in the USA was forced offline following a ransomware attack attributed to the DarkSide criminal group (Example 9). The pipeline supplied nearly half of the East Coast's fuel, and the disruption led to fuel shortages, rising prices, and an emergency declaration (Russon, 2021).

In 2022, the Lapsus$ group carried out a series of high-profile cyber-attacks on organisations including Nvidia, Samsung, Ubisoft, and Microsoft (Example 10). Their approach relied on phishing to gain access and extortion through leaking stolen data, rather than encryption (O'Connor, 2022).

In October 2023, the British Library suffered a ransomware attack (Example 11) due to the lack of multi-factor authentication on an administrator account (ICO, 2025).

In 2024, Transport for London (TfL) confirmed that a sophisticated cyberattack had exposed customer data, including bank details, and forced parts of its digital infrastructure offline (Example 12). While transport services continued, contactless systems, refund processing, and journey history were disrupted, and the organisation estimated the cost at several million pounds (Edwards, 2024).

In 2025, Marks & Spencer (M&S) was hit by a ransomware attack (Example 13), with speculation that the breach originated through a service supplier. Hackers reportedly stole data and encrypted key systems, disrupting operations and causing over £500m to be wiped from the company's stock market value (Butler, 2025). Also in 2025, a cyberattack against Collins Aerospace caused widespread disruption across European airports, including Brussels, Dublin, Berlin, and Heathrow (Example 14). The incident led to flight delays, cancellations, and manual check-in procedures (Rahman-Jones, 2025)

Online security is now recognised not just as a technical challenge but as a socio-technical issue that involves both systems and people. Traditionally, cybersecurity focused primarily on technological

defences such as firewalls, encryption, and intrusion detection systems. However, the growing complexity of attacks, particularly those that exploit human behaviour, such as social engineering, has revealed the limitations of relying solely on technical solutions. As digital interactions become a part of our daily lives, users are no longer just passive recipients of technology; they are active participants whose decisions and behaviours directly influence security outcomes. This socio-technical perspective emphasises that effective security relies not only on robust technical measures but also on understanding how people perceive, detect, and respond to threats in real-world situations.

1.1 Prevalence of Online Threats and Attacks

The European Union Agency for Network and Information Security (ENISA) produces annual threat reports that provide an overview of the current cybersecurity threat landscape in the European Union, highlighting emerging trends, vulnerabilities, and threats affecting Europe. Kettani and Wainwright (2019) used the ENISA 2018 Threat Landscape report to investigate the top cyber threats across Europe and how they have evolved over time. The study identified malware, denial of service (DoS), phishing, spam, data breaches, identity theft, and ransomware as some of the most prevalent threats in 2018. It was observed that phishing and spam increased substantially between 2012 and 2018, with phishing advancing from the seventh rank in 2012 to the fourth rank by 2018. The authors also examined threat sources, reporting that the majority of detected malware was delivered via email compromise (92%), with a smaller proportion attributed to websites and browsers (6%), and that over 90% of malware infections and 72% of data breaches originated from phishing attacks. In addition, the analysis briefly highlights affected sectors and organisations, noting that healthcare, government, financial, and commercial organisations are particularly impacted by threats such as data breaches, ransomware, web application attacks, and cyber-espionage, with high-profile incidents such as the Equifax data breach cited as illustrative examples. However, while the study outlines trends, threat vectors, and organisational-level impacts, it does not examine how these cyber-attacks affect individuals or how users experience, perceive, and respond to such threats. In addition to the previous study, the recent ENISA Threat Landscape 2023 report identified common threats in 2023, which included ransomware, malware, social engineering, and data breach (ENISA, 2024). I could not find any information specifically about the landscape of threats to individual users at a European level.

Moving from the European threat landscape to a UK-specific context where I was able to find information specifically about threats to individuals, and focusing on individual users rather than organisations, in the United Kingdom (UK), Ofcom (2023) found that 87% of adult internet users said they encountered content they believed to be a scam or fraud, and around 25% of those affected lost money as a result, with one in five victims losing more than £1,000. These figures underline the fact that, despite advances in cybersecurity infrastructure and awareness campaigns, individuals continue to face widespread exposure to online threats and fraudulent activity.

In the Kingdom of Saudi Arabia (KSA), publicly available cybersecurity reports primarily focus on detecting attack activity targeting online services and platforms, rather than individual users. In the KSA, Kaspersky (2022) reported that in the first half of 2022, nearly 478,000 financial phishing attacks were detected and blocked. Of these, 74% targeted online shopping platforms, 20% focused on payment systems such as PayPal and Apple Pay, and 6% targeted banks, highlighting that

financial fraud remains a dominant risk in the region. I could not find any data from KSA about the effects and cost of cyberattacks on individuals.

The definitions of threat types mentioned above are in Table 2.1.

1.2 Research Motivation

Coles-Kemp et al. (2020) explored how the widespread integration of digital technology into all aspects of life has completely transformed how we think about security. They emphasised that as digital technology becomes more embedded through services, smart devices, and other technological advancements, constant connectivity has increased the security difficulties and become linked with societal and human elements rather than technological challenges. This transformation reflects Cramer's (2015) concept of "post-digital", which captures the era in which digital technology is so firmly embedded into society that new approaches to security are required. The new security approaches must move beyond technical controls to account for how users interpret, experience, and respond to online threats. Post-digital security therefore requires greater attention to users' concerns, experiences, and contextual decision-making, rather than relying on generic or prescriptive guidance alone.

However, even as cybersecurity has evolved into a socio-technical challenge influenced by human behaviour and societal norms, much of the existing support remains focused on technical infrastructure and organisational support. For example, the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Centre (MS-ISAC) collaborate to issue guidance to help security experts and software developers in organisations to understand the techniques used by attackers in a phishing attack and how to reduce its impact and build more secure software (CISA, 2023). While these efforts are needed to support the institutional defences, they often overlook individual users, who lack equivalent resources and support.

As more people share personal and financial information online, cybercriminals find greater opportunities to exploit this data for malicious purposes. One of the most common and effective cyber threats is phishing, which tricks users into revealing sensitive information. Over the years, phishing attacks have evolved to become more sophisticated, making them a persistent and serious security concern (ICO, 2024).

Young adults are among the most digitally active groups, yet they may also exhibit overconfidence, under-estimating threats and overestimating their ability to recognise them, especially given how cleverly phishing attempts can mimic legitimate communications (Alabdan, 2020; Computing and Communication Services, 2025).

Despite the pressing and evolving landscape of cybercrime, most current research on individual users is mainly based on self-reported surveys (Alzahrani, 2021; Alzubaidi, 2021; Parsons et al., 2014; Sawaya et al., 2017), phishing field studies which send out simulated threats in different forms (Goel et al., 2017; Greitzer et al., 2021) and some lab-based experiments (Aleroud et al., 2020; Jaeger & Eckhardt, 2021). While valuable, these approaches often fail to capture actual lived experiences of participants, leaving a gap in our understanding of how users encounter and respond to threats in real-world contexts. Researchers and security experts have recognised the need to identify these individual differences and emphasised the importance of implementing security solutions that

consider users' differences and needs (Alohali et al., 2017; Coles-Kemp et al., 2020; Furman et al., 2012).

As cybersecurity incidents become more publicised, users are increasingly aware of the risks they face. However, this awareness often does not appear to lead to effective action. Many struggle to follow best practices, like protecting passwords or enabling two-factor authentication, often due to a lack of understanding. This gap in user knowledge undermines security guidance and leads to poor attitudes and behaviours, such as ignoring warnings and neglecting basic cybersecurity hygiene (Cain et al., 2018).

There is even a problem of understanding the terminology around cybersecurity. A study by Wu et al. (2020) found that 61% of the security terms used by security experts are difficult to understand by young adults (18–25 years old) who represented 70% of the study sample, even if they have an IT background. and though they may not be able to evaluate the risks associated with their actions.

There has been limited research focusing on cybersecurity awareness among young adults in Saudi Arabia, and even fewer studies have integrated individual characteristics, such as risk-taking, decision making, consideration of future consequences, and security behaviour intentions, to provide a comprehensive understanding of their online threat experiences. While some studies, such as that by Rawindaran et al. (2023), have examined cybersecurity awareness in the UK and KSA, they have mainly concentrated on policy and governance in small- and medium-sized enterprises rather than individual users. Consequently, there are even fewer studies that directly compare how young adults in these two countries experience online threats, including their attitudes and behaviours related to security.

Most research in KSA on online security primarily uses general questionnaires that ask questions about security awareness and IT usage. Only a few studies use standardised measures. While some researchers have examined the effect of Big-Five personality traits (Alseadoon et al., 2012), very few have utilised well-established scales to measure individual characteristics, which are common in cybersecurity research in Western countries. Following the suggestion that user studies from developed countries should be replicated in developing regions (Vashistha et al., 2018), this study uses some scales, such as the Security Behaviour Intention scale (SeBIS) (Egelman & Peer, 2015), to better understand younger adults' (aged 40 or younger) security attitudes and behaviours in a way that can be compared across cultures.

Given that this study compares the experiences of individuals from two different cultures, the following section provides a brief profile of the UK and KSA, highlighting key similarities and differences relevant to culture, digital infrastructure, and online security.

1.3 Choice of Populations for this Programme of Research: Younger Adults in the KSA and UK

This thesis investigated younger adults' perceptions and behaviours of online security threats in two culturally distinct yet technologically advanced countries: KSA and the UK. The choice of both the cultural contexts and the age range is deliberate, as they provide an opportunity to explore cultural similarities and differences in reactions to online security threats in an age group with particular vulnerabilities.

Culture has long been recognised as an important factor affecting individuals' attitudes in relation to online security (Halevi et al., 2016; Sawaya et al., 2017; Shah et al., 2023; Vashistha et al., 2018). In cybersecurity research, culture has been investigated and measured in different ways. Many researchers have used Hofstede's framework of cultural dimensions (e.g. individualism vs collectivism, power distance, uncertainty avoidance), for example, research by Shah et al. (2023). Other researchers have taken a more general approach, using participants' nationality or country of residence as a proxy for culture, for example research by Halevi et al (2016) and Sawaya et al. (2017).

While these individual studies produce many valuable insights but the use of very different measures of culture makes it challenging to compare their results.

In this thesis, I used the nationality of the participants (Saudi or British) to represent their cultural background. I did not use a specific cultural scale, such as Hofstede's dimensions, because I was not familiar with any recent scale for measuring culture in detail when I developed the programme of research. Also, using nationality as a proxy for culture is a common approach in research, particularly in studies on online security.

A study by Sakikawa (2024) offered a comparative cultural analysis between the UK and Saudi Arabia, drawing on Hofstede's framework. According to that study, the UK scores highly on individualism, indicating a strong emphasis on personal autonomy, independence, and self-expression. British culture also tends to favour low power distance, meaning that hierarchies are relatively flat, and authority can be questioned. The UK also demonstrates low uncertainty avoidance, suggesting that its institutions and people are more comfortable with ambiguity and risk-taking. In contrast, Saudi Arabian culture scores highly on collectivism, reflecting the importance of family ties, group cohesion, and loyalty. It also ranks high in power distance, meaning hierarchical structures are more accepted, and deference to authority is more common. Saudi Arabia also exhibits high uncertainty avoidance, pointing to a preference for rules, stability, and predictability in social and professional contexts. Thus, the UK and KSA are two countries with very different cultural profiles which are potentially relevant to online security.

Understanding how cultural context shapes cybersecurity has become increasingly important in explaining differences in security practices and has implications for the deployment of user-facing security systems. Creese et al. (2021) examined this issue through the Cybersecurity Capacity Maturity Model for Nations (CMM), developed by the University of Oxford's Global Cyber Security Capacity Centre. This model assesses how countries build cybersecurity capabilities across five dimensions: policy and strategy, culture and society, education and skills, legal and regulatory frameworks, and standards and technologies. Using data from 78 nations, they found regional differences in cybersecurity maturity, although these were influenced largely by economic development, governance quality, and internet usage rather than cultural factors alone. The study concluded that while cultural values, trust, and public awareness are important, they operate through broader social, economic, and institutional contexts that shape how cybersecurity is practised at the national level.

Cybersecurity culture in Saudi Arabia is shaped by its collectivist and high-context societal structure, where social norms, family networks, and religious values strongly influence perceptions and practices related to online security. Alowais et al. (2023) found that Saudi participants demonstrated

lower cyber hygiene practices compared to their American counterparts, partly due to cultural traits such as high power distance and collectivism. In such contexts, individuals are more likely to adopt security behaviours when authority figures mandate them and may place less emphasis on personal responsibility for cybersecurity.

The UK, reflecting a more individualistic culture, in which security is often considered a personal right and responsibility. A study by Harbach et al. (2016) showed that UK users generally demonstrate a relatively high level of engagement with basic cybersecurity practices. In a cross-national comparison of smartphone security behaviours, Harbach et al. (2016) found that 76.4% of the UK participants used secure locking methods, a higher rate than in the United States and other countries. Participants from the UK were also less likely to mention an "absence of threat" as a reason for not locking their devices compared to participants from Japan and Italy. These findings show a stronger baseline awareness of online risks and a greater sense of individual responsibility for device protection. Moreover, a password study indicated that language and cultural context also shape cybersecurity behaviour, with UK users, for example, often incorporating culturally meaningful words such as "football" into their password choices (Mori et al., 2020), reflecting how everyday culture influences security practices.

In relation to digital maturity, KSA has made rapid progress in building its digital infrastructure, becoming one of the most connected countries in the world. According to the Ministry of Communications and Information Technology (MCIT, 2025), fibre-optic networks now reach more than 3.9 million homes, and internet access covers almost 99 % of the population. This places Saudi Arabia among the top nations globally for online connectivity. The Communications, Space and Technology Commission (CST, 2025) reports that in KSA mobile phones are the main way people access the internet, accounting for 99.4 %of all online use. On average, each user consumes around 48 GB of mobile data every month, about three times the global average. The report also notes that KSA ranks among the top five G20 countries[1] for mobile internet speed. These achievements are part of the national Vision 2030 programme and the Digital Government Strategy 2023–2030, which aim to expand digital services, e-government systems, cloud computing, and large-scale data centres. Together, these efforts show the Kingdom's strong commitment to technological advancement and create a society where digital platforms are deeply integrated into daily life (National Portal, 2025). This high level of connectivity and rapid technological growth provide an important background for understanding how younger adults in KSA engage with online security.

The United Kingdom has also developed a robust and advanced digital infrastructure, making it one of the most digitally connected nations in Europe. According to Ofcom's Connected Nations 2024 report, full-fibre broadband is now available to 69% of UK households (Ofcom, 2025). Mobile connectivity is widespread, around 96% of the UK landmass now benefits from reliable outdoor 4G coverage provided by at least one operator, while 5G networks currently extend across roughly 62% of the landmass (Ofcom, 2025). These figures highlight the UK's well-established and mature communications infrastructure, supported by national initiatives such as Project Gigabit and the Wireless Infrastructure Strategy (Department for Science, Innovation and Technology, 2023).

[1] The members of the G20 are as follows: Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Republic of Korea, Mexico, Russia, Saudi Arabia, South Africa, Türkiye, the United Kingdom, the United States, the African Union and the European Union. (from: https://www.dfat.gov.au/trade/organisations/g20)

Together, they reflect a technologically advanced environment where individuals, particularly young adults, are highly connected and increasingly dependent on digital platforms for everyday life.

Overall, the UK and KSA represent two contrasting contexts for examining online security behaviour. Both countries have highly connected populations and advanced digital infrastructures, yet their cultural and social environments differ in meaningful ways. In the UK, social values tend to emphasise individual responsibility, autonomy, and privacy awareness, which align with more independent approaches to managing online risks. In contrast, Saudi society is characterised by collectivist values, where family, social ties, and respect for authority play an influential role in shaping digital behaviours. Despite these cultural differences, younger adults in both countries share similar levels of technology use and exposure to online threats, making this comparison valuable for understanding how cultural and contextual factors influence online security perceptions and practices.

This research programme focused specifically on younger adults, as they represent a significant proportion of Internet users globally. Almost all young people in the UK use the Internet, 99% of 16–44-year-olds are Internet users (Office for National Statistics, 2021). Similarly, in KSA, 98% of young people aged 15–34 years old are Internet users and have frequent access to social media websites (Saudi General Authority for Statistics, 2023). A recent study targeting students from King Khalid University in KSA examined the effect of internet addiction on young adults. It found that 21.57% of participants spent about 10 hours every day using the Internet (Wani & Wani, 2020).

Younger adults are often referred to as digital natives (Prensky, 2001a) because they have grown up using digital media and online communication. This constant exposure helps them to become skilled with technology and influences the way they think and interact online. However, their familiarity with the internet can sometimes lead to overconfidence, causing them to underestimate certain online risks such as phishing and malware. It is debatable whether their security practices are superior to those of previous generations. Research has shown that growing up with technology does not necessarily lead to improved security practices and knowledge (Furnell & Moore, 2014; Petrie & Merdenyan, 2016). A study by Vishwanath (2015) found that frequent use of online services, particularly social networking sites, has been identified as a factor that increases users' vulnerability to online threats.

Participants for this research programme were drawn from two culturally distinct countries, the UK and KSA but from the same age groups, to allow for comparison across these different cultural contexts. This approach enabled the exploration of whether the types of threats encountered, the cues used to identify them, and the solutions adopted to respond varied by country. It also enabled an examination of how cultural background may shape younger adults' perceptions and behaviours in relation to online security threats.

1.4 Methods Used in this Programme of Research

In this research programme, two primary methods were used: scenario-based surveys and diary-based questionnaires. The initial surveys (see Chapter 3 and Chapter 4) aimed to gather both quantitative and qualitative insights into younger adults' recent experiences with online threats. While surveys are a widely used method for capturing user attitudes and behaviours, they are often

criticised for relying on self-reported data, which can be prone to social desirability bias, memory limitations, and varied interpretations of security-related terminology.

To address these concerns, this research employed a scenario-based approach in the survey design. Instead of asking abstract or technical questions, the scenarios were grounded in real-world threat types that are commonly directed at individual users rather than organisations. These scenarios were carefully constructed based on an extensive review of actual threat characteristics, cues, and consequences for individual users. Participants were prompted with concrete descriptions of what they might see or experience on their devices (e.g. unexpected pop-ups, device crashes, or suspicious messages), facilitating them to more accurately recall and report relevant incidents.

Importantly, this study also drew upon two established cybersecurity threat frameworks, specifically, the Cyber Kill Chain and the MITRE ATT&CK frameworks, to guide the development and categorisation of these scenarios. These models helped to identify how individual users encounter, recognise, and respond to threats, particularly during the delivery and exploitation stages, where user behaviour is most critical. By aligning scenario design with recognised attack stages, this approach offers a novel analytical lens for evaluating user interactions within threat and enhances the theoretical robustness of the survey method.

Moreover, the scenario-based surveys aimed to improve data accuracy by shifting the focus from participants' abstract understanding of security incidents to their actual observations and behaviours. In contrast, previous studies (e.g. White et al., 2017) often relied on broad, technical questions such as "Have you experienced a virus or identity theft on your home computer?", an approach that assumes users can correctly identify and remember the details of such incidents. However, many participants may not realise they have been affected by malware or targeted by phishing, particularly when the attack is designed to appear legitimate or goes unnoticed due to subtle methods. For instance, participants might not recognise a phishing email or phone call if it is crafted in a highly convincing manner, or they may remain unaware of a malware infection if the device continues to function normally or if security software silently blocks the threat without user notification. By framing the questions around recognisable consequences and cues and placing them within the context of known threat stages, this study sought to reduce misreporting and better capture participants' experiences of online threats.

However, the scenario-based survey approach also had its limitations. Most notably, it restricted the investigation to researcher-defined threats, which may not fully capture the diversity of threats in users' real-world experiences. While the structured format allowed for consistent data collection across participants, it may have overlooked novel or less commonly recognised threats that users encounter in everyday digital contexts.

To address this limitation as well as other research questions, the second part of the research programme adopted a diary study method (see Chapter 5 and Chapter 6), in which participants were asked to monitor and report any suspicious online experiences they encountered any suspicious online experiences they encountered each day for a limited period of time. Unlike surveys that rely on general information, diary studies allow users to report events as they happen (or very soon after they happen), thus providing detailed and more nuanced insight into online threat exposure and detection.

The diary method offered several advantages for studying security behaviours. First, it helped confirm the frequency and types of threats that users encounter in everyday digital environments. It provided insight into how participants recognised and responded to potential threats within their specific contexts. Second, it enabled the observation of behavioural patterns over time, such as whether participants were consistently suspicious, ignored certain cues, or chose to interact with threats, patterns that are difficult to capture through traditional surveys. Third, the method encouraged reflection, prompting participants to articulate why they considered something suspicious and how they responded. This produced valuable qualitative data that helped unpack users' reasoning and decision-making processes. To the best of my knowledge, diary-based methods have not been used to study users' experiences of online security threats, making this approach a methodological contribution of the current research. Additionally, participants were asked to take screenshots of the threats they encountered, which added further depth to the analysis by allowing for examination of cues, such as layout, language, or common tactics, that are often overlooked or inaccurately recalled in retrospective self-reports.

1.5 Research Aim and Objectives

The main aim of this research is to explore how younger adults in the United Kingdom (UK) and the Kingdom of Saudi Arabia (KSA) perceive, detect, and respond to online security threats, and to understand how individual differences affect these experiences.

Overall Aim

The main aim of this research is to explore how younger adults in the United Kingdom (UK) and the Kingdom of Saudi Arabia (KSA) perceive, detect, and respond to online security threats, and to understand how individual differences affect these experiences.

Objectives

To achieve this aim, the research pursues the following objectives:

1. To identify the types and frequency of online security threats encountered by younger adults in the UK and KSA.
2. To examine how younger adults in both countries detect and respond to online threats and the cues that support their threat recognition.
3. To investigate how individual characteristics, such as risk-taking, security behaviour intentions, consideration of future consequences, and unrealistic optimism, affect their experiences of online threats.
4. To compare cultural similarities and differences between younger adults in the UK and KSA regarding their threat experiences, perceptions, and online security behaviours.

1.6 Thesis Structure

The remainder of this thesis is organised into six chapters, each addressing a specific component of the research process. An overview of the thesis chapters is as follows:

Chapter 2: This chapter reviews existing research on online security behaviours, focusing on individual users. It discusses various types of threats, defines these threats, and explores analytical

frameworks. Additionally, it presents an overview of the research on individual characteristics that influence user awareness and behaviours, as well as research methods related to researching online threats.

Chapter 3: This chapter presents the scenario-based survey of younger adults in the UK regarding their experiences with online security threats. It examines the cues they used to identify these threats and their responses. Additionally, it explores the relationship between their experiences of threats and their self-reported online security behaviours, measured by the SeBIS scale, and participants' computer knowledge and past experiences with online threats.

Chapter 4: This chapter presents the scenario-based survey of younger adults in the KSA regarding their experiences with online security threats, using the survey questionnaire as used in the UK study. It examines the cues they used to identify these threats and their responses. Additionally, it explores the relationship between self-reported behaviours, measured by the SeBIS scale, and participants' computer knowledge and past experiences with online threats.

Chapter 5: This chapter presents a 30-day diary study with younger KSA adults, exploring their real-time experiences with online security threats. It covers the types of threats encountered, participants' responses, and levels of suspicion. The analysis examines the appropriateness of these responses and how individual characteristics, such as security behaviours and risk-taking, influence interactions with threats.

Chapter 6: This chapter presents the diary study conducted with younger adults in the UK, refining the methodology used in the KSA study, examining their encounters with online threats. It focused on the frequency and types of threats, detection cues, and the influence of individual differences.

Chapter 7: This chapter presents a final discussion of all four studies to address the thesis research questions regarding younger adults' experiences with online threats in the UK and KSA. It compares findings from survey and diary data, and from the two countries, emphasising patterns in the types of threats, cues for detection, and response behaviours.

Chapter 2 Literature Review

2.1 Introduction

This literature review chapter provides an overview of research that has investigated online security from a human perspective. It examines studies on online threats that target individuals and how individuals respond to these threats and attacks. It also addresses factors that increase individuals' vulnerability to cyberattacks and the different approaches used to study individuals' susceptibility to cyber threats and how they respond to such threats.

2.2 Types and Definitions of Cyber Threats

Online threats are diverse and constantly evolving, making classification challenging. As new attack methods emerge and old ones are adjusted for new technologies, threat classification must be updated to remain relevant (Furnell, 2021). This research focuses specifically on threats targeting individuals rather than organisations. A review of research literature and reports from reputable cybersecurity organisations was conducted to identify the main threat types currently affecting individual users. In this thesis, the term "threat" refers specifically to intentional and malicious activities designed to compromise users' confidential data or online safety, such as phishing, malware, identity theft, and spoofed websites. Other forms of threats, such as accidental data loss, natural disasters, or unauthorised access caused by technical vulnerabilities and exploited by attackers, were not included in this review. These issues are primarily technical or organisational in nature rather than individual, and therefore fall outside the focus of this research, which examines how individuals experience and respond to online threats. The scenarios used in this programme of research were developed from a user's perspective, emphasising how individuals encounter and recognise security incidents during their everyday online activities. For instance, while hacking or unauthorised access occur through technical exploitation of systems, users typically perceive these incidents only through their consequences, such as suspicious messages or stolen accounts. In contrast, events like a lost or stolen hard drive involve physical rather than online security and are therefore outside the scope of this study.

Table 2.1 presents definitions of the online threats from the UK National Cyber Security Centre (NCSC) and the National Institute of Standards and Technology (NIST). In addition to the definitions in the table, other academic and industry sources were used to help understand each type of threat. Definitions from general security textbooks such as Pfleeger (2015) and Steinberg (2019) were also included in this section.

Table 2.1: Definitions of threat types affecting individuals used in this thesis.

Threat type/ subtype	Description	Source
Malware	**"**Derived from 'malicious software', malware is any kind of software that can damage computer systems, networks or devices. Includes *viruses, ransomware* and *trojans*.*"*	NCSC (n.d., section 13)
	"Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose."	NIST (n.d.-a)
Trojan horse/ Trojan	"A computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorisations of a system entity that invokes the program."	NIST (n.d.-b)
Virus	"A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk."	NIST (n.d.-c)
Ransomware	Ransomware is "a type of *malware* which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption."	NCSC (n.d., section 18)
Scareware	"Malware that scares people into taking some action. One common example is malware that scares people into buying security software."	Steinberg (2019)
Adware	"Software that generates revenues for the party operating it by displaying online advertisements on a device. Adware may be malware run without permission of a device's owner, or it may be a legitimate component of software."	Steinberg (2019)
Spyware	"A type of malware that installs on a device without the user's consent, collecting data and then sending it to a third party."	NCSC (n.d., section 19)
Phishing		
Phishing	"Scam emails or text messages that contain links to websites which may contain malware or may trick users into revealing sensitive information (such as passwords) or transferring money."	NCSC (n.d., section 13).
	"A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person."	NIST (n.d.-e)

Threat type/ subtype	Description	Source
Spear phishing	"A form of *phishing* targeting particular individuals, where the email is designed to look like it's from a trusted or known person."	NCSC (n.d., section 19).
	"A colloquial term that can be used to describe any highly targeted phishing attack."	NIST (n.d.-f)
Smishing	Smishing or SMS phishing is a "Combination of 'SMS' and 'phishing'. Untargeted text messages sent to large numbers of people, asking for sensitive information, or encouraging them to visit a fake website."	NCSC (n.d., section 19)
Vishing	Vishing or voice-based phishing is "phishing via POTS, that stands for 'plain old telephone service'."	Steinberg (2019)
Spoofed website	"A technique attackers use to appear to make their communications appear from a legitimate source. Email addresses, display names and domains can all be spoofed."	NCSC (n.d., section 19)

Expanding on the definitions in Table 2.1, the discussion below provides concise explanations of the threat types affecting individuals.

Malware, a term broadly defined as software intentionally designed to cause harm, includes variants such as viruses, ransomware, spyware, adware, scareware, and Trojan horses (Pfleeger et al., 2015). Shirey (2007) emphasised that viruses and Trojans typically disguise themselves as legitimate programs while performing hidden or destructive actions. Building on this, Steinberg (2019) described user-oriented threats such as scareware and adware, which manipulate individuals through pop-up messages or fake security alerts to prompt risky behaviour. Malware is frequently delivered through social engineering methods such as phishing, where deceptive emails or messages imitate trusted organisations to trick users into sharing sensitive data or clicking malicious links (Pfleeger et al., 2015; Steinberg, 2019). Modern variants include smishing and vishing, which use text or voice messages to reach victims. Closely related are spoofed websites, which replicate the appearance of legitimate sites such as banks or e-commerce platforms to harvest login credentials and financial information (Kaspersky, n.d.). These examples illustrate that many cyber threats now combine technical intrusion with psychological manipulation, exploiting users' trust and behaviours rather than purely technical weaknesses.

2.3 Classifications, Taxonomies and Analytic Frameworks

Humayun et al. (2020) undertook a systematic review of online threats and how frequently these threats appeared in security research. The systematic review process analysed 78 papers from 2007 to 2018, focusing on empirical studies and those that provided solutions to cybersecurity vulnerabilities. The authors found that 40% (16 out of 78) of the selected articles were published by researchers from the US and India, which indicated that these countries were the most active in this area. The victims most frequently mentioned in the reviewed articles were classified into two broad categories: individuals and organisations. The results suggested that organisations were more vulnerable to attacks. However, the authors stated, "There are some vulnerabilities that target both individuals and organisations" (p. 3182). This claim was not clearly supported by the results, as it was not explained carefully. Additionally, the review primarily aimed to identify the most frequent online attacks in the literature but referred to both threats and vulnerabilities. However, the behaviours identified as "Threats and Vulnerabilities" ("credential reuse", "cross-site scripting (XSS)", "denial-of-service (DoS)", "malware", "phishing", "session hijacking and man-in-the-middle attacks" and "SQL injection attack") are all examples of threats or attack methods, not vulnerabilities. Humayun et al. (2020) concluded that malware was the threat discussed most in the literature reviewed, followed by phishing.

Many taxonomies have been proposed to classify cyber threats, reflecting the growing complexity and evolving nature of the threat landscape. However, as Rabitti et al. (2024) note, the lack of standardisation and consistency among these taxonomies can lead to confusion and inconsistencies in threat analysis. Their study reviewed and grouped existing cyber risk taxonomies into four main types – attack-based, harm-based, operational risk-based and holistic – offering a clearer framework for understanding and comparing classification approaches.

One framework developed to help security experts analyse and understand various phases and features of cyber threats is the *Cyber Kill Chain*, developed by Lockheed Martin (n.d.). Another

example under attack-based taxonomies is the *MITRE ATT&CK framework***.** These two frameworks, which are used in this study, are discussed below.

2.3.1 Cyber Kill Chain

A kill chain is a conceptual model originally developed in military contexts to describe the structured sequence of steps required to carry out an attack, from initial planning to execution and final impact. In developing the Cyber Kill Chain, Lockheed Martin (n.d.) extended the military notion of a kill chain and applied it to cybersecurity. The Cyber Kill Chain, as it is currently known, divides cyber attacks into seven phases: reconnaissance, weaponisation, delivery, exploitation, installation, command & control, and actions and objectives (see Figure 2.1). The aim of the Cyber Kill Chain framework is to identify attackers' steps or the phases they must complete to compromise systems. If security experts (defenders) can stop the attackers in any phase, they will break the chain of the attack.

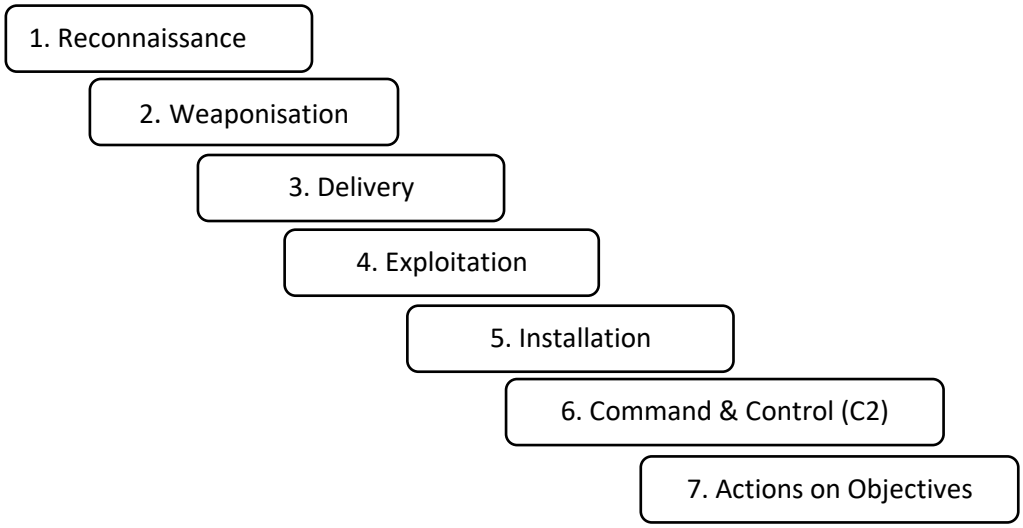


Figure 2.1: Cyber Kill Chain (Source: adapted from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html).

In the first phase, *Reconnaissance*, attackers try to identify a target by collecting information and conducting research about potential targets. This can be achieved by looking for targets on social media networks, collecting email addresses and finding information on target websites or newspapers. It is very difficult for the defenders to detect attackers in this phase.

The second phase is *Weaponisation*, in which attackers prepare the attacks. Attackers may use automated tools to generate malware and put it in a deliverable payload. Again, defenders can't detect this phase as it happens.

The third phase is *Delivery*. In this phase, the attackers launch their attacks and deliver their malicious files or links to their targets through emails, USB sticks, social media, or fake websites. This phase offers the most important opportunity for defenders to prevent the attack.

In the fourth phase, *Exploitation*, the attackers try to access the victims' systems. This can be done by exploiting software or human vulnerability and creating triggered exploits (nudging victims to open attachments or click on malicious links). Defenders can stop attackers from succeeding in this

phase by increasing target awareness and providing training for users. Among the measures that can be taken are scanning systems for vulnerabilities and restricting access to important resources by granting limited privileges.

The fifth phase is *Installation*, in which attackers install an implant or backdoor to gain long-term access. Defenders need to use various instruments to detect installation activities in this phase.

The sixth phase is *Command and Control*. In this phase, attackers remotely control the implants to manipulate victims' devices. This phase is considered the last chance for defenders to detect and block an attack.

In the final phase, *Actions and Objectives*, the attackers accomplish their original goals. These goals might include using ransomware to extract payment, destroying systems, modifying data, collecting users' credentials, or escalating access privileges.

2.3.2 MITRE ATT&CK

Another framework is MITRE ATT&CK, which provides a knowledge base of how attackers may breach systems and networks. It describes the problems of cyber attacks from the attackers' perspective (MITRE ATT&CK®, n.d.-a). The ATT&CK framework is designed to understand attackers' goals and their specific methods. The framework components include the following:

- *Tactics:* Represent the attackers' goals or motivations behind their actions (Why).
- *Techniques:* Describe the specific methods attackers use to accomplish their goals (How).
- *Sub-techniques:* Provide a more detailed, low-level breakdown of techniques to describe specific behaviours.
- *Procedures:* Outline the exact implementations or real-world examples of how adversaries employ these techniques or sub-techniques.

There are 14 tactics and within each tactic category, there is a series of techniques, each of which describes one way in which attackers may try to achieve their goals. Table 2.2 presents the tactics used in this study, together with the associated techniques (and sub-techniques where relevant). (For the full MITRE matrix, with all tactics and techniques, see https://attack.mitre.org/matrices/enterprise/)

The tactics and techniques are as follows: reconnaissance (10 techniques), resource development (8 techniques), initial access (10 techniques), execution (14 techniques), persistence (20 techniques), privilege escalation (14 techniques), defence evasion (44 techniques), credential access (17 techniques), discovery (32 techniques), lateral movement (9 techniques), collection (17 techniques), command and control (18 techniques), exfiltration (9 techniques) and impact (14 techniques).

Table 2.2: MITRE ATT&CK tactics, techniques and sub-techniques used in this study.

Tactic	**Proposed tactic ID**	**Technique (N sub-techniques)**	**Sub-techniques**
Reconnaissance	TA01	Phishing for Information (4)	Spearphishing Service Spearphishing Attachment Spearphishing Link Spearphishing Voice
Resource Development	TA02	Compromise Account (3)	Social Media Accounts Email Accounts Cloud Accounts
		Establish Accounts (3)	Social Media Accounts Email Accounts Cloud Accounts
		Obtain Capabilities (7)	Tools
		Acquire Infrastructure (8)	Domains Servers
Initial Access	TA03	Drive by Compromise	N/A
		Phishing (4)	Spearphishing Attachment Spearphishing Link Spearphishing Via Service Spearphishing Voice
Execution	TA04	User Execution (3)	Malicious Link Malicious File Malicious Image
Credential Access	TA05	Brute Force (4)	Password Guessing Password Cracking Forged Web Credentials: Web Cookies
		Credential from Password Stores (6)	Credential from Web Browsers
Impact	TA06	Data Encrypted for Impact	N/A

The main difference between the Cyber Kill Chain and MITRE ATT&CK frameworks is that the latter does not prescribe a specific order for the tactics and techniques it describes, whereas the Cyber Kill Chain presents a linear structure of an attack (Kidd, 2022). These frameworks have been explored in various studies that have compared their features, advantages and disadvantages (Naik et al., 2022)

The Cyber Kill Chain and MITRE ATT&CK frameworks were selected for this programme of research because they provide systematic and widely adopted approaches to describe the stages and methods used in cyberattacks. Although both were originally designed to describe cyberattacks from an attacker's perspective, their structured nature provides a clear way to map how different types of threats are experienced by individuals, for example, through the delivery of phishing messages, installation of malware, or data exfiltration.

Alternative frameworks such as the NIST Cybersecurity Framework (NIS, 2025) and Microsoft's STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) (Wikipedia, 2025) were also reviewed. STRIDE is highly effective for identifying vulnerabilities during system development; it is less suited to exploring how individual users experience online threats in everyday contexts. Similarly, the NIST framework emphasises risk management and organisational resilience rather than focusing on individual users' experiences.

In contrast, the Cyber Kill Chain and MITRE ATT&CK frameworks enable the identification of specific points where users interact with or are affected by an attack, aligning with the socio-technical focus of this thesis. Their wide recognition and practical application in both industry and academic research further support their suitability for analysing security threats.

2.4 The Impact of Online Threats

Security companies and organisations, such as Norton, Kaspersky, McAfee, the NCSC in the UK and Saudi Cert[2], have frequently sought to learn about the various consequences of different types of cyber threats. For example, Chigada and Madzinga (2021) undertook a systematic review to examine the impact of online threats and attacks during the COVID-19 pandemic. They found that attackers benefited from the chances that opened up to them due to the shift from operating in physical locations to engaging in digital communications.

Chigada and Madzinga's (2021) review showed that in the first quarter of 2020, cyber threats and attacks targeting financial institutions increased by 238% globally. There was a significant increase in ransomware attacks targeting healthcare organisations. More than 450 email addresses and passwords were leaked by attackers who had access to the World Health Organisation (WHO) server. In Asia, cybercriminals used fake news and the spreading of disinformation to deceive people. The study found that malicious URLs increased by more than 260% worldwide. More than 4,000 running domains linked to COVID-19 were used by attackers to collect personal information. Denial of service (DoS) attacks were expected to increase in 2020 to overload the servers of hospitals, businesses and governmental organisations with fake requests. Numerous spam and phishing emails with content related to COVID-19 were sent. In April 2020, 18 million COVID-19 phishing emails with malware were reported by Google.

The study also presented examples of mobile threats created by attackers during the pandemic period (2020-21). A ransomware application called *CovidLock*, pretending to be an Android app for tracking COVID-19 cases, was discovered as a malicious app. Users' phones were locked and they had 48 hours to pay US$100 in Bitcoin to unlock their devices (Chigada & Madzinga, 2021).

Once the consequences of an experienced threat have been identified, it is important to provide recommendations and guidance to help users respond to such threats. Lemonnier and Regan (2022), from AVG, recommend installing antivirus software, running virus scans, deleting infected files and restarting devices as mitigation measures against malware attacks. In addition, Kaspersky (n.d.-f) outlines 10 steps for malware removal, other than those mentioned by AVG, including disconnecting from the Internet, rebooting the computer in safe mode and updating software, browsers and operating systems.

[2] The national Computer Emergency Response Team (CERT) for Saudi Arabia

The McAfee Safety Series Phishing Protection Guide (McAfee, 2022) sets out four steps to be taken when someone experiences a phishing attack: reset passwords, let the company or institution involved know about the attack, report the phishing attack to the government's fraud agency, and monitor for credit and identity theft. Similar steps are outlined by Saudi Cert (n.d.) and in Phishing Scams: If You've Shared Sensitive Information, published by the NCSC (2021), for those who click on phishing links: inform banks in case they have entered their account details, update anti-virus software and scan the device, report the incident to the relevant IT people, change passwords and ensure activate two-factor authentication (2FA). Also, if they have entered one of their accounts, such as a social media account or email address, and they think it could be compromised, contact the service provider directly.

For website spoofing, Kaspersky Lab (2024) and Stouffer (2022) proposed steps to avoid being spoofed, which are considered prevention mechanisms rather than restorative measures.

The differences in recommendations from well-known security companies highlights the inconsistencies in guidance available to individuals facing cyber threats. These inconsistencies may be due to the evolution of cybersecurity practices over time, but they also emphasise the challenges individuals encounter when seeking guidance during attacks.

While recommendations for dealing with online attacks are crucial, prevention is equally important. One key preventive measure is maintaining good cyber hygiene. Cain et al. (2018) demonstrated the importance of cyber hygiene for users, as attackers always look for vulnerabilities that may arise due to users not following the best security practices. Recent research by Vishwanath et al. (2020) has formalised the idea of cyber hygiene as a measurable set of user practices that help prevent online risks and protect digital assets. These authors developed and validated a comprehensive framework for understanding and measuring cyber hygiene among individual Internet users. They defined cyber hygiene as the set of everyday practices and behaviours that protect users' devices, data, and online identities from compromise. The study introduced the Cyber Hygiene Inventory (CHI), a multidimensional, quantitative measure that captures five key domains of user security practices: storage and device hygiene, authentication and credential hygiene, email and messaging hygiene, transmission hygiene, and social media hygiene. Using a survey of 404 Internet users in Singapore, the authors tested the CHI's reliability and demonstrated its predictive value for cyber safety outcomes. Participants with higher CHI scores reported greater confidence in their ability to stay safe online (cyber self-efficacy) and engaged in fewer risky online behaviours. The study provided a validated conceptual definition and an evidence-based tool for assessing individuals' cyber hygiene, offering a more structured approach to understanding how everyday behaviours contribute to online security and risk reduction.

2.5 Research on Users' Perceptions and Behaviours Concerning Online Security

Many previous studies have highlighted the importance of the role users play in security solutions, as they greatly affect the success or failure of online security. When users fall victim to cyberattacks, the consequences can be serious, including financial loss, identity theft, reputational harm and even threats to personal safety. Thus, understanding users' attitudes is important to identify the factors that affect their actions or responses to online threats. Human error and behaviours are related directly or indirectly to many security incidents and data breaches (Evans et al., 2019). According to CybSafe (2020), users' mistakes account for 90% of cyber data breaches in the UK. Cybercriminals

frequently utilise social engineering techniques to deceive users into clicking malicious links or downloading damaging attachments, enabling their attacks (Alkhalil et al., 2021).

To better understand human aspects of cybersecurity, Spero and Biddle (2020) discussed the relationship between users' mental models of security and the design of user interfaces (UIs). They highlighted the need to enhance the sources of users' mental models, which are shaped by their direct experiences, analogies to other domains and stories from others. They presented three case studies, on malware, phishing and fraudulent websites, to illustrate that the current state of UI design typically does not sufficiently assist users in forming appropriate mental models of security. This gap may lead to risky behaviours and increased vulnerability to cyberattacks. The authors proposed that improving the visibility of security information in UIs could facilitate better-informed decision-making and enhance overall attitudes to security.

Moustafa et al. (2021) examined the impact of human factors on enhancing cybersecurity. They reviewed previous studies that focused on how human practices, such as sharing passwords, falling victim to phishing attacks and ignoring security warnings, can heighten vulnerability to cyber threats. They discussed the influence of individual differences in behaviours related to security practices, particularly traits like procrastination, impulsivity, future-oriented thinking and risk-taking behaviours.

Pattnaik et al. (2023) provided a comprehensive review of user perspectives on security and privacy in home networking environments. Through a meta-review of 52 papers and a systematic literature review of 126 papers for studies published between 2010 and 2021, they explored how users' awareness, perceptions, and behaviours shape cybersecurity practices in connected smart homes. Their findings revealed that users' protective practices, such as managing passwords, securing Wi-Fi, and configuring smart devices, are often inconsistent despite high awareness of risks. Many users rely on default security settings or informal support from family and friends rather than formal guidance. The review also highlighted demographic and contextual influences, including differences by age, gender, and household type, as well as the impact of usability and trust in devices on security behaviour. The authors concluded that empowering users through improved interface design, personalised awareness interventions, and clearer privacy controls is critical for reducing home network vulnerabilities.

Dodge et al. (2023) applied Protection Motivation Theory (PMT) to examine the factors influencing individuals' intentions to adopt cybersecurity practices. The study used a factorial survey experiment in which participants responded to hypothetical phishing vignettes that varied perceived threat severity, vulnerability, and response cost. Based on a sample of 720 American adults, the findings showed that higher perceived severity and vulnerability significantly increased users' willingness to follow recommended security actions, while greater self-efficacy and belief in the effectiveness of protective measures also encouraged compliance. In contrast, higher perceived response costs, such as time or effort required to act securely, reduced the likelihood of following safe practices. The authors concluded that interventions focusing on enhancing users' confidence and perceived effectiveness of security measures are more likely to promote lasting behavioural change than fear-based approaches.

Recent research has examined cybersecurity awareness in Saudi Arabia, with particular attention to younger users and educational contexts. Alotibi (2024) developed a comprehensive cybersecurity awareness model specifically designed for Saudi students to protect them from social engineering attacks on social media. Using a design science methodology, the study reviewed fifty previous works on cybersecurity awareness in the Kingdom and proposed a four-stage model focusing on education and training, developing policies and guidelines, improving school security, and continuous monitoring and evaluation. The model highlights the need for structured awareness programs that consider cultural, linguistic, and institutional factors unique to the Saudi context, aiming to promote responsible online behaviour and enhance digital literacy among students.

Several studies were conducted to explore how psychological theories can explain and predict users' cybersecurity behaviours.

2.6 Measuring Users' Attitudes and Behaviours Concerning Online Security

Methods for measuring attitudes and behaviours have been investigated in many studies, with a range of different methods being used. Questionnaires and standardised scales are among the most common methods.

2.6.1 Security Behaviour Intention Scale (SeBIS)

Egelman and Peer (2015) developed the Security Behaviour Intention Scale (SeBIS) to measure users' attitudes towards common security practices. The scale consists of 16 items mapped to four security areas: device securement, password generation, proactive awareness, and updating. The development of this scale followed the approach outlined by Netemeyer et al. (2003):

- Construct definition and content domain: Clearly define what the scale is supposed to measure.
- Generating and judging measurement items: Developing a list of possible questions and analysing them to exclude invalid ones.
- Designing and conducting studies to develop and improve the scale: Exploratory factor analysis (EFA) is used to reduce the questions and find hidden constructs to develop a model.
- Finalising the scale: Confirmatory factor analysis (CFA) is used to check that the scale fits the intended model, as well as assuring the reliability of the study.

Initially, the researchers collected security advice offered to users by nationwide US organisations such as the US Computer Emergency Readiness Team to create an initial set of security behaviours. This set was revised after interviews with six security experts, resulting in 30 behaviours that were written as personal statements and evaluated on a five-point Likert scale. The scale was initially evaluated with a sample of 479 Mechanical Turk participants, which resulted in the number of items being reduced to 24. The scale was then refined and an additional group of participants revised the set of items. This resulted in a final scale consisting of 16 items, four subscales: Device Securement, Password Generation, Proactive Awareness and Updating.

The SeBIS was validated in a further study that correlated four subscales with observed security behaviours. Egelman et al. (2016) conducted three experiments to demonstrate the predictive value of the scale for actual security behaviours. The first experiment was done online using Mechanical Turk participants to examine awareness and password subscales. For the Proactive Awareness subscale, 718 participants completed three tasks (not part of this study), but with a screenshot of a

website displayed between each task, two were legitimate (Amazon and Twitter) and one spoofed PayPal. Participants needed to check the URL to identify which website was legitimate or not.

At the end of the part of the experiment, the participants were asked to create a password to be used after two weeks to complete the second part of the experiment, which was completing the SeBIS Scale. The password creation requirements were simple and weak to check if participants would create strong passwords. Also, they were asked if they would reuse passwords they had already used previously. The passwords were assessed with the Password Guessability Service (PGS) and 14.7% passwords could not be cracked. For those who created strong and uncrackable passwords, their mean scores on the Password Generation subscale of the SeBIS were significantly higher than for those who created weak passwords, validating this subscale. In addition, to validate the Proactive Awareness subscale, participants' accuracy in recognising the spoofed website was investigated. Participants who correctly identified the spoofed website scored significantly higher on the Proactive Awareness subscale, validating that subscale.

The second experiment was conducted to validate the Updating subscale. 281 Mac-using participants were recruited from Mechanical Turk. They were asked to complete the SeBIS Scale and provide information about their Mac device. This allowed the researchers to determine whether a recent update for the Mac had been installed. Only 24.2% of the participants were found to update their devices promptly and their scores on the Updating subscale were significantly higher than those who had not updated their devices.

The SeBIS securement subscale was validated with a third experiment with participants from PhoneLab (an experimental platform of 200 Android smartphone users who agreed to participate in research). Their devices were monitored to record whether they used PIN or drawing patterns to lock their device, or another less secure method, the slide to lock. 49.3% were found to use the insecure method, and their scores on the Device Securement subscale were significantly lower than those who locked their devices with either PIN or patterns.

These three experiments were a good initial validation of all four subscales of the SeBiS. This scale has also been used in other studies to examine the relationship between individual factors and cybersecurity behaviours (Egelman & Peer, 2015a; Gratian et al., 2018).

A limitation of this validation of the SeBIS Scale was that these experiments used Mechanical Turk workers, with no screening of participants for location or success on Mechanical Turk being mentioned. At the time of the study, about 75% of MTurkers were located in the USA, about 16% in India and the remaining 9% in a range of other countries (Difallah et al., 2018). This means that the samples of users from the US may not be representative of user behaviours worldwide, with a bias toward the USA. Cultural diversity, different levels of digital knowledge and different threat types can all have an impact on security behaviours. Additionally, many researchers (and journals) are somewhat sceptical of the quality of data from Mechanical Turk, citing issues such as inattention, inconsistent English fluency, and excess speed in completing tasks (due to low monetary rewards) as issues (Aguinis et al., 2020; Douglas et al., 2023). There are now recommendations for how to use Mechanical Turk to improve data quality (Aguinis et al., 2020), as well as other platforms which recruit participants specifically for research and provide more appropriate compensation (e.g. Prolific).

Huang et al. (2023) built on SeBIS to create a psychometric scale for assessing users' behaviours in relation to smartphone security. First, they evaluated the four dimensions of SeBIS for smartphone security behaviours. The findings suggested that while SeBIS provides a solid foundation, its dimensions need refinement to better reflect smartphone-specific security intentions. As a result, they developed the Smartphone Security Behaviour Scale (SSBS), comprising 14 questions grouped into two factors: Technical approach and social approach. However, this newly developed scale was validated with a Mechanical Turk sample, so it has the same limitations as discussed in relation to SeBIS.

2.6.2 Human Aspect of Information Security Questionnaire (HAIS-Q)

Another standardised scale is the Human Aspect of Information Security Questionnaire (HAIS-Q), developed by Parsons et al. (2013, 2014). The first stage in developing the HAIS-Q comprised a hybrid method employing qualitative and quantitative methods for data collection and analysis. Interviews were conducted with senior managers from three Australian government organisations. The results of the interviews helped develop an exploratory questionnaire, which was completed by employees from the same organisations.

Parsons et al.'s (2013, 1014) work aimed to develop and test the reliability and validity of the HAIS-Q, as well as to determine if there were positive correlations between respondents' knowledge of information security policy and procedures, attitudes towards policy, and procedures and self-reported behaviour when using computers for work. It is based on the Knowledge-Attitude-Behaviour model, which proposes that the level of knowledge users have about security policy and procedures affects their attitudes and when attitudes improve, it leads to improvements in security behaviour. The HAIS-Q contains 63 items, divided into 7 areas: password management, email use, Internet use, social media use, mobile devices, information handling, and incident reporting. Each area has three sub-areas, measured by a separate KAB item. HAIS-Q items are measured on a five-point scale from "strongly disagree" to "strongly agree".

The validity of the HAIS-Q was assessed using different methods and participants (employees, students and the general public) in an Australian context. Parsons et al. (2017) conducted an empirical, lab-based phishing study with 112 university students who assessed eight emails to determine which was a phishing email. Then they completed the HAIS-Q. A positive correlation was found between the HAIS-Q score and performance in the phishing identification task. Parsons et al. (2017) noted that while this scale has been used in the Australian context and among a range of populations, it needs to be validated for use in different countries and cultures.

The HAIS-Q was used by McCormac et al. (2016) to examine the effect of age, gender, personality and risk-taking propensity on ISA. The study conducted a survey of 505 working Australians to assess individual differences. Individuals' ISA were found to be largely explained by conscientiousness, agreeableness, emotional stability and risk-taking propensity, rather than age or gender.

The HAIS-Q has also been used to compare the results of self-reported surveys and interviews. Pattinson et al. (2016) conducted two studies involving an online survey and interviews in which they recruited 23 Australian university students and asked them about their attitudes towards the seven areas of the HAIS-Q: They found that participants' attitudes towards password management,

social media use, information handling and incident reporting did not correlate with their behaviours.

While previous studies have used standardised and validated questionnaires, Bitton et al. (2020) employed a different approach, conducting a long-term study to evaluate smartphone users' ISA. They used three methods: a security questionnaire, a mobile device agent and a network traffic monitor. The study aimed to assess users' ability to mitigate social engineering (SE) attacks, a major security threat targeting mobile devices through human vulnerabilities.

The first method employed was a self-reported security questionnaire, designed to measure users' cybersecurity behaviours. This questionnaire contained 40 items categorised into five areas: application installation, application handling, browsing and communication, device management and communication channels. Responses were recorded on a five-point Likert-type scale (anchored at “never” and “always”) to assess the likelihood of users engaging in security-related actions.

To overcome the limitations of self-reported data, the study also logged users' actual behaviours through two data collection methods. A mobile device agent monitored participants' device connectivity, installed applications, content and security settings, while a network traffic monitor observed Internet activity by tracking domain names, application-layer protocols and contextual data. Over seven weeks, 162 university students were unknowingly subjected to various security challenges, including phishing attacks, spam pop-ups, permission requests and certificate manipulations. Participants were told the study focused on browsing habits to prevent changes in their natural behaviour.

The findings revealed a discrepancy between self-reported and actual security behaviours. While the data collected from the mobile agent and network traffic monitor correlated positively with participants' success in facing security challenges, the questionnaire responses showed no significant correlation with actual awareness levels. This suggests that self-reported security awareness may not accurately reflect real-world behaviour, reinforcing the need for objective behavioural assessments in ISA research.

There are ethical issues with such a study as participants’ real data were collected and this may include some confidential data. The authors stated that the institutional review board approved the study as the participants were participating of their own volition; they received a one-time payment and were aware of the type of data that would be collected. However, they had not provided informed consent about the security challenges.

2.7 Susceptibility to Online Threats: Research Methods

Several studies have highlighted the increasing sophistication of phishing attacks and their widespread impact on individuals and organisations (Alkhalil et al., 2021; Chiew et al., 2018). These studies have emphasised that phishing remains a persistent security concern, evolving alongside technological advancements.

2.7.1 Methods for identifying phishing susceptibility

Researchers have employed various methodologies to understand better how people fall for phishing. Some of the most common approaches that have been widely used in the literature are set out below.

Survey methods
Alyahya and Weir (2021) employed a scenario-based survey to examine how Saudi undergraduate students responded to phishing emails. The scenarios were structured around social engineering strategies and incorporated elements of the Theory of Planned Behaviour (TPB) to measure user responses. Albladi and Weir (202) used an online questionnaire to develop a predictive model of user vulnerability based on individual characteristics, including social network involvement, usage motivation, and perceived competence in managing online threats. Another study by Wu et al. (2020) used online questionnaires to measure participants' understanding of different security terms used by experts when they wrote security texts and articles.

Lab experiments
Aleroud et al. (2020) designed a lab experiment to investigate Jordanian students' susceptibility to spear phishing. The participants were asked to visit three spoofed web pages created to mimic the university's web pages. They were instructed to check the content and components of the pages and log in to examine the services. Once they completed the tasks, they were asked to answer dichotomous (yes/no) questions related to what they did. Then, they were asked to rate their security-related knowledge, trust-related issues and susceptibility to spear phishing.

Simulation and role-play
Jayatilaka et al.'s (2021) study asked participants from an Australian university to process phishing and legitimate emails in a simulated web client. The experiment used think-aloud and role-play approaches to understand the decision-making processes among the participants. Different factors were found to increase participants' susceptibility to phishing, such as sender legitimacy, professional look, emotional attachment within the email, familiarity of the title and body of the email, alignment with participants' context and previous phishing experience.

Another study by Jaeger and Eckhardt (2021) was conducted in a simulated office environment. The participants acted like employees and processed 20 emails using a webmail system similar to one they would use at work. Each participant received a username and password and was told to treat this account information as their own, without a focus on security. An eye tracker recorded where they looked and what they did on the screen during the task. The email set included 14 real emails and 6 phishing emails that had fraudulent links or attachments. After finishing the email task, participants completed a questionnaire to avoid any bias. The study ended with a discussion about phishing risks. The entire session lasted about 60 minutes on average.

Greitzer et al.'s (2021) study involved a three-week phishing campaign, with three simulated phishing emails. Each email represented a different context from everyday life: an IT helpdesk issue, a package delivery failure and a suspicious credit card charge. The emails were sent using the Gophish platform and each email directed users to a realistic phishing landing page. The domain names were carefully crafted to resemble legitimate ones but contained subtle inaccuracies (e.g. using .com instead of .edu). The primary measure of phishing susceptibility was tracking how many

users clicked on the phishing links. Additional technical and behavioural data were also collected, including click timestamps, user roles and operating systems. Pre- and post-campaign surveys assessed user traits, such as impulsivity, emotional stability and security habits. The participants were generally informed about the phishing test through a broad notification email, but not about the specific details of the emails. After the campaign concluded, a debriefing email was sent to all participants.

Diary Methods

Diary studies offer an alternative approach by capturing users' experiences with phishing over time. By tracking daily interactions with suspicious messages and security decisions, diary studies provide a more detailed understanding of phishing susceptibility, user awareness, and response patterns.

Diary studies have been widely used in HCI research to capture user experiences, behaviours and interactions over an extended period of time. They allow researchers to collect qualitative and quantitative data on people's experiences with technologies in their everyday lives. Diary studies have become useful methods for studying security and privacy behaviours. Unlike retrospective surveys, which rely on memory recall, diary studies allow researchers to collect longitudinal data on how individuals recognise, interpret, and respond to potential security risks.

For example, a study has been conducted to understand the experience of online risks by adolescents (Wisniewski et al., 2016). A web-based diary study was conducted over two months with 68 American teenagers (ages 13–17), who documented their weekly online experiences involving four types of risks: information breaches, online harassment, sexual solicitations, and exposure to explicit content. Participants received automated weekly reminders. When participants encountered any risk, they responded to open-ended diary questions detailing their experiences. Throughout the study, a total of 207 unique risk events were reported, including 119 instances of exposure to explicit content, 31 cases of information breaches, 29 reports of sexual solicitation, and 28 incidents of online harassment.

Diary studies have also been applied to emerging security concerns in smart home and IoT environments. For instance, researchers used diary methods to examine how users experience security and privacy risks in smart home and IoT products (Chalhoub & Kraemer, 2021; Turner et al., 2022).

2.7.2 Measures of Susceptibility to Online Threats

Many studies measured user susceptibility by examining the indicators they use to differentiate phishing attempts from legitimate emails and websites. For example, Kang et al. (2021) asked participants to evaluate a set of images as either legitimate or phishing and phishing emails were created using some open source services such as Phish Bowel.[3] In another study, a role-play scenario-based experiment was conducted in which participants evaluated 20 different Facebook profiles, each accompanied by a contextual scenario about the profile owner, to assess trustworthiness (Algarni et al., 2017).

Greene et al. (2018) undertook a long-term phishing field study to examine how individuals make decisions when they encounter links or attachments in phishing emails. They collected phishing click-

[3] https://it.cornell.edu/phish-bowl.

rate data over 3.5 years, followed by three phishing training emails designed around real-world threats at the time. After each email, a corresponding survey was distributed to gather feedback on participants' click decisions. The participants were more likely to click on phishing emails if the content aligned with their work role. When the email premise was misaligned with their work environment, they focused on other specific cues, such as the sender's email address and layout. A notable distinction emerged between clickers and non-clickers**:** clickers were primarily concerned with the consequences of not responding, whereas non-clickers focused on the potential consequences of clicking, such as malware infection.

Building on Greene et al.'s (2018) results, Steves et al. (2020) developed the NIST Phish Scale to aid organisations and security experts in their phishing training and awareness. The scale was designed to assess the difficulty of identifying phishing emails by evaluating the specific cues present in the message and their contextual relevance for the recipient. The Phish Scale aims to standardise the evaluation of phishing email complexity and explain variations in user susceptibility, even when individuals are exposed to the same phishing simulation. The scale has two key components: cue count and alignment. Cue count refers to the number of commonly recognised indicators of phishing found in the email, such as spelling errors, mismatched sender names, urgent language, generic greetings and suspicious URLs. A higher cue count usually indicates a more obviously malicious email, making it easier to detect. Alignment, in contrast, refers to how well the email content matches the recipient's role or responsibilities. When alignment is high, the email is considered more difficult to identify as a threat. In the NIST study, trained analysts used a coding protocol to identify these cues and evaluate alignment levels across different simulated emails. These ratings were then used to assign each email a Phish Scale score, indicating the relative difficulty of detection.

Kang et al. (2021) analysed 40 emails, comprising 20 phishing emails from Cornell University's "Phish Bowl" database and 20 legitimate emails received by the research team. The researchers examined 12 different cues embedded within these emails to assess whether they indicated legitimacy or phishing. They found that while phishing emails contained more suspicious cues on average, legitimate emails could also include misleading elements, such as misspellings or missing greetings. Similarly, phishing emails sometimes incorporate non-suspicious features to appear legitimate. These findings highlight the complexity of phishing detection, as no single set of cues can reliably distinguish phishing emails from legitimate ones, making user decision-making more challenging.

2.8 Individual Differences in Cyber Security Behaviours and Susceptibility Due to Individual Differences

To date, several studies have highlighted factors that influence individuals' security behaviours and attitudes in online contexts. These cover a wide range of dimensions, including personality traits, psychological aspects and contextual variables. However, the findings from various studies have tended to be inconsistent in terms of identifying which dimensions have the greatest impact on individuals' behaviour and attitudes. Among the many dimensions studied, some have emerged frequently in the research literature. These include personality traits, impulsivity, risk perception, risk propensity, cognitive biases (such as unrealistic optimism and the third-person effect), perceived threats, perceived severity, fear appeals, decision-making styles, self-efficacy and perceived benefits. It is important to note that while these dimensions have repeatedly been examined in studies, their relative importance and impact on individuals' cyber security behaviours and attitudes may differ

depending on the context and population being studied. Understanding the complex relationships between these dimensions is an important step in effectively addressing cyber security challenges.

Albladi and Weir (2018) developed and validated a user-centric framework to understand individuals' susceptibility to social engineering attacks on social networks. The novelty of this framework lies in its ability to identify the most important attributes that affect individuals' threat detection abilities and explain how they behave in response to online attacks. The framework consists of 14 attributes, grouped into four categories:

- *Socio-psychological:* Personality traits, demographics and culture
- *Social-emotional:* Trust in social network providers, trust in social network members and motivation to use social networks
- *Perceptual:* Perceived risk of social networks, perceived severity of threats, perceived likelihood of threats, self-efficacy, privacy awareness, security awareness and past experience
- *Habitual:* Level of involvement in social networks

The framework was validated through a mixed-method study. In the quantitative phase, a survey targeted information security specialists, asking them to rate the importance of the framework's factors on a five-point Likert-type scale. In the qualitative stage, security experts from academia were asked open-ended questions about the framework, such as which factors should be combined, split, or added. The framework was then revised based on the feedback from the experts.

The results indicated that gender was not considered an important attribute in determining users' vulnerability to social engineering attacks, while computer knowledge was identified as the most critical factor overall. Interestingly, the perceived severity of threats received the lowest ranking among the perceptual attributes.

Although this study highlighted several key attributes, many of which have been previously discussed in the literature as influencing users' susceptibility to online attacks, it did not fully answer the main research question: How do these factors specifically influence users' vulnerability to SE attacks? Furthermore, although the study sought to explore the role of culture by comparing the feedback of experts from different nationalities regarding the importance of each factor in the framework, this approach did not adequately reflect the true effect of culture on people's vulnerability to SE attacks. The feedback was limited to the experts' professional opinions rather than actual user behaviour and did not account for how cultural norms, values and social dynamics might influence users' behaviours when faced with SE attacks. The authors themselves acknowledged that the chosen validation approach may not have been the most effective. They highlighted that at some stage experimental studies would be necessary to obtain more accurate and reliable results.

2.8.1 Risk Perception and Decision-Making in Online Security

Van Schaik et al. (2017) conducted a quantitative online survey to examine the relationship between risk perception and precautionary behaviours related to online threats among university students. The study involved 436 experienced Internet users from the UK and the US, with a mean age of 23 years. The researchers assessed 16 online threats, including identity theft, phishing and malware, by measuring risk perceptions through various dimensions such as severity, voluntariness and control, while also tracking self-reported precautionary behaviours such as the use of antivirus software. The

findings revealed that perceived severity and catastrophic potential were the strongest predictors of higher risk perception, while perceived control significantly influenced precautionary behaviours. Notably, participants who felt less in control of security risks were more likely to perceive those risks as higher; conversely, those who felt more in control were more inclined to engage in protective actions, such as installing security software.

In 2018, Van Schaik et al. conducted a similar study that also measured risk perception across multiple dimensions, including severity, dread, voluntariness and control. While the first study focused on general online security threats, the second study tailored its questions to specific privacy and security settings on Facebook, such as sharing phone numbers or email addresses, and targeted non-students in the UK. The study confirmed the previous study's findings regarding the dimensions that influence risk perception. Significant predictors of perceived risk included participants' attitudes towards sharing information on Facebook, feelings of dread, a sense of voluntariness, catastrophic potential and their experience with the Internet. Similarly, the predictors of precautionary behaviour included perceived risk, a sense of control, voluntariness and Internet experience.

While these studies employed customised questions to assess risk-taking behaviours in the context of cyber threats, standardised scales have also been used to provide a validated framework for investigating the relationships between individual constructs, such as risk perception and decision-making, and cybersecurity attitudes and behaviours. Two studies, conducted by Egelman and Peer (2015a) and Gratian et al. (2018), used the Domain-Specific Risk-Taking (DOSPERT) scale developed by Weber et al. (2002). This scale was designed based on insights from Weber and colleagues regarding the various elements that influence risky decision-making. The DOSPERT scale allows researchers to measure two key components: conventional risk attitudes, which refer to the extent of risk a person reports being willing to accept, and perceived risk attitudes, namely a person's willingness to take a risk based on how risky they think it is. The scale addresses five areas in which people frequently make risky decisions: ethical, financial (divided into gambling and investment), health/safety, social and recreational. The scale was developed to cover a broad range of risks experienced by young adults in Western countries.

The scale was revised in a further study by Blais and Weber (2006), which produced a shorter and more general scale that could be used with participants representing different age groups, educational levels and cultures. The revised scale has 30 items instead of the original 40 and has been translated into many languages, including Italian, Dutch, German and Spanish. In the revised version, a different analytic approach was used to help understand the relationship between risk-taking and risk perception. To improve psychometric quality, the scale points were increased from five to seven, all labelled. Also, recognising that the respondents might not have the experience or background to have faced each of the situations described on the scale, they were instructed to indicate how likely they would be to engage in the described activities or behaviours if they were in those situations.

Egelman and Peer's (2015a) study measured decision-making, risk-taking, personality traits and security behaviours to determine the strongest predictors of cybersecurity and privacy. They explored the relationship between SeBIS and other psychological constructs, identifying a correlation between SeBIS and various other scales: DOSPERT, General Decision Making Style (GDMS), Need for Cognition (NFC), the Barratt Impulsiveness Scale (BIS), and Consideration for Future Consequences (CFC). Participants with higher inquisitiveness (as measure by the NFC scale) and greater

consideration for future consequences (as measured by the CFC) showed better security practices across all four SeBIS subscales. Willingness to take risks was inversely correlated with the proactive awareness and software updates subscales. Additionally, those who engaged in better security behaviours were less likely to procrastinate (GDMS avoidant sub-scale) and those scoring low on GDMS dependence scored high on SeBIS awareness, indicating proactive security behaviours. Finally, many security behaviours were inversely correlated with impulsivity, suggesting that good security practices involve foresight.

Gratian et al. (2018) surveyed 369 students and faculty from a university in the US to examine the correlation between cybersecurity behaviour intentions and four factors: demographic characteristics, personality traits, risk-taking and decision-making style. The study was built on the works of Egelman and Peer (2015) and Egelman et al. (2016). Egelman and colleagues were among the first to investigate the correlation between security behaviours, such as device protection, password creation, proactive awareness and updates, and risk-taking preferences and decision-making styles. Gratian et al. (2018) validated and expanded Egelman's work by applying SeBIS and analysing the correlation between risk-taking preferences, decision-making styles and security behaviour intentions. Moreover, they extended the previous research by exploring the links between demographics, personality traits and security behaviour intentions, an approach they claimed had not been applied before. This expansion provided a comprehensive evaluation of how these human factors influence cyber security behaviours.

Gratian et al. (2018) conducted a principal component analysis on the SeBIS and revealed that the factor loadings and variance explained by the four SeBIS subscales were consistent with the findings of Egelman and Peer (2015b), providing further validation of SeBIS. In terms of demographic factors, gender had a significant effect on three SeBIS subscales, Password Generation, Proactive Awareness and Updating, with women reporting weaker security behaviour intentions than their male counterparts. Additionally, for personality traits, extraversion emerged as a significant predictor of good Device Securement behaviour.

Aligning with the findings of Egelman and Peer (2015b), there was no effect of risk-taking preferences on Device Securement. However, unlike that study, a correlation was found between rational decision-making and Device Securement. Also, there was no relationship between avoidant decision-making and Device Securement, in contrast to the results of Egelman and Peer (2015b).

There was no correlation between risk-taking preferences and the Password Generation subscale, whereas Egelman and Peer (2015b) found ethical and social risk-taking were significant predictors of Password Generation scores. Additionally, while Egelman and Peer (2015b) identified both rational and avoidant decision-making as predictors of strong Password Generation scores, Gratian et al. (2018) found only avoidant decision-making to be significant. Consistent with Egelman and Peer (2015b), Gratian et al. found that ethical risk-taking significantly affected Proactive Awareness scores. Their findings supported Egelman and Peer's results showing correlations between proactive awareness and rational, avoidant and dependent decision-making styles. However, Gratian et al. (2018) found no relationship between ethical risk-taking and Updating subscale, while health/safety risk-taking remained a significant predictor. Additionally, while both studies found correlations between updating and rational, avoidant and spontaneous decision-making styles, Gratian et al.'s (2018) study showed that adding personality traits, particularly conscientiousness, suppressed the effect of the avoidant style.

Ayyagari and Crowell's (2020) study further assessed SeBIS as a security behaviour intention scale among students from an American university. It proposed using a scale that specifically measured risk associated with online security rather than general risk, such as the risk-taking scale (DOSPERT), as employed by Egelman and Peer (2015b). Ayyagari and Crowell, chose not to use DOSPERT in their study because security-related risks in information security, such as password management and device securement, do not fit well within DOSPERT's existing categories such as health and financial risks. Instead, they developed a security-specific risk scale to more accurately measure these unique risks, enhancing the understanding of information security behaviours and aligning better with the security context they were studying.

Rogers (2017) adapted the DOSPERT scale, reducing it from 30 to 18 items and replacing culturally sensitive items like the reference to gambling to fit the United Arab Emirates (UAE) cultural context better. However, despite these adjustments, the study sample primarily comprised international students from 22 countries, including North America, Africa, Europe, and Asia, rather than a specifically Arab population. Also, the reduction made to the scale items was not explained clearly, especially since the author removed a complete area (ethical) without justifying how this dramatic change would make the scale more suitable for the context of Arab populations.

Overall, these studies suggest further research is needed to gain a better understanding of how individual characteristics such as risk perception and decision-making style affect security behaviours and intentions in different contexts.

2.8.2 Impulsivity as Predictor of Susceptibility to Online Threats

Impulsivity and locus of control have been examined as predictors of susceptibility to online threats. Impulsivity is defined as a tendency to act quickly without considering the consequences (Coutlee et al., 2014). This sub-section will examine research that has explored the influence of this feature on users' susceptibility to online threats and their security behaviours.

Li et al. (2020) conducted an experimental study to examine individuals' vulnerability to phishing attacks, focusing on the influence of several behavioural and demographic characteristics. The three weeks study involved 6,938 faculty and staff members, aged 27 to 41 years, at a large university in the USA. The findings showed that higher impulsivity was correlated significantly with an increased likelihood of clicking on phishing emails, highlighting the susceptibility of impulsive individuals to cyber threats. This result agrees Egelman and Peer's (2015a) finding that impulsivity is inversely correlated with good security practices.

Hadlington (2017) examined the relationship between impulsivity and risky cybersecurity behaviours, with 515 participants in the UK aged 18–84 years. The study employed a standardised impulsivity scale, the Abbreviated Impulsiveness Scale (ABIS). Hadlington developed two other scales for the purpose of the study: the Risky Cybersecurity Behaviour Scale (RScB), which adapted and improved the SeBIS scale to measure security behaviours in a business context, and the Attitude toward Cybersecurity and Cyber Crime in Business (ATC-IB) scale, developed using input from security experts. The results revealed that the ABIS subscales were significant predictors of risky behaviours. Additionally, positive security attitudes were predictors of security behaviours. These findings were consistent with previous research, suggesting that individuals with high levels of impulsiveness tend to act without considering the consequences and potential costs of their actions.

Whitty et al. (2015) also investigated impulsivity in the context of password decision-making. Impulsivity was assessed using the UPPS-R Impulsivity Scale, a 45-item and includes four subscales: lack of premeditation, urgency, sensation seeking and lack of perseverance. The sample comprised 497 participants from the UK, with an average age of 41.86 years. Those who scored highly on the Lack of Perseverance were more likely to share their passwords.

2.8.3 Consideration of Future Consequences as Predictors of Susceptibility to Online Threats

An early example of research on measuring the extent to which people are concerned about the potential results of their current behaviours was conducted by Strathman et al. (1994), who developed the Consideration of Future Consequences scale (CFC), which measured the extent to which individuals consider the potential future outcomes of their current behaviours. They developed a scale of 24 items and validated it among many samples from US universities. Then they produced a subset of 12 items based on reliability assessment and factor loading. They conducted a series of tests to demonstrate the effects of CFC on information processing.

The CFC scale has also been validated in other studies and in different contexts (e.g. Ainin et al., 2015; Joireman et al., 2012; She et al., 2021). Joireman et al. (2012) revised the CFC scale and created two factors. In their version, they grouped 14 items into 2 subscales: 7 items for the immediate consequences sub-scale, which measures the tendency to prioritise short term result and focus on immediate consequences of actions, and 7 items for the future consequences subscale, which measure the extent to which individuals consider long term consequences of their actions. Responses were given on a 7-point items (1 = very uncharacteristic of me and 7 = very characteristic of me). This new version was used by Egelman and Peer (2015b) to identify the correlation between CFC and the four sub-scales of SeBiS. Although they described the CFC as a one-dimensional measure, they referenced the updated two subscales version of the CFC scale. Egelman and Peer's analysis of the CFC as a single factor may therefore have overlooked the more complex ways in which individuals balance short-term and long-term considerations in their decision-making that are measured by the CFC.

2.8.4 Unrealistic Optimism as Predictor of Susceptibility to Online Threats

People's perception of risk is frequently inaccurate, either due to a lack of knowledge needed to assess risks properly or a tendency to downplay potential consequences (H.-S. Rhee et al., 2005). People therefore often believe they are less vulnerable to negative outcomes than others. This tendency to underestimate the likelihood of experiencing negative consequences is referred to as unrealistic optimism, or the optimistic bias.

Rhee et al. (2005) discussed this bias in relation to information security. They noted that optimistic bias is typically measured by comparing how likely people think something is to happen to them versus to others, since actual future probabilities are often unavailable in this area and hard to express numerically. Their study measured optimistic bias by examining two key factors that have been found to influence it: perceived controllability and the comparison target. There are two techniques for assessing how people compare their chances of experiencing an event to someone else's. In direct comparison, a person provides a single estimate of how probable they believe it is they will experience an event compared to someone else. In indirect comparison, a person provides two separate estimates: one for how likely they believe they are to encounter the event and another for how likely they believe someone else will experience the same event in the future.

Rhee et al. (2005) used indirect comparison with 248 students with American graduate students, mean age of 28.93 years. The participants rated their perceptions of risk related to their own information systems and their controllability. The same questions were asked again to evaluate the participants' perceptions of their friends' systems and those of an average person. Participants perceived their own level of risk to be significantly lower compared to that of their friends and the average person. In terms of perceived controllability, they believed they had significantly more control over protecting their information. The findings indicated that users' optimistic perceptions of their information security reflected two aspects, defensive and functional optimism. Defensive optimism refers to a form of naïve optimism whereby individuals believe negative events, such as security breaches, are unlikely to happen to them. Functional optimism refers to the perception of one's capability and control of personal resources necessary to take proactive measures for self-protection.

Hewitt and White (2021) adapted existing scales to measure cyber optimistic bias (COB) in cybersecurity, perceived vulnerability (PV) and technical optimism and examined the effect of security education and training on optimistic bias among college students in the USA. Security education and training influenced individuals' PV, technical optimism, COB and the number of security incidents they experienced. Specifically, individuals with more security education tended to feel less vulnerable to security breaches and perceived themselves as less likely to experience such incidents than their peers. In addition, individuals who perceive themselves as more likely to become cyber-victims tend to report a higher number of security incidents and are more likely to visit untrusted websites. Interestingly, time spent on the computer was not associated with security incidents, and prior computer or security education did not appear to influence levels of cyber optimism.

2.8.5 Demographic Factors and Online Security Behaviours

This sub-section explores the relationship between a range of demographic factors (age, gender, education and security knowledge, previous experience, culture) and online security behaviours.

Age and gender

Age has been examined as a factor affecting security behaviours, but the results have been inconsistent. Some studies indicate that younger individuals may engage in riskier online behaviours due to higher impulsivity, whereas older individuals may encounter difficulties with security measures due to a lack of technological knowledge.

Debb et al. (2020) studied generational differences in cybersecurity behaviours, examining the cybersecurity attitudes and behaviours of American university students from so-called Generation Y (those born in 1977–1994) and Z (those born in 1995 and later. They employed a subscale of the Online Security Behaviours and Beliefs Questionnaire (OSBBQ) to measure the cybersecurity behaviours of the participants. In this sample, the younger adults from Generation Z showed less compliance with well-known best practices. This was especially noticeable when examining privacy policy, identifying unusual computer performance and being aware of automatic antivirus and malware notifications. The findings indicated that individuals from Generation Y in this self-reported sample engaged in safer information security procedures than their Generation Z counterparts. A criticism of this study is that the age differences between so-called Generation Y and Z are not that great, and the “generational” differences may be more of a populist myth than scientific reality.

A study comparing the use of multi-factor authentication among Swedish users of different age groups (Kävrestad et al., 2024) highlighted the impact of age on cybersecurity behaviours. The study categorised participants as young digital natives (aged 18-27), older digital native (28-43) and digital immigrants (aged above 43). The results indicated that although users from all age groups were willing to use multi-factor authentication when required, younger users were more likely to use it willingly without external encouragement.

Some studies have found that younger participants exhibit poor security behaviours compared to older counterparts. For example, Whitty et al. (2015) studied the risky behaviours of sharing passwords among participants aged 18-72 from the UK. They found that younger adults engaged in riskier behaviours, such as password sharing, more often than older adults. In Gratian et al.'s (2018) study, younger participants (aged 18–25 years) created weak passwords and had weak updating behaviour intention and proactive awareness compared to older participants. Also, Algarni et al. (2017) found that younger participants were significantly more susceptible to social engineering attacks through Facebook.

In contrast, some studies have found that older adults are more susceptible to online attacks. For example, Lin et al. (2019) found that older participants (58 and older) were more susceptible to spear phishing attacks than the younger group. Other studies have found that age does not significantly affect individuals' online behaviours or susceptibility to attacks. In terms of phishing attacks, Greitzer et al. (2021) found that age was not significant or had a limited effect on participants' susceptibility to simulated phishing attacks. This was also concluded by a study investigating people's susceptibility to social engineering attacks in Saudi Arabia (Aljeaid et al., 2020).

Sarno et al. (2023) highlighted inconsistencies in findings regarding the effects of age, personality traits, impulsivity and experience on phishing susceptibility. Their study found that younger, impulsive and extroverted individuals, particularly those who made quick decisions and scored lower for openness and agreeableness, were more likely to fall for phishing attacks.

Gender

Inconsistent findings have been reported regarding the impact of gender on online security behaviours and susceptibility to threats. Halevi et al. (2016) found men were more confident than women in dealing with security attacks. Moreover, in Cain et al.'s (2018) study, males were found to know more about cyber hygiene than females, but they did not have better cyber hygiene behaviours. In contrast, Fatokun et al. (2019) found that age and gender were stronger predictors of security behaviours than educational background.

Some studies have explored how gender influences susceptibility to various types of online attacks. Algarni et al. (2017) found that women were significantly more vulnerable to social engineering attacks than men.

Education and Security Knowledge

Algarni et al. (2017) found that participants with more security knowledge were less vulnerable to online attacks. Their study focused on employees from three organisations in Saudi Arabia, with participants ranging in age from 18 to over 45. However, Sawaya et al. (2017) found that self-confidence in security knowledge influenced security behaviours more than actual knowledge. Their

study involved participants from seven countries: China, France, Japan, Korea, Russia, the United Arab Emirates (UAE), and the United States (US), with average participant ages ranging between 36 and 43.

Online Security Experience

Online security experience has been defined in various ways in cybersecurity research, including the time spent on a computer, the level of cybersecurity knowledge, self-reported expertise and direct encounters with cyber threats. These differing definitions have resulted in inconsistencies when assessing the impact of experience on security behaviour (Sarno et al., 2023).

Online security experience has been found to enhance an individual's informal security awareness. Such experience is frequently obtained from a variety of sources. These could include stories recounted by family and friends, media coverage of security incidents, or actual experiences of cyber threats. Informal knowledge can influence how people perceive and respond to future security threats (Alohali et al., 2017). However, in a study examining the relationship between various factors and phishing susceptibility, Greitzer et al. (2021) found that previous phishing experiences may not result in increased awareness or better security behaviour in facing phishing attacks but rather increase the likelihood of being deceived again in the future.

A number of studies have been conducted to understand the differences between experts' and non-experts' behaviours in the face of attacks. Wash (2020) studied how experts detect phishing emails. In interviews with 21 IT experts, it was found that the IT experts followed a three-step method. In the first step, they read the email and found inconsistencies. As more inconsistencies were discovered, they suspected phishing and went to the second level, conducting additional research by reviewing technical details. Finally, in the third stage, if phishing were proven, they took action, usually by deleting or reporting the email.

Culture

Many studies have argued that culture affects people’s security behaviours. A study by Harbach et al. (2016) examined cultural differences in smartphone locking behaviours among more than 8,000 participants from 8 countries (Australia, Canada, Germany, Italy, Japan, the Netherlands, the UK and the US). They conducted an online survey of Android users. There were significant differences in locking behaviours across countries. Italy had the lowest use of secure locking, while the UK had the highest. The motivations for locking devices also varied across countries. Japanese and Italian participants reported preventing unwanted access to calls and apps as the main reason for locking, while German participants reported the importance of protection in general. Across all countries, inconvenience was the main reason for not locking screens. Even though this study did not examine the causes of these differences between the countries, the authors argued that differences in the cultures and history of the various countries lead to different motivations.

Another study by Sawaya et al. (2017) found that cultural norms and perceptions of risk shape security behaviours, based on a study of 3,500 participants from 7 countries using the SeBIS. The researchers translated and validated the SeBIS in multiple languages and used nationality rather than Hofstede’s dimensions to define culture as the independent variable. Japanese participants demonstrated the least secure behaviours, while French, Emirati and American participants showed stronger practices.

A systematic review by Vashistha et al. (2018) also emphasised the importance of cultural norms in shaping attitudes towards security and privacy. Hofstede's cultural values, such as collectivist versus individualist orientations, social constructions of gender, trust and religion, were found to shape preferences for security and privacy. For instance, in collectivist cultures, decisions regarding security and privacy may be more influenced by community norms than individual preferences.

In a study by Aleroud et al. (2020), a notable finding was that trust significantly predicted susceptibility to spear phishing in non-English-speaking countries. This indicates that incorporating social context in phishing messages enhances trust and increases the likelihood of a successful attack.

Shah et al. (2023) undertook a study comparing cybersecurity awareness and practices between the US and the UAE using Hofstede's cultural dimensions theory. The authors found that the UAE participants exhibited lower cybersecurity awareness than their US counterparts, particularly in terms of password management, online banking security and phishing awareness. They attributed these differences to cultural traits such as high power distance and collectivism in the UAE, which they claimed led to less individual responsibility for cybersecurity.

However, the study's reliance on Hofstede's framework raises concerns. This model, based on 1970s IBM employee data, assumes that national cultures are static and homogeneous, ignoring regional and socioeconomic variations (Baskerville, 2003). Additionally, there is a Western-centric bias, implying that individualism is superior, which may not reflect real-world cybersecurity outcomes. For instance, despite its high power distance, the UAE has a strong cybersecurity infrastructure that contrasts with the expectations of the framework. The study overlooks other factors, such as cybersecurity initiatives and stricter regulations in the UAE, which could explain the lower reported experiences of cybercrime. Furthermore, countries like the US and the UK may achieve strong cybersecurity not only due to cultural traits but also because of their long history of investment in advancing their cybersecurity compared to other countries.

In contrast to previous works, some researchers have suggested that culture might not significantly influence security behaviours. For instance, Chetty et al., (2015) found that users from diverse cultural backgrounds, such as the USA, South Africa and India, all express more interest in understanding their Internet usage rather than focusing solely on their online privacy. This finding was unexpected for the researchers. It suggests that preferences regarding security and privacy could be influenced by contextual factors that extend beyond culture.

Table 2.3 provides a summary of findings of studies examining the relationship between individual factors and online threat susceptibility.

Table 2.3: Relationship between individual characteristics and susceptibility to online threats

Factor	Studies showing a relationship with vulnerability	Studies showing no relationship/conflicting results
Gender	Females created weaker passwords, had less proactive awareness and weaker updating behaviour (Gratian et al., 2018) Male students had higher scores in security self-efficacy and computer knowledge than female students (Fatokun et al., 2019) Chinese male students had higher scores for self-efficacy and situational support than females (more confident and supported in handling security-related tasks) (Hong & Furnell, 2021)	No significant gender differences were found in relation to cyber security behaviours (Albladi & Weir, 2018)
Age	Respondents aged 18–25 years created weaker passwords and reported weaker proactive awareness intention (Gratian et al., 2018) Older adults (>60) are more vulnerable to online attacks (Lin et al., 2019a) Digital immigrants (aged above 43) showed better password practices than digital natives (18–43) (Kävrestad et al., 2024)	No significant age differences were found in cybersecurity behaviour (Greitzer et al., 2021)
Education	Security education increases the ability to recognise online threats (White et al., 2017)	Security self-confidence is more important than actual knowledge (Sawaya et al., 2017)
Previous Experience	Technical background and negative experiences correlated with adopting security practices (Honolulu & Chi, 2020).	Those previously phished are more likely to fall victim again (Li et al., 2020)
Culture	Cultural values and norms affect cybersecurity behaviours (Vashistha et al., 2018)	Cultures may not affect security behaviours (Chetty et al., 2015)
Risk-taking/ Perception	Ethical and social risk-taking predict the strength of password generation (Egelman & Peer, 2015b)	No correlation was found between risk-taking preferences and password generation intention (Gratian et al., 2018)

Table 2.3 summarises the factors examined in prior research in relation to online threat susceptibility. As shown, findings across these studies are mixed and often context-dependent, with no consistent evidence that demographic or individual characteristics operate uniformly across

populations. As discussed in Chapter 1 (Section 1.3), the UK and KSA differ in their cultural and technological contexts including sharing high levels of digital connectivity among younger adults. In the present thesis, these factors were therefore not treated as explanatory variables to be tested directly. Instead, basic demographic information (such as age, education, and self-reported security knowledge) was collected to describe the British and Saudi samples, while other factors, including risk-taking, online security behavioural intentions and unrealistic optimism, were explored.

Rather than focusing on testing particular demographic predictors, this thesis adopts an experience-focused approach, examining how younger adults in each context recognise, detect, and respond to online threats. In this way, the literature summarised in Table 2.3 informed the scope and boundaries of the study by highlighting the limitations of relying solely on individual characteristics, thereby motivating the comparative and scenario-based design of the empirical chapters that follow.

2.9 Limitations and Gaps in the Literature

While previous research has explored cybersecurity behaviours and awareness, much of it relies on self-reported data through general surveys, which may not reflect the full real-life contexts in which threats occur. While young adults have been the focus of some studies, particularly in Western countries, research exploring online security experiences in Saudi Arabia remains limited. Furthermore, few studies have made direct comparisons between young adults in different national settings, particularly using methods that allow for in-depth reporting of threat experiences. Existing research often emphasises users' intentions or general awareness, rather than how they actually recognise and respond to threats in their daily digital interactions. To address these gaps, the present research employs a mixed-method approach using realistic, scenario-based surveys and diary studies, enabling young adults in both the UK and Saudi Arabia to report and reflect on their real encounters with online threats. This approach offers a more grounded understanding of user behaviour and threat perception than studies relying solely on hypothetical or retrospective accounts.

Chapter 3 Experiences and Concerns of Online Threats among Younger Adults in the United Kingdom

3.1 Introduction

The rapid growth of digital technology and social media platforms has significantly changed the way younger adults interact with the online world. As they increasingly engage with digital environments, they are also becoming more vulnerable to various online threats such as phishing, cyberbullying, identity theft, and other forms of cyberattacks. Despite growing awareness of these online threats and attacks, there remains a critical gap in understanding how younger adults perceive and respond to these threats.

This chapter presents the first study I conducted to explore the experiences of younger British adults regarding online threats. The study's main aim was to investigate the types and frequency of online threats encountered by younger adults in the UK and how their experience of different online threats is associated with their level of worry about these threats.

This study builds on the overall research Objectives 1–3 outlined in Chapter 1. It focuses on understanding the types and frequency of online threats encountered by younger adults in the UK, how they detect and respond to such threats, and how their level of worry and security behaviour relate to these experiences. The following are study 1-specific research questions:

RQ1: What are the types and frequency of online threats encountered by younger adults in the UK?

RQ2: How do younger UK adults detect and respond to online threats?

RQ3: What are the levels of worry about online threats among younger adults in the UK, and how are these levels related to their experiences of such threats?

RQ4: What are the online security behaviour intention scores of younger adults in the UK, and how are these scores related to their experience of online threats, computer and security knowledge?

Table 3.1: Mapping of thesis objectives to Study 1 research questions.

Thesis objectives	**Study 1 (UK Survey)**
Obj. 1: Identify online threats: types and frequency	RQ1
Obj. 2: Examine how younger adults detect and respond to online threats	RQ2 and RQ3
Obj. 3: Investigate the effect of individual characteristics on online security experiences	RQ4

3.2 Method

3.2.1 Design

To investigate younger UK adults' experiences of online threats and attacks, a survey was conducted to collect both qualitative and quantitative data. As it was conducted during COVID-19, it was an online survey.

The study focused on younger adults aged 18–30 years in the UK. While the overall research (see section 1.3) targeted younger adults aged 40 or below, this narrower range was selected for the survey study in the current research to align with previous cybersecurity studies that examined the online behaviours of "Generation Z" users (e.g. Debb et al., 2020). Individuals in this group are often described as "digital natives" (Prensky, 2001a, 2001b) who have grown up with technology, actively use multiple digital platforms for social and professional purposes, and are therefore more likely to encounter cybersecurity threats in everyday life. Focusing on this age range provided a relevant and theoretically consistent sample for exploring cybersecurity concerns and risky online behaviours among highly connected users.

However, despite their familiarity with digital technology, younger adults may lack the experience and knowledge necessary to deal with complex and innovative online threats (Ofcom, 2023). They may engage in risky online behaviours, such as sharing passwords, clicking on suspicious links, or downloading apps from untrusted sources, which makes them potential targets for cybercriminals (Algarni et al., 2017; Whitty et al., 2015). Additionally, younger adults may overestimate their level of online security because they think they are knowledgeable in terms of technology and online security, which makes them even more vulnerable. This optimistic bias observed among young adults in previous research leads to a false sense of security (Rhee et al., 2005).

In making a choice of a data collection method, simply asking individuals whether they have encountered threats and to describe them may not result in detailed or accurate responses. People may have difficulty recalling such incidents or providing detailed information. For this study, scenarios were used as part of the survey. Scenarios are often used in human-computer interaction, though most typically they are used by designers and developers as an aid in guiding the development of an interactive system (Shneiderman & Plaisant, 2016) or to situate tasks for participants in usability evaluations (Dumas & Redish, 1999). However, they can also be used in surveys to provide information to participants and have been used in relation to eliciting information about phishing experiences (Rocha Flores et al., 2014). Using realistic scenarios which describe different types of threats may prompt participants' memory, engagement and understanding. Additionally, presenting realistic scenarios depicting the problems or consequences commonly associated with different online threats can help participants relate to the scenario and recall similar incidents. This approach enhances the accuracy of responses and leads to a better understanding of individuals' experiences with online threats.

A further consideration in developing the study is that online threats are not delivered from one source. Attackers use all possible transmission media to reach their victims. Attackers may launch attacks via emails, text messages, social media platforms, or phone calls. So, it was important to ask about different possible sources of threats. Finally, cyberattacks target all types of digital devices, so the study also asked about the device types on which participants received threats.

Therefore, a set of 12 realistic scenarios was presented to participants, covering different types of threats from different sources (see Table 3.3). The term "realistic" refers to the fact that the scenarios were developed to reflect real, everyday online situations that younger adults are likely to encounter. The scenarios were created through an iterative process informed by the literature on online threats (Pfleeger et al., 2015; Steinberg, 2019) and recent cybersecurity reports. Each scenario described a situation involving common threats such as phishing, malware, or spoofed websites, and was written from a first-person perspective to enhance relevance and relatability.

Further details about the scenario development process are provided in Section 3.2.3. This design ensured that the scenarios captured real-world examples of online threats faced by individual users.

Participants were asked if they had encountered a situation like this scenario (not necessarily exactly this scenario), and if they had, they were asked a short series of questions to learn more about their experience with this type of scenario. They were also asked to rate their level of worry about nine online threats. These threats were similar to those presented in the scenarios. This data enabled me to understand the relationship between participants' experience of online threats and their level of worry about these threats.

Participants also completed a previously developed measure of online security behaviour, the Security Behaviour Intentions Scale (SeBIS) (Egelman & Peer, 2015b) which is used to measure security behaviours. This scale was selected as it is a well-known scale that has been validated and used to assess security behaviour intention across different cultures (see section 2.6). This data enabled me to understand the relationship between participants' experience of online threats and their self-reported overall security behaviour.

3.2.2 Participants

The inclusion criteria for the study were being a self-identified British individual residing in the United Kingdom and aged between 18 and 30. 84 participants were recruited through the Prolific recruitment website, but 3 failed attention check questions (see Appendix A: Attention Check Questions (AC) and Analysis), leaving 81 participants for analysis. The demographic characteristics of the participants are summarised in Table 3.2. The participants were equally divided between men and women and showed a wide range of educational levels

Participants rated their general computer knowledge, online security knowledge, and confidence in identifying cybercriminal attacks using 7-point Likert items, ranging from 1 (not at all knowledgeable/confident) to 7 (very knowledgeable/confident). Wilcoxon one-sample signed-rank tests were conducted, Z-scores could be used as the sample size exceeded 25 (Howell, 2013). Participants rated themselves significantly above the midpoint of the rating scale for all three ratings.

Table 3.2: Demographic characteristics of the participants in Study 1.

Age	
Range	18–30 years
Mean	24.0
Gender	
Female	40 (49 %)
Male	41 (51 %)
Highest educational level (N, %)	
High school	28 (35 %)
Bachelor's degree	34 (42 %)
Postgraduate degree	15 (19 %)
Professional qualification	3 (4 %)
Prefer not to say	1 (1 %)
Self-rating of general computer knowledge	
Median (Semi Interquartile range)	5.0 (0.5)
Z score (probability)	6.25, $p < 0.001$
Self-rating of online security knowledge	
Median (Semi Interquartile range)	5.0 (1.0)
Z score, probability	4.90, $p < 0.001$
Self-rating of ability to identify an attack from a cybercriminal	
Median (Semi Interquartile range)	5.00 (1.0)
Z score, probability	5.57, $p < 0.001$

3.2.3 Materials

The development of the scenarios was an iterative process with several rounds of revision. To develop an appropriate set of online threats to include in the scenarios. I reviewed the literature (Section 2.2) and in particular two sources (Pfleeger et al., 2015; Steinberg, 2019) which discuss various types of online threats and how users comprehend these threats (see Table 2.1). Then several brainstorming sessions were held with my supervisors to discuss the range of threats to include in the scenarios. These discussions resulted in a set of online threats, described in their technical terms and examples illustrating how users may encounter these threats.

Table 3.3 summarises the initial set of online threats that emerged from this process and were selected to be investigated in this study. The selection criteria were: (1) the threat targets individual users rather than organisations, and (2) the threat is current and has been identified in recent reports published by cybersecurity companies.

This approach allowed me to identify a range of online threat types and instances, their possible sources and consequences, forming the basis for creating the scenarios.

Table 3.3: Initial set of online threats.

Threat type/ Specific instances	How users encounter the online threat	Possible threat sources	Possible consequences
Malware			
Malware through a link (Trojan Horse or virus)	The users receive a link or file through email or from an unfamiliar website. Believing the content to be legitimate or harmless, they click the link or download the attachment.	Downloading an email attachment, or clicking on a link in email, SMS, or social media	Poor device performance: e.g. user's computer running slowly or crashing more frequently than normal. Strange device behaviour: e.g. programs running the user did not initiate or other unexplained processes being executed on the user's device. Pop-up and spam interruptions.
Malware (Ransomware)	The users receive a deceptive email, message, or pop-up that contains a malicious attachment or link. Believing it to be trustworthy, such as a job offer, invoice, or system alert, the user clicks the link or opens the file	Downloading files or apps from email, website or social media	Users are unable to access all or some of their files stored on their device.
Malware (Scareware)	A message appeared to the user stating that the device is infected with some virus and only a particular antivirus product can remove it, with a link to purchase that product. Or a message from IT support requesting immediate action to download software that helps to fix some problems or remove a virus.	Clicking on ad pop-ups or suspicious links on a website or social media	Users notice many fake pop-ups and notifications appearing frequently on screens. Poor device performance: such as the device slowing down and crashing frequently.
Malware (Adware)	The user finds free software, a mobile app, or a browser extension from an unofficial or untrusted source.	Downloading a free app from an untrusted source or software from the Internet	Users notice changes in the web browser home page. Numerous pop-up ads. Poor device performance. Apps downloading without users' permission.
Malware (worms)	The users receive an infected file via email, USB drive, or download it from a	Infected files or links delivered via email, USB devices, or downloads	Pop-up windows frequently appeared. The homepage was changed

Threat type/ Specific instances	How users encounter the online threat	Possible threat sources	Possible consequences
	compromised website.	from compromised websites	Mass emails were sent from the user's email. Slow computer performance. Unknown programs start up when the computer turns on.
Malware (viruses in mobile devices)	The user encounters a seemingly legitimate app from an untrusted source, a deceptive pop-up, or receives a link via SMS or messaging app	SMS links, pop-ups, third-party app stores, mobile phishing messages	Pop-ups frequently appeared. Unrecognised apps were installed Spam texts were sent to my contacts. Increased battery drains The phone overheated and apps repeatedly crashed.
Phishing			
Phishing	Receiving messages through email, social media apps, or phone calls that ask about some personal information, such as the user's account number, or ask to click on a link to reset password due to a possible data breach.	Phone call, SMS, email or message on social media	The user's information has been used by attackers to make illegal purchases or to commit fraudulent acts.
Spear phishing	Users receive personalised messages sent via SMS, social media or email. For example, a personalised message seems to be from a boss, friend, or trusted parties such as banks who has an urgent request.	SMS, email or message on social media	Users respond to the request (e.g. transferred money). Malicious code downloaded onto users' devices.
Suspicious Website			
Spoofed websites	Searching for an online service then users found a website for this service, but something about it didn't seem right. the interface seemed outdated, or the grammar was incorrect.	A website that may appear first in a search	Enter personal information, such as usernames and passwords. Malicious codes are installed on the user's device.

From this range of threats, 12 scenarios were created, incorporating the threats into concrete situations which participants in the study could easily relate to. Each scenario was written from a first-person perspective and incorporated a situation in which the threat might be encountered, a threat source (or range of sources) and some possible consequences of the threat. Then the scenarios were discussed with my supervisors and refined to create the final set of scenarios, which are presented in Table 3.4.

It was important to ask questions using wording which would be understandable to all participants, regardless of their knowledge about online security issues, so in the scenarios, I avoided technical terms from cyber security such as ransomware, trojan horse, or phishing attack.

To properly represent the 12 scenarios, they were grouped into specific categories based on the nature of the threats presented, as shown in Table 3.4.

All scenarios were grouped under three main categories:

1. Malware-related scenarios, which are Scenarios 1,2,3,4,7 and 8.
2. Identity and Data theft-related scenarios, which are Scenarios 5,6 and 12.
3. Phishing and Spear phishing-related scenarios, which are Scenarios 9, 10 and 11.

In the scenarios, S1 and S8 appear similar in content, but they differ in terms of the consequences described and the type of device being targeted. S1 focuses on general device performance issues, such as freezing, slow operation, or repeated crashes, which are broad consequences typically associated with desktops or laptops. In contrast, S8 was designed to reflect mobile-specific malware, including consequences like the installation of apps without user permission.

Table 3.4: The 12 scenarios used in Study 1, with codes, short names and categories.

Code	Scenario	Category
S1	I click on a link (e.g. on a website, in social media, in a SMS) and then notice my device acting strangely (e.g. the device freezes, runs slowly or crashes repeatedly). I realise this may have been caused by clicking on the link. Short name: Malware through link	Malware
S2	I download an attachment (e.g. from an email or website) and then notice my device acting strangely (e.g. device freezes, runs slowly or crashes repeatedly). I realise this may have been caused by downloading the attachment. Short name: Malware through attachment	Malware
S3	I download a free app or game from an unknown or possibly untrustworthy source. Then I notice my device is running slowly or crashing more frequently than normal. Short name: Malware free app	Malware

Code	Scenario	Category
S4	I install some software or a file on my device from a link or attachment I received in an email, then notice the device acting strangely. I can't access some or all of my files and then I am asked to pay a ransom to be able to retrieve these files. I realise this may have been caused by installing that software/file. Short name: Malware ransomware	Malware
S5	I realise that someone has made a purchase using my credit card or bank account details. I remember that I have recently entered these details online and they may have been stolen. Short name: Theft bank details	Data and Identity Theft
S6	I realise that someone has used my personal information or something I have stored online (e.g. your name, a photo). I remember that I have stored that online and they may have been stolen. Short name: Theft personal information	Data and Identity Theft
S7	I download some anti-virus/malware software to try to protect my device. But it does not seem to be effective and it keeps showing me advertisements on the device. Short name: Malware adware	Malware
S8*	I click on a link (e.g. on a website, in social media, in an SMS) and then notice strange things happening on my device (e.g. pop-ups appearing frequently, unrecognised apps being installed). I realise this may have been caused by clicking on the link. Short name: Malware phone	Malware
S9	My friends report receiving strange messages from me (e.g. requesting money because I'm in trouble, including suspicious links). I realise someone must have illegally used one of my accounts. Short name: Spear Phishing, impersonating participant	Phishing and Spear Phishing
S10	I receive a message or call from what seems to be a trustworthy source (e.g. via email, social media, SMS or phone call) asking me for personal information (e.g. account details, password) for a legitimate reason (e.g. updating data). At some point, I realise this is a fake message or call. Short name: Phishing msg/call, from a trusted party	Phishing and Spear Phishing
S11	I receive a message or call which seems to be from someone I know (e.g. via email, social media, SMS) asking me to give them urgent assistance (e.g. transfer money). At some point, I realise this is a fake message. Short name: Spear Phishing msg/call, impersonating someone	Phishing and Spear Phishing

Code	Scenario	Category
S12	I need to undertake an urgent task on the government website (e.g. renewing my passport or driving licence). I search quickly for the website in Google. The website asks for personal information (e.g. my name, date of birth or credit card details). After entering my personal information and making a payment, I realise it was not the actual government website, but a fraudulent one with a very similar address and information. Short name: Theft personal information, spoofed website	Data and Identity Theft

* S8 focuses specifically on malware consequences of mobile devices, such as frequent pop-ups and the installation of unrecognised apps.

Finally, the scenarios were analysed using two well-known security threat lifecycle frameworks: the Cyber Kill Chain by Lockheed Martin (2014) and the MITRE ATT&CK framework (2022) (see 2.3.1 and 2.3.2). This analysis is summarised in Table 3.5. Both frameworks were chosen because they provide a comprehensive and structured way to understand the attack from an overall point of view, including the attacker's point of view. By using these two frameworks, I was better able to understand the steps involved in each threat and ensure that the scenarios reflected real-world possible threat tactics and techniques.

I used the Intrusion Kill Chain framework to focus on two key phases, delivery and exploitation, as these are critical points when users can detect and prevent threats. The delivery phase describes how attackers deliver malicious content, such as through an email with suspicious links or attachments, deceptive websites, or untrustworthy software. The exploitation phase describes user interactions with these threats, such as clicking on links, downloading attachments, or installing software, which can lead to consequences such as unusual device behaviour, difficulty accessing files, or unauthorised financial transactions.

The MITRE ATT&CK Tactics and Techniques framework components were used to identify the methods attackers use at different stages in their cyberattacks. This systematic approach helped to map each scenario to tactics (the "why") and techniques (the "how"), outlined in the framework, ensuring that scenarios align with realistic threats' behaviours. For example, I analysed each scenario to determine how attackers might gain access to users (e.g. phishing), what techniques they might employ to exploit the users' systems (e.g. malware installation), and what consequences or goals they might achieve (e.g. data theft). For a full list of tactics and techniques, see the MITRE ATT&CK Enterprise Matrix (MITRE ATT&CK, 2024).

Table 3.5: Cyber Kill Chain and MITRE ATT&CK analysis of the 12 scenarios.

Scenario: Short name	Cyber Kill Chain analysis	MITRE ATT&CK analysis
S1: Malware through link	**Delivery:** Phishing (website, social media, SMS) **Exploitation:** Malware	**Tactics:** **TA03: Initial Access** Techniques: Phishing **TA04: Execution** Techniques: User execution: Sub-technique: Malicious link
S2: Malware through	**Delivery:** Phishing (email,	**Tactics:**

Scenario: Short name	Cyber Kill Chain analysis	MITRE ATT&CK analysis
attachment	website) **Exploitation**: malware	**TA03**: **Initial access** Technique: Phishing **TA04**: **Execution** Technique: User execution Sub technique: Malicious file
S3: Malware-free app	**Delivery**: Malicious Code (in free app or game) **Exploitation:** Malware	**Tactics:** **TA03: initial access** **Techniques:** Drive-by compromise
S4: Malware ransomware	**Delivery:** Phishing (attachment in email, website) **Exploitation:** Ransomware	**Tactics:** **TA04: Execution** Techniques: User execution Sub technique: malicious file **TA06: Impact** Technique: Data encrypted for impact
S5: Theft Bank Details	**Delivery:** Unknown **Exploitation:** Data Theft, Identity Theft	**Tactics**: **TA02: Resource development** Technique: Compromise Accounts (getting access to one person's account)
S6: Theft Personal Information	**Delivery:** Unknown **Exploitation:** Data Theft, Identity Theft	**Tactics**: **TA02: Resource development** Technique: Compromise Accounts (getting access to one person's account)
S7: Malware adware	**Delivery:** Malicious Code (free app) **Exploitation**: Malware (Adware)	**Tactics**: **TA02: Resource Development** Techniques: Obtain capabilities: Tools (i.e., acquiring a legitimate anti-virus and modifying it) **TA04: Execution** Technique: user execution Sub technique: malicious file
S8: Malware Phone	**Delivery**: Phishing (link on website, social media, SMS) **Exploitation**: Malware	**Tactics**: **TA03: Initial access** Technique: Phishing
S9: Spear Phish Impersonating Participant	**Delivery**: Spear Phishing (Social media messaging systems, email) **Exploitation**: credential theft	**Tactics:** **TA05: Credential Access** Techniques: password guessing, Password cracking, Credential from web browsers
S10: Phish Message/call Trusted Party	**Delivery**: Phishing (email, social media, SMS or phone call)	**Tactics:** **TA01**: **Reconnaissance** Technique: Phishing

Scenario: Short name	Cyber Kill Chain analysis	MITRE ATT&CK analysis
	Exploitation: stolen personal information or financial fraud	Sub techniques: spear phishing voice, spear phishing service **TA02: Resource development** Technique: Establish accounts Sub technique: email accounts
S11: Spear Phish Impersonating a known person	**Delivery**: Identity Theft (of another person), Spear Phishing **Exploitation**: financial fraud	**Tactics:** **TA05: Credential access** Technique: brute force/password guessing
S12: Data theft spoofed website	**Delivery**: Spoofed Website **Exploitation**: Data Theft, Identity Theft	**Tactic:** **TA02: Resource development** Technique: Acquire Infrastructure (e.g. registering a server with a domain close to a real one and advertising the same service to appear in web searches)

3.2.4 Online Questionnaire

An online questionnaire was developed and deployed through Qualtrics survey software. The questionnaire consisted of four parts:

Part 1: the 12 scenarios of online security threats were presented in random order, and participants were asked whether they had experienced anything like the situation in the scenario on a 7-point Likert item (from “never”, scored as 1 to “many times”, scored as 7). If they had never experienced a particular threat, they were directed to the next scenario; otherwise, the following information was elicited:

1. **Device type:** the device on which the threat occurred (multiple choice, one answer possible): options included desktop, laptop, tablet, phone, or cannot remember.
2. **Source of the threat:** where the threat originated (multiple choice, one answer possible): options included website, app, social media, SMS, phone call, email or cannot remember.
3. **Consequences:** participants selected one or more outcomes that reflected what had happened as a result of the incident (multiple choice, multiple answers possible): The list of possible consequences was tailored to the specific scenario, based on the threat type described.
    - For malware-related scenarios (S1–S3, S7–S8), consequences included: screen frozen, device ran slowly, device crashed repeatedly, unknown apps were installed, or frequent pop-ups.
    - For ransomware (S4), consequences included: unable to access some or all files, or paid the requested ransom.
    - For financial or data theft (S5–S6), options included: lost money, identity stolen, credit card could not be used, bank account overdrawn or received blackmail messages.
    - For phishing (S9–S11), consequences included: contacts received fraudulent messages, responded to fake requests, could not access some of their online accounts, sent money to the fraudulent person, personal information used illegally.
    - For spoofed websites (S12), consequences included: lost money, entered personal data or credit card details or malware downloaded.

In all scenarios, participants could also select "other" or "cannot remember" to report unlisted consequences.

4. **Description of the incident:** an open-ended question asked participants to describe the incident (e.g. what happened, how they recognised the problem, and how they resolved it).

The lists of multiple-choice options were developed through a review of the cybersecurity literature and were directly aligned with the specific threat types used in the 12 scenarios (see Table 3.3). The full wording of the questionnaire can be found in Appendix C: Full The full wording of the Scenarios Questionnaire, Study 1, and 2.

Part 2: a set of nine statements to rate on 7-point Likert items (from "not at all worried" scored as 1 to "very worried" scored as 7), to measure the level of worry for various types of security threats (see Table 3.6). These were developed from the threats in the scenarios.

Table 3.6: The nine worry statements used in Study 1.

	Worry statement	**Attack type**	**Relevant scenarios**
1	My device will be accessed by an attacker and my data will be destroyed	Data theft	S4
2	I will receive an email with a link leading to a fake website	Phishing Website spoofing	S1, S8, S12
3	I will receive an email with an attachment that may include malicious code	Phishing Malware	S2
4	Someone will lock me out of my device(s) and demand money to restore access	Ransomware	S4
5	Someone will access my device(s) or account(s), look at my information and use it to blackmail me	Ransomware	S6, S9
6	Someone will steal my online identity and misuse it	Identity theft	S6
7	Someone will access my device(s) or account(s), steal my data and use it for malicious purposes or to their advantage (e.g. make illegal purchases)	Identity theft	S5
8	I will receive a phone call from someone asking about my confidential data (e.g. password, bank account details)	Spear phishing Identity theft	S10
9	I will click on a link in a SMS message or email from a source that I cannot verify its origin, whether it is trustworthy	Phishing	S11, S12

Part 3: SeBIS Scale

The Security Behaviour Intention Scale (SeBIS) (Egelman & Peer, 2015) which measures users' attitudes towards common security practices. It consists of 16 items with four subscales: Device Securement, Password Generation, Proactive Awareness, and Updating.

The SeBIS scale had some items that used somewhat outdated terminology, so more appropriate but equivalent terminology was developed (e.g. "computer/mobile phone" was changed to device to cover the wider range of devices used now). In addition, there were two very similar items ("I use a password/passcode to unlock my laptop or tablet" and "I use a PIN or passcode to unlock my mobile phone"). These were combined into one item: "I use passwords/passcodes to lock my devices".

Statements in the SeBIS scale were rated on 5-point Likert items from “Never” to “Always”. To create a greater variance in responses and be consistent with other questions, the rating scale was changed to 7-point Likert items. The final set of 15 items is presented in Appendix B: Original and modified SeBIS Scale.

Three attention-check question sets (six questions in total) were added to the SeBIS scale, being positive and negative versions of the same statement (see Appendix A). The SeBIS scale was presented to participants with five statements and two attention check questions per screen, making a total of 3 screens. The order of screens was randomised, and the two attention check questions from the same set never appeared on the same screen.

Part 4: asked about demographic information, including age, nationality, country where the participant is currently living, and highest educational background. This part also included items to rate computer knowledge, online security knowledge, and ability to identify online attacks on 7-point Likert items (1= Not at all knowledgeable/confident to 7 = Very knowledgeable/confident).

The full wording of the questionnaire can be found in Appendix C.

3.2.5 Procedure

A pilot study was conducted with two researchers in the HCI Research Group at the University of York. They were asked to check the time required to complete the questionnaire, the clarity of the questions, and any spelling and grammar mistakes. Some small adjustments were made based on their feedback.

Participants were recruited using the Prolific platform (prolific.com), sampling from UK adults aged 18–30. Participants received a brief invitation explaining the purpose of the study and the compensation for participating in this study. If they accepted the invitation, the first screen provided a more detailed explanation of the study, their right to withdraw, and data protection information. A consent screen then asked for explicit consent. Participants received GBP 2.00 for completing the study which took approximately 15 minutes.

The study was approved by the Physical Sciences Ethics Committee at the University of York with the approval code (Aldaraani20211216).

3.2.6 Data Analysis

SPSS statistical software was used to analyse the quantitative data. Data was cleaned by removing incomplete responses or responses for participants who failed to pass the attention check questions.

Rating data frequently failed to meet normality and homogeneity of variance (Shapiro-Wilk tests, Field & Hole, 2002), so non-parametric statistics were used.

For the open-ended question, qualitative content analysis was used (Flick, 2014).

I was interested in understanding the participants’ perceptions of online threats presented in the scenarios, how they recognised the threats and if they followed the best practices to solve the problems associated with threats. So the coding process involved first identifying possible categories for the three steps of dealing with a threat:

1. Identifying threat indicators (cues) that participants used to recognise the threats: This involved carefully examining the texts to extract the signs participants recognised as indicative of an online threat. Examples of categories of threat indicators include device performance, content of messages or emails, or request type.
2. Identifying categories of solutions that participants followed to address the security threats: This involved analysing the actions taken by participants in response to the perceived threats and grouping them into distinct categories based on common themes or approaches. Solutions ranged from installing antivirus software or changing passwords to ignoring suspicious emails or seeking assistance from specialists.
3. Identifying the adequacy of the actions taken by the participants: The adequacy of the solutions was evaluated by identifying the most suitable recommendations from security experts and comparing them with the actions participants took to address the security issues.

Having identified categories for each step in the process of dealing with a threat, I was able to generate a code dictionary for each step. Two coders, my supervisor and I, then independently coded the data using these categories. We assessed intercoder reliability on the solutions, and it ranged from 66.7% to 100%, with an average of 83.2%

3.3 Results

3.3.1 Frequency of Encountering Different Types of Threats

Table 3.7 summarises the frequency with which participants reported encountering the three different types of threat and each of the 12 scenarios. These are the percentage (and number) of participants reporting having encountered this type of threat, and for those who did encounter it, the median rating of the frequency of encountering it.

More than three-quarters of participants (77 %) reported encountering Phishing and Spear Phishing threats, which shows how common these threats are. Malware was also frequently encountered, reported by nearly three-quarters of participants (74 %). Data/Identity Theft was less common, reported by less than one-third of participants (30 %). The differences in the frequency ratings were not as dramatic, Phishing and Spear Phishing had the highest frequency rating (median 4.0), close to the midpoint of the scale, but the other two categories had medians of 3.0, a little lower.

In the Phishing and Spear Phishing category, spear phishing through messages or calls from seemingly trusted sources (S10) was the most encountered type of phishing reported by over half of the participants (56%). For Malware, participants reported similar rates of encountering different types of Malware scenarios (21% to 35%), except for the ransomware scenario (S4), which was substantially lower at 4 %. This may indicate that ransomware attacks are less likely to target individuals in comparison with organisations, from whom attackers can demand large payouts.

When examining the individual scenarios, the median ratings show that S10 had a high median encounter rating of 5.0, showing that phishing from trusted sources is frequently experienced by participants. Similarly, the high median for S6 (Theft personal information) of 5.0 reflects frequent exposure to this threat among affected participants, although only a few participants encountered this type of threat.

Table 3.7: Percentage (number) of participants encountering threats related to each scenario, median rating (SIQR) of frequency of encountering it (from "never" scored as 1 to "many times" scored as 7).

Scenario type/Instance	% (N) Participants encountering[1]	Median rating of frequency (SIQR)[2]
PHISHING AND SPEAR PHISHING	**62 (77 %)**	**4.0 (1.0)**
S9: Spear Phishing, impersonating participant	22 (27 %)	3.0 (1.5)
S10: Phishing msg/call, from a trusted party	45 (56 %)	6.0 (1.75)
S11: Spear Phishing msg/call, impersonating someone	31 (38 %)	3.0 (1.5)
MALWARE	**60 (74 %)**	**3.0 (1.5)**
S1: Malware, link	28 (35 %)	3.0 (1.5)
S2: Malware, attachment	19 (24 %)	2.0 (0.5)
S3: Malware, free app	17 (21 %)	3.0 (1.5)
S4: Malware, ransomware	3 (4 %)	5.0 (n/a)[3]
S7: Malware, adware	20 (25 %)	4.0 (1.0)
S8: Malware, phone	24 (30 %)	4.0 (1.5)
DATA/IDENTITY THEFT	**25 (30 %)**	**3.0 (1.5)**
S5: Theft Bank Details	14 (17 %)	2.5 (1.5)
S6: Theft Personal Information	11 (14 %)	5.0 (1.0)
S12: Theft personal information, spoofed website	2 (3 %)	2.5 (n/a)[3]
ALL SCENARIOS	**77 (95 %)**	**3.5 (1.5)**

1. For Scenario category, the number of participants encountering at least one of the scenarios in the category.
2. For Scenario category, based on all ratings of individual scenarios.
3. SIQR could not be calculated due to the small number of ratings.

The results of the subsequent multiple choice questions answered by participants who encountered particular threats are presented below in Tables 3.8 to 3.15.

3.3.2 Devices where Online Threats are Encountered

The devices on which participants encountered threats are summarised in Table 3.8.

For Phishing and Spear Phishing Scenarios (S9, S10, and S11), device type information was not collected, as it was assumed that, as these scenarios asked about spear phishing messages or calls, they would primarily be encountered on a phone. However, with the increasing prevalence of applications capable of receiving messages across multiple devices, it would have been interesting to ask participants to specify the device type in these scenarios as well.

Malware threats were encountered in 42 % of incidents on desktop machines, considerably more than encountering this type on laptops (24 %) or phones (22 %). Whereas Data/Identity Theft was reported as being encountered on phones (44 %) compared with desktops (19 %) or laptops (15 %).

When examining the device types associated with specific malware types within scenarios, it can be seen that adware (S7) was most commonly reported on desktops, with 70% of participants encountering it on that type.

Interestingly, in S8, which was designed to reflect malware typically encountered on mobile devices, most participants reported encountering this threat on a desktop instead, with none reporting it on a phone.

Phones were the most common device for encountering malware through free apps or games in S3, with 64.7% of participants reporting this. Whereas Data/Identity Theft was reported by more participants as being encountered on phones. For example, in S6, which involved stolen personal details, 54.5% of the participants reported encountering them on phones.

Table 3.8: Device types on which participants encountered online threats.

Scenario type/ Instance	**N***	**Desktop**	**Laptop**	**Tablet**	**Phone**	**Not sure**
Malware	**111**	**47 (42 %)**	**27 (24 %)**	**6 (5 %)**	**24 (22 %)**	**7 (6 %)**
S1	28	7 (25 %)	13 (46 %)	0	8 (29 %)	0
S2	19	6 (32 %)	11 (58 %)	0	2 (11 %)	0
S3	17	1 (6 %)	1 (6 %)	2 (12 %)	11 (65 %)	2 (12 %)
S4	3	3 (100%)	0	0	0	0
S7	20	14 (70 %)	1 (5 %)	0	3 (15 %)	2 (10 %)
S8	24	16 (67 %)	1 (4 %)	4 (17 %)	0	3 (13 %)
Data/ Identity theft	**27**	**5 (19 %)**	**4 (15 %)**	**0**	**12 (44 %)**	**6 (22 %)**
S5	14	3 (21 %)	1 (7 %)	0	5 (36 %)	5 (36 %)
S6	11	2 (18 %)	2 (18 %)	0	6 (55 %)	1 (9 %)
S12	2	0	1 (50 %)	0	1 (50 %)	0

*N in the main threat type rows (e.g. *Malware, Data/Identity Theft*) refers to the total number of reported instances, which may include multiple responses from the same participant. N in the scenario-specific rows (e.g. S1, S2...) refers to the number of unique participants who experienced the threat in that specific scenario.

The finding that malware was most frequently reported on desktop computers suggests that many threats still exploit activities such as downloading files, installing software, or opening email attachments, tasks that are more common on desktops and carry a higher risk of malware execution. In contrast, mobile phones were more often linked to data and identity theft, likely because they are used for social media, messaging, and online payments. One possible explanation is that mobile devices, although widely used, tend to operate within more restricted ecosystems (e.g. app stores or sandboxed environments), which may limit direct malware execution but still expose users to phishing and data theft through social media and messaging applications. Overall, this shows that threat exposure depends largely on how people use each device rather than on the device itself.

3.3.3 Sources of Online Threats

The sources of online threats through which participants encountered threats are summarised in Tables 3.9 to 3.11. For malware scenarios (Table 3.9), websites were the most commonly mentioned source of threat, accounting for 59% of reported instances (65 mentions). In contrast, SMS was the least reported delivery method, with only one mention (1 %). Interestingly, recommendations from friends or family members emerged as a potential source in the adware scenario (S7), where three mentions were identified from open-ended responses. These involved participants encountering adware after downloading software recommended by someone they knew (a source not originally listed in the answer options but revealed during qualitative analysis of participants' responses to the final open-ended question in the scenario).

Table 3.9: Sources of threat for scenarios related to malware.

Source	S1	S2	S3	S4	S7	S8	All Malware
Website	15 (54%)	13 (68)	5 (29)	2 (67)	14 (70)	16 (67)	65 (59)
App	1 (4 %)	2 (11)	8 (47)	0	1 (5)	1 (4)	13 (12)
Social media message	6 (21%)	0	1 (6)	0	0	4 (17)	11 (10)
SMS	1 (4)	0	0	0	0	0	1 (1)
Email[1]	2 (7%)	2 (11)	0	1 (33)	0	0	5 (5)
Human recommendation[1]	0	0	0	0	3 (15.0)	0	3 (2.7)
Not sure/Don't know	3 (11%)	2 (11)	3 (18)	0	2 (10)	3 (13)	13 (12)

1. Option not included in multiple choice but coded from answers to the open-ended question.

For the source of threats in Data/Identity theft (Table 3.10), fewer sources were reported than for malware. The most frequently reported source was again websites, 30% mentions. App and social media messages were the next most frequently reported sources, 19% mentions, in the scenarios related to stolen bank /personal information (S5 and S6).

Table 3.10: Sources of threats for scenarios related to data and ID theft.

Source	S5	S6	S12	All data/ID theft
Website	4 (29%)	3 (27%)	1 (50%)	8 (30%)
App	4 (29%)	1 (9%)	0	5 (19%)
Social media message	0	5 (46%)	0	5 (19%)
SMS	1 (7 %)	0	1 (50 %)	2 (7.4%)
Not sure/Don't know	5 (36%)	2 (18 %)	0	6 (22 %)

For the sources of threats in Phishing and Spear phishing (Table 3.11), social media messages and emails were the most frequently reported sources (32 % and 31 %, respectively). Interestingly, a

phone call was the source of a threat in only one scenario (S10), which was about phishing from what seems to be a trusted party.

Table 3.11: Sources of threats for the scenarios related to phishing and spear phishing.

Source[1]	S9	S10	S11	All Phishing
Email	5 (23 %)	14 (31 %)	11 (36%)	30 (31 %)
Social Media Message	16 (73 %)	1 (2 %)	14 (45 %)	31 (32 %)
SMS	0	14 (31 %)	6 (19 %)	20 (20 %)
Phone call	0	15 (33.3%)	0	15 (15 %)
Not sure/Don't know	1 (5 %)	1 (2 %)	0	2 (2 %)

1. Options offered but never chosen: app, website, other.

Across the three threat types (Table 3.12), websites were the most frequently reported source, accounting for 31%, particularly in malware scenarios, where it was reported in 65 instances. Social media messages were the second most reported source overall, accounting for 20 % (47 instances), and in Phishing (32%, 31 instances) and Data/Identity theft scenarios (19 %, 5 instances).

Table 3.12: All data for sources of threats across all scenarios.

Source	Phishing	Malware	Data/ID Theft	All
Email	30 (31 %)	5 (5 %)	0	35 (15%)
Social Media Message	31 (32 %)	11 (10 %)	5 (19%)	47 (20%)
SMS	20 (20 %)	1 (1 %)	7 % (2)	23 (10 %)
Phone call	15 (15 %)	0	0	15 (7 %)
Website	0	65 (59 %)	8 (30%)	74 (31 %)
App	0	13 (12 %)	5 (19 %)	18 (8 %)
Human recommendation	0	3 (3 %)	0	3 (1 %)
Not sure/Don't know	2 (2 %)	13 (12 %)	6 (22 %)	21 (9 %)

The findings suggest that malware arises during everyday web use, such as browsing or downloading from unfamiliar sites. This highlights the fact that unsafe web practices remain a major route for malware and data theft. In contrast, phishing threats received through social media messages show how attackers increasingly take advantage of personal connections and trust within online networks, making these threats harder to recognise. The limited reporting of threats from SMS and email may reflect better user awareness of these traditional methods of cyberattack.

3.3.4 Consequences of Online Threats

Participants selected from a list of possible consequences of encountering situations similar to those in the scenarios. Each scenario was followed by a set of consequences relevant to that specific threat presented in the scenario.

In all scenarios, participants were provided with two additional response options for reporting consequences: "Other, explain in a later question" and "Cannot remember or not sure". The first

option allowed participants to describe consequences not listed among the predefined choices. This open-ended response was later reviewed, and if relevant, coded and included in the analysis (e.g. pop-ups in S1 were identified through such responses). When participants' answers to “other” were too vague or unclear to interpret, they were coded as “Not specified”. The second option, “Cannot remember or not sure,” was offered in case participants were unable to recall any specific outcomes.

To enhance the clarity and accuracy of the reported percentages for actual consequences, responses marked as “Not sure” or “Not specified” were excluded from the main consequence tables. However, they were added as notes below the tables.

In malware-related scenarios (Table 3.13), the most frequently cited consequence is device slowdowns, accounting for 40 % of all mentions. This issue was especially common in S2 and S3, where 79 % and 82 % of participants, respectively, reported that their devices became noticeably slower after encountering the threat.

Strange pop-ups were also frequently reported, particularly in S8 (75 %) and S7 (55 %). Screen freezing was reported in 21 % of cases, most notably in S1, where 43 % of participants described their device becoming unresponsive. Device crashes were less commonly reported (15 %), but still appeared across several scenarios, particularly S1 and S2.

Scenario S4, which involved ransomware, offered a different set of consequences. Instead of performance-related issues, participants were presented with and selected the option “Could not access some of the files,” which was chosen by 67 % of them.

Among Data and Identity Theft scenarios, financial consequences were most frequently reported in S5 (Table 3.14). More than half of those who experienced a similar scenario reported losing money. Additionally, 29 % indicated that they were unable to use their credit card.

In contrast, Scenarios S6 and S12 mainly resulted in non-financial consequences (Table 3.15). Receiving annoying SMS or calls, reported by 46 % of participants in S6, followed by identity theft (36%). S12 was less common, with 1 participant reporting that they had handed over personal data to a fraudulent website.

In the phishing and spear phishing scenarios (Table 3.16), in Scenario 9, which dealt with spear phishing and impersonation, nearly three-quarters of participants (73 %) noted that many of their contacts received fraudulent messages that appeared to come from them.

Even though participants reported Scenarios 10 and 11 as the most encountered threat types among the 12 scenarios, a substantial portion of participants did not specify the consequences associated with experiencing such scenarios.

The results show that the consequences experienced by participants ranged from minor device disruptions to more serious outcomes such as data loss or financial impact. This pattern suggests that while many threats cause noticeable inconvenience, a smaller number lead to lasting harm.

Table 3.13: Consequences of malware online threats (multiple choices possible).

	Screen frozen	Device slow down	Device crash	Strange pop-up
S1 N = 28	12 (43 %)	16 (57 %)	8 (29 %)	3 (11 %)
S2 N = 19	6 (32 %)	15 (79 %)	6 (32 %)	N/A
S3 N = 17	5 (29 %)	14 (82 %)	4 (24 %)	N/A
S4* N = 3	N/A	N/A	N/A	N/A
S7* N = 20	6 (30 %)	0	3 (15 %)	11 (55 %)
S8* N = 24	0	9 (38 %)	0	18 (75 %)
Total $N_{mention}$ = 136	29 (21 %)	54 (40 %)	21 (15 %)	32 (24 %)

*Offered in S4: Could not access some of the files, and selected by 2(67 %)
*Offered in S7: Browser homepage changed selected by 4(20 %)
*Offered in S8 : (Unknown software/apps installed, and selected by 4 (16.7%), and Mass emails were sent from my email address, selected by 3 (13 %))
* There is an option "Not sure/cannot remember", and 12 participants across all Malware scenarios selected it.

Table 3.14: Consequences of S5: theft of bank details (multiple options possible).

	Lost money	Could not use credit card	Bank account became overdrawn
S5 N = 14	8 (57 %)	4 (29 %)	0

*Five responses were not specified

Table 3.15: Consequences of S6: theft of personal information and S12: data theft spoofed website (multiple options possible).

	Blackmailed by someone	Identity stolen	Annoying SMS/calls	Gave personal data
S6 N = 11	0	4 (36 %)	5 (46)	N/A
S12* N = 2	N/A	N/A	N/A	1 (50)

*Offered in S12, but not selected (handed over personal data to the fraudulent website, handed over credit card number to the fraudulent website, device was infected with malicious software)
* Five responses were unspecified (2 in S6 and 1 in S12)

Table 3.16: Consequence of phishing scenarios.

	Friend responds/ upset	Friends received messages	Entered personal data	Responded, but not with info requested
S9 N=22	5 (23 %)	16 (73 %)	N/A	N/A
S10 N = 45	N/A	N/A	12 (27 %)	N/A
S11 N = 31	N/A	N/A	N/A	6 (18)

*Option offered in S10, but never selected: I could not access some of my online accounts, my personal information was used illegally, Malicious software was downloaded to my device
*In S10, 29 selected "other", and in S11, 24 selected "other" answers were not specified,
* Ten participants selected not sure/cannot remember

3.3.5 Participants' Accounts of a Memorable/Recent Online Threat Incident

Participants were asked in an open-ended question to briefly explain a memorable/recent incident of the type of online threat, including what actions they took, how they realised something was wrong, and how they tried to solve the problem.

Almost all participants (75/81, 93%) answered this question in relation to one or more of the scenarios. In total, there were 223 answers out of a possible 236 opportunities, so 95 % of relevant scenario reports included an answer to this question (Table 3.17).

The text of participants' answers was analysed with a content analysis. A code dictionary was created based on the participants' answers. The analysis was organised into three main topics: threat detection, solutions and the adequacy of solutions, which are presented below.

Table 3.17: No. of answers provided by the participants to the open-ended question.

Scenario type	Scenario	N Participants	N answers	% answers
Malware	S1	28	27	96
	S2	19	18	95
	S3	17	14	82
	S4	3	3	100
	S7	20	18	90
	S8	24	23	96
Data/Identity Theft	S5	14	12	86
	S6	11	11	100
	S12	2	2	100
Phishing/Spear Phishing	S9	22	20	91
	S10	45	45	100
	S11	31	30	97
Total			223	

3.3.5.1 Participants' Descriptions of Threat Detection Cues

The ways participants detected threats fell into five main categories: Message content and design, Suspicious Activity, Impersonation Device/System behaviour and Prior Knowledge. See Table 3.18 for definitions and examples of the detection cues.

Table 3.18: Content analysis threat detection cues.

Main category/Subcategory	Definition	Example
MESSAGE CONTENT AND DESIGN		
Poorly constructed content	The language makes a message seem unprofessional or fake; it may have spelling/ grammar mistakes	S10: after looking at the email address it came from and re-read the email I noticed some spelling errors and realised it wasn't legit (P2) S11: It was asking to send important information but the grammar was off so we knew it was a fake e-mail (P39)
Suspicious Design	Design/layout unusual/ unprofessional, includes suspicious tabs, pop-ups or designs imitating legitimate websites.	S8: I knew something was immediately wrong as various new tabs were opened, which included 18+ material (gambling, pornography, etc.) (P66)
Suspicious/incorrect content	Message about services not requested	
Request for personal information	Message asks for personal information, e.g. bank account details	S10: I received a call from somebody claiming to be from my bank, saying that suspicious activity had been detected on my account. They then began asking me for my details, which I didn't provide and hung up the phone (P60)
Suspicious/unknown sender	Sender address/number is unfamiliar/ suspicious	S10: I received a phone call from a number I did not recognise, when I answered it I was told it was a debt collection agency. I don't have any debt so I hung up. (P35)
Unknown/suspicious link	link unusual, unfamiliar, or unexpected	S10: Legitimate looking email pretending to be LinkedIn, but the link was for another site (P36)
DEVICE/SYSTEM BEHAVIOUR		
Device performance	Device performance changes e.g. slowdown, frozen, restricted access, device/app/software crashes	S1: I clicked on a link that would take me to a clothing site that a friend had sent me and it made my phone run very slowly (P9)
Inappropriate downloads	App download/run without authorisation	S8: I noticed random apps being installed onto my device of which I have never heard of (P75)

Main category/Subcategory	Definition	Example
SUSPICIOUS ACTIVITY		
Suspicious notification	Notifications from individual/organisation of unusual/unauthorised transactions or activity from online accounts.	Sc 6: Someone was using my name on Instagram, pretending to be me or my account. realised when a friend told me (P51) S9: A Yahoo email account was hacked and used to send emails asking for money. I realised this after a few friends contacted me about it (P17)
Suspicious purchase/transaction	Unexpected/unknown purchases on online accounts (e.g. Amazon, delivery service) or on bank/credit card	S5: I noticed an unusual purchase I didn't make from a delivery food app on my online banking and was afraid my details may have been compromised (P5)
IMPERSONATION		
User being impersonated	Personal information (e.g. name, photo) used by someone without consent	S6: Someone used my photos on a dating app but with a different name (P45) Someone stole my photos and set up a Tinder account in my name using my photos as well as my name. (P48)
Sending spam emails/messages	Unauthorised messages sent from the user's account.	S9: I believe my Facebook account was hacked into and a message was sent to many of my Facebook friends asking them to follow a link. My closest friends and family members messaged me to say they had received a link. I then reported this and changed my password immediately. (P60) S9**:** My email was hacked, and some spam was sent to my friends. One of them told me about it, and I changed my email account password straight away. (P78)

Main category/Subcategory	Definition	Example
Receiving spam messages	Noticeable increase in spam messages	S6: My Apple ID was hacked and I received annoying texts and emails. They tried using my email address to sign up for things (P11) S6: Someone got my name and number from somewhere as I received a barrage of spam calls over a few weeks period and they seemed to know my name. I just blocked all the numbers and it stopped eventually (P41)
PRIOR KNOWLEDGE		
Common threat type	Known as common/already encountered	S10: I believe this style of fraudulent call is quite common. I immediately hung up and blocked the number. (P31) S11: I've also had similar fraudulent SMS texts from people claiming to be the post office, dhl, other delivery services etc... Also had them from "NHS" saying I was in contact with someone for "Omicron". All of these were immediately identified as scams (P66)
Threat type known from family/friends/media	Known from family/friends/mass/ social media	S10: Anything that claims to be urgent or pressing can be checked online to see if it's genuine because others will usually be talking about it as well. (P65)

Table 3.19 lists the cues used to detect the threats based on the codes defined in Table 3.18. The most frequently cited category was content or design cues (36 % of total mentions), particularly in phishing scenarios. This includes cues like suspicious content, poorly constructed messages, or requests for personal information. For instance, suspicious content and requests for personal details were frequently identified in S10 and S11, both of which involved phishing messages from seemingly trusted sources.

Device behaviour was also a major detection cue, especially in malware-related scenarios, accounting for 26 % of total mentions. Participants often reported system slowdowns or crashes as indicators of infection, particularly in scenarios S1, S2, and S3.

Another prominent category was suspicious activity, representing 14 % of the total. This included unusual notifications, unexpected messages sent or received, and suspicious transactions. Notably, the most frequent cue within this group was the participant's account sending spam messages to others, primarily in scenario S9 (spear phishing via impersonation), which alone accounted for 17 of these mentions.

Lastly, prior knowledge played a role in detection in about 11 % of cases. Participants relied on general familiarity with scams (e.g. “common scam methods”) or warnings from family, friends, or media to recognise the threat, particularly in phishing-related scenarios.

Table 3.19: Frequency of reporting different threat detection cues for the 12 scenarios.

Cue/Scenario	**Malware**						**Data/ID Theft**			**Phishing**			
	S1	S2	S3	S4	S7	S8	S5	S6	S12	S9	S10	S11	Total (%)
CONTENT/DESIGN													**73 (36 %)**
Poorly constructed											4	2	6 (3 %)
Suspicious design	4	2			11	13					1		31 (15)
Suspicious content											6	5	11 (5)
Personal info											9	6	15 (7)
Suspicious sender											6		6 (3)
Suspicious link											4		4 (2)
DEVICE BEHAVIOUR													**53 (26 %)**
Performance	17	10	12	1	5	1				1			47 (23)
Downloads		3				3							6 (3)
SUSPICIOUS ACTIVITY													**28 (14 %)**
Suspicious notification		1					1	3		8		5	18 (9)
Suspicious transaction							10						10 (5)
IMPERSONATION													**25 (12 %)**
Being impersonated								3					3 (2)
Sending messages						1				17			18 (9)
Receiving messages						1		3					4 (1)
PRIOR KNOWLEDGE													**23 (11 %)**
Common threat type											8	4	12 (6)
Known f/f/m											4	7	11 (5)
TOTAL	21 (10)	16 (8)	12 (6)	1 (1)	16 (8)	19 (9)	11 (5)	9 (4)	0 (0)	26 (13)	42 (21)	29 (14)	202

* In some cases, participants did not provide enough detail to determine which cue they used to detect the threat. These were coded as “Not clear”. The number of such responses per scenario was as follows: S1: 5, S2: 7, S3: 3, S4: 2, S7: 3, S8: 4, S5: 1, S6: 2, S12: 2, S9: 3, S10: 8, S11: 9

3.3.5.2 Participants' Descriptions of Solutions to Threats

Table 3.20 presents the categories of participants' descriptions of their attempts to address the problems associated with online threats. There are three main categories: Technical Actions, Manage accounts and Support and Report, each with subcategories.

Not all participants included solutions in their answers, and in such cases, 'not clear' was used. For Scenarios 10 and 11, some participants reported recognising the threats and choosing not to interact with them. As a result, there were no problems to address, meaning no solutions were required because they avoided engaging with the threats. In this case, the responses were categorised as "no solution and no interaction made". This was the case for 20 responses in S10 and 15 in S11.

Table 3.20: Categories and subcategories of solutions followed by participants in the 12 scenarios.

Category	Definition	Examples
TECHNICAL ACTIONS		
Close/Quit/Restart	Close/force quit a message/ webpage/file/program/app/ device	S1: I accidentally clicked on a side of the screen advert box. It opened a link to a different page and my screen froze. I force-closed the window (P24) S2: However, once I had downloaded it the screen froze. I tried to restart the laptop, however it took 15 minutes before it rebooted. (P23)
Reinstall software/ Clear cache	Reinstalling apps, programs, browsers, OS. Clear or delete the cache on their device or browser	S8: I was unable to close all the pop-ups so I tried to close Instagram down however it did not work. so I re-booted my whole phone and wiped Instagram from my phone and then re-installed it (P23) S8: I had to clear all my cache and redownload my browser as I saw it was trying to download things. (P18)
Delete/uninstall	Participants reported action to delete or uninstall an app, file, program, game, folder, or remove themselves from email lists in response to a potential threat	S8: Google looking different when I opened it and I was getting ads so I went on my files and deleted anything installed that day. (P33)
Use/update security software	Conducting a scan for viruses includes scanning and deleting viruses	S2: Run an antivirus/antimalware scan, find the infected file and delete it asap. (P81)
MANAGE ACCOUNTS		
Change details	Update or change the security details	S8: Clicked on a link and noticed my email account sent loads of emails to spam people.

Category	Definition	Examples
	of online accounts in response to a security threat. This includes changing passwords, updating security questions, or modifying account settings to enhance security.	I changed my email password, and it never happened again. (P19) S9: I believe my Facebook account was hacked into and a message was sent to many of my Facebook friends asking them to follow a link. My closest friends and family members messaged me to say they had received a link. I then reported this and changed my password immediately. (P60)
Cancel card/payment	Acting to close or cancel a card, payment, or transaction in response to a security threat	S6: Someone hacked my Deliveroo account and tried to place an order, I closed my account and luckily my bank blocked the transaction (P77) S5: I called my bank who cancelled my card and got the money back (P13)
Block/confront popups/attackers	Confront someone who is misusing personal information or images or blocking or preventing unwanted popups, emails, phone numbers	S6: I remember once my male friend was using my Facebook photos to troll some men on dating apps. It was only two photos and I did call him out for it and he stopped. (P73) S7: A lot of pop-ups just show up. Antivirus and anti-malware don't really stop popups. Have to block popups to stop them (P50)
SUPPORT AND REPORT		
Warn others/report	If participants notify friends, family, colleagues, or contacts that someone is pretending to be them, and sending messages from their account. informed the service provider such as a bank or social media provider about the security issues	S9: I realised this after a few friends contacted me about it. I deleted the account swiftly and warned my friends about it. (P17) S11: A friend had their Instagram account hacked, and they had posted a story asking for £100 urgently. I did not respond to the request as my friend messaged me on a separate social media app telling me not to. I reported the account and I believe it was taken down. (P44)
Seek human advice	Seek advice from professionals, family or friends to resolve a security issue	S5: Someone had been using my credit card to purchase Amazon Prime, I notified Amazon and they suspended the account and card in question. (P57)
No solution: Threat recognised and no interaction made	Participants identified the threat as suspicious or fake and chose not to engage with it (e.g. ignored the message or avoided clicking links).	S10: A robodial call telling me that my national insurance number had been blocked and that HMRC needed to talk to me. I knew that this was fake because I knew that national insurance numbers can't be blocked, that's not a meaningful concept. I hung up before I was asked to take any action. (P47)

Table 3.21 shows the frequency with which participants reported solutions they followed to address problems associated with encountering threats similar to those presented in the scenarios.

Participant responses revealed a wide variety of attempted solutions to online threats, with the most frequent responses falling into the category of technical actions, particularly deleting or uninstalling software. This solution was used in nearly all malware-related scenarios and accounted for the largest proportion of responses overall (26 %). For example, in scenarios S3 and S7 (involving free apps and adware), uninstalling problematic software was the most common reaction.

Use or update of security software was reported less frequently (12 %), but appeared across all types (Malware, Identity theft and Phishing) scenarios, which may suggest a moderate level of awareness of formal protection tools.

In the case of data and identity theft, participants were more likely to take account management actions, such as cancelling payment cards or changing login details, particularly in scenarios S5 and S6. Notably, cancelling cards appeared in 11 cases, which may indicate awareness of financial protection measures.

One interesting finding was the use of blocking or confronting attackers (11 %), especially in phishing scenarios (S10 and S11). This active response demonstrates a degree of confidence or experience in managing threats, though it may not align with best security practices.

Reporting or warning others was relatively rare (8 %), and very few participants mentioned seeking expert or human advice (6 %). These low figures highlight a potential gap in user awareness of available support and reporting channels.

The code "No solution as no interaction with the threat" emerged from responses to S10 and S11. In these scenarios, 20 participants (44 %) in S10 and 15 participants (50 %) in S11 stated that they recognised the threat and chose to ignore it. As no further action was taken, these responses were not coded as solutions in Table 3.21.

Table 3.21: Frequency of reporting different attempts to solve threats.

Solution/Scenario	**Malware**						**Data/ID Theft**			**Phishing**			
	S1	S2	S3	S4	S7	S8	S5	S6	S12	S9	S10	S11	Total
TECHNICAL ACTIONS													**102 (60 %)**
Close/Quit/Restart	16	2		1		6			2		2		29 (17)
Reinstall s/w	1		1			4				1			7 (4)
Delete/uninstall s/w	1	4	11	2	6	5	1	4		2	4	5	45 (26)
Use/update security s/w	1	4	1			4	1	4		1	4	1	21 (12)
MANAGE ACCOUNTS													**45 (26 %)**
Change details						1	1			9	5		16 (9)
Cancel card/payment							9	2					11 (6)
Block/confront attackers					1			3			6	8	18 (11)
SUPPORT AND REPORT													**24 (14 %)**
Warn others/report						1				7	3	3	14 (8)
Seek human advice							9	1					10 (6)
TOTAL	19	10	13	3	7	21	21	14	2	20	24	17	171

3.3.5.3 Adequacy of Participants' Attempts and Solutions

Participants' responses on their attempts to solve the online threat were also analysed to assess whether the solutions would be adequate. To assess the adequacy of solutions, I identified appropriate solutions for each online security threat in the scenarios. Initially, a set of recommendations or countermeasures was gathered from reputable companies, including Kaspersky, Norton, Google, and the United Kingdom's National Cyber Security Centre (NCSC). The full table of the recommended solutions is in Appendix D: List of Recommended Solutions Provided by Security Expert. However, it became evident that there is no clear, step-by-step advice available for individual users to follow when they encounter particular online threats. Typically, a mix of preventive and proactive steps was mentioned.

For example, both Norton and the NCSC provide guidance on responding to malware infections, but they differ in emphasis and detail. The NCSC's guidance focuses on system-level actions such as updating the device, running antivirus scans, and, if necessary, performing a full system wipe and reinstallation, followed by restoring from a clean backup, assuming that preventive measures such as regular backups were in place before the infection (NCSC Guidance, 2018). In contrast, Norton's advice includes more step-by-step user actions, such as disconnecting from the internet, starting the system in Safe Mode, checking for malicious apps in the activity monitor, using a malware scanner, verifying browser settings, and clearing the cache (Buxton, 2025)

This issue has already been noted in the literature, for example, by Egelman and Peer (2015) who stated that "current computer security recommendations targeted at end-users are highly scattered, inconclusive and inconsistent. This could be very confusing to end-users who are not highly educated on this topic" (p. 2888).

To address this, a brainstorming session with my supervisors was conducted to review the recommendations and to create a table of adequate solutions for each scenario (see Appendix D). I then used the table to assess whether each solution mentioned by participants was considered adequate.

Table 3.22 summarises the analysis of the adequacy of the solutions. Overall, the adequacy of solutions provided by participants was 52 %.

Data/Identity Theft scenarios had the highest proportion of adequate solutions, especially in *S5 (Stolen Bank Details)*, where all responses that included a solution were considered adequate (100%)

Malware scenarios showed more inadequate responses. In *S1* (Malware through link*),* although 59 % of participants reported taking action, only 25% of those responses were considered adequate. Similarly, in S3 (Malware, free app) where 92 % of solutions were inadequate. Two scenarios (S4 and S7) did not have any adequate solutions.

Phishing/Spear Phishing had a mixed pattern of adequacy. For phishing attempts that appeared to come from trusted parties (S10), nearly 91% of respondents took appropriate action. Additionally, all solutions for spear phishing, where attackers impersonate someone else (S11), were adequate. However, it seemed to be more complicated for the participants when it involved impersonating participants (S9), as 64 % of the solutions in this case were inadequate

In some cases, there are multiple viable solutions. In scenario 9, for example, the countermeasures provided by experts, consisted of three required actions (notify your friends, try to recover the account, and change your passwords). However, 64 % of participants followed inadequate solutions to solve the problem by only taking one action, which may be required, but is insufficient to solve the problem.

Participants provided no adequate solutions for scenarios 4, 7, and 12, which involved ransomware, adware, and spoofed websites. This could imply that such threats are not very common among younger adult users in the UK, as shown in Table 3.6 scenario result above, where participants reported that ransomware and spoofed websites are the least frequent threats. Adware was encountered by 25 % of respondents, and the majority of them reported that strange pop-ups appeared frequently as a result of this threat. This could refer to participants' lack of awareness about adware and their ability to deal with it.

Table 3.22: Assessment of adequacy of participants' solutions addressing the security threats.

Scenario N*	(%) answers with/without solutions	Assessment of solution adequacy	Examples
MALWARE			
S1. Malware, link N= 27	With solutions: 16 (59 %) Without solution: 11 (41 %)	Adequate solutions: 4 (25%) Inadequate: 12 (75%)	Adequate: I pressed a link by accident and it crashed the app multiple times and made my phone run slowly. Subsequently, I restarted my phone and scanned for viruses etc..(P53)
S2. Malware, attachment N=18	With solutions: 8 (44 %) Without solution: 9 (50 %)	Adequate solutions: 5 (63%) Inadequate solutions: (76%)	Adequate: something being downloaded without my permission and then I had computer problems. I was however able to uninstall it then I downloaded some anti-virus software to check my mac for viruses and remove them (P61)
S3. Malware, free app N=14	With solutions:12 (86 %) Could not be coded: 1 (7 %) Without solution: 1 (7 %)	Adequate solution: 1 (8%) Inadequate solutions: 11 (92 %)	Adequate: it was a game which slowed down my phone and made the battery life decrease fast so I assumed it was a crypto miner so I found the apk of the same game and put in into virus total and it came back positive for crypto miners and I immediately uninstalled and everything was fine (P69) Inadequate: I tried to get a game for free off an unknown app store and this caused my device to run very slowly, I couldn't figure out how to fix it so I had to uninstall the game. (P74)
S4. Malware, ransomware N=3	With solutions: 3	No adequate solution	Inadequate: I was unable to access my files after downloading some free software from a website. I had try to uninstall the software which eventually worked (P75)
S7. Malware, adware N=18	With solutions: 7 (39 %) Without solution: 11 (61 %)	No adequate solution	Inadequate: A lot of pop-ups just show up. Antivirus and anti-malware don't really stop popups. Have to block popups to stop them (P50)
S8. Malware, phone N=23	With solutions: 15 (65 %) Without solution: 8 (35 %)	Adequate solutions: 6 (40%) Inadequate solutions: 9 (60%)	Adequate: Pop-ups appear, one or more, close them all down (alt-f4 spam) or ctrl-alt-del and restart the PC, then check for viruses/malware. (P81) Inadequate: I clicked on a link saying free iPhone. It downloaded something onto my computer which I had to delete (P67)

Scenario N*	(%) answers with/without solutions	Assessment of solution adequacy	Examples
DATA/IDENTITY THEFT			
S5. Theft bank details N=12	With solutions: 10 (83 %) Without solution: 2(17%)	Adequate solutions: 10 (100%)	Adequate: I have had my bank card used for iTunes gift cards, I don't know how they would have got my details though. I knew this was wrong as I don't shop at iTunes. I contacted my bank straight away to get a new card and also they were able to get my money back (P39)
S6. Theft personal info N=11	With solutions: 4 (36 %) Without solution: 7(64 %)	Adequate solutions: 3 (75%) Inadequate solutions: 1 (25%)	Adequate: I remember seeing details of me on a website and getting messages about it. I contacted the website to remove my details. (P64)
S12. Theft personal information, spoofed website N=2	With solutions: 2	No adequate solution	Inadequate: I received a text saying something had expired that I thought was true and went onto the website that was linked and entered some personal information before realising it was fraudulent and then I closed the site. (P32)
PHISHING/SPEARPHISHING			
S9. Spear Phishing, impersonating participant N=20	With solutions: 14 (70%) Without solution: 6 (30%)	Adequate solutions: 5 (36%) Inadequate solutions: 9 (64%)	Adequate: Someone hacked into my account and sent a link to lots of contacts. I told people what had happened and changed my password (P24) Inadequate: Facebook messages to multiple friends advertising some malware or something similar. I clarified it wasn't me and they ignored it (P57)
S10. Spear Phishing msg/call, from a trusted party N=45	With solutions: 21(47 %) Without solution: 24(53 %)	Adequate solutions: 19(91 %) Inadequate solutions: 2 (10 %)	Adequate: someone hacked my friend's Instagram account and messaged me saying she had sent something, to access it I had to put in my login details. I realised what had happened after putting in my details so I changed my password, and added extra security to my account. (P28) Inadequate: I was told I'd get a DVLA refund for my road tax, clicked on the link and began typing in my card details when I realised it was a scam and deleted the page. (P57)
S11. Spear Phishing	With solutions: 14 (47 %)	Adequate solutions: 14	Adequate: This has happened to me once on FB messenger.

Scenario N*	(%) answers with/without solutions	Assessment of solution adequacy	Examples
msg/call, impersonating someone N=30	Without solution: 16 (53 %)	(100%)	Someone posing as a close friend said they needed 200 quid. I had heard of the scam before so I called my friend who confirmed it wasn't them. I blocked and reported the profile (P41)

* N is the number of answers to the open-ended question

3.3.6 Participants' General Worries about Online Threats and Their Relationship to Experiences of Online Threats and Computer and Security Competencies

Participants' ratings of the level of worry on the 9 statements are summarised in Table 3.23.

Ratings of the two statements related to malware were not significantly different from the midpoint of the scale (4.0). The only statement with a rating significantly above the midpoint of the scale was one of the three related to Data/Identity Theft (Someone will steal my online identity and misuse it). The other two statements in this category had ratings not significantly different from the midpoint. All the Phishing statements had ratings significantly below the midpoint, indicating that participants are least worried about this kind of online threat.

Table 3.23: The worry statements measuring the level of worry about online security threats.

Threat type/Statements	**Median (SIQR)**	**Z Score**	**p**
Malware			
Someone will lock me out of my device(s) and demand money to restore access	4.0 (1.5)	-0.66	n.s.
Someone will access my device(s) or account(s), look at my information and use it to blackmail me	4.0 (2.0)	-0.91	n.s.
Data/Identity Theft			
My device will be accessed by an attacker and my data will be destroyed	4.0 (1.5)	-0.51	n.s.
Someone will steal my online identity and misuse it	5.0 (1.5)	2.09	0.03
Someone will access my device(s) or account(s), steal my data and use it for malicious purposes or to their advantage (e.g. make illegal purchases)	5.0 (1.5)	1.50	n.s.
Phishing /Spear phishing			
I will receive a phone call from someone asking about my confidential data (e.g. password, bank account details)	3.0 (1.5)	-4.34	< 0.00
I will click on a link in a SMS message or email from a source that I cannot verify its origin, whether it is trustworthy	3.0 (1.5)	-3.66	< 0.00
I will receive an email with a link leading to a fake website	3.0 (1.5)	-4.44	< 0.00
I will receive an email with an attachment that may include malicious code	3.0 (1.5)	-3.12	0.002

A principal component analysis (PCA) was conducted on the ratings of the 9 statements and produced a very clear solution of two components, which accounted for 71.7% of the variance, with all statements having factor loadings of over 0.68 (See Table 3.24). The first component, Theft Worries, accounted for most of the variance (58.6%) with 5 statements, and the second component, Phishing Worries, with 4 statements, accounted for a further 13.1%.

Table 3.24: Principal component analysis (PCA) of online threat worries.

Component	% Variance
THEFT WORRIES	58.6%
My device will be accessed by an attacker and my data will be destroyed Someone will lock me out of my device(s) and demand money to restore access Someone will access my device(s) or account(s), look at my information and use it to blackmail me Someone will steal my online identity and misuse it Someone will access my device(s) or account(s), steal my data and use it for malicious purposes or to their advantage (e.g. make illegal purchases)	
PHISHING WORRIES	13.1%
I will receive an email with a link leading to a fake website I will receive an email with an attachment that may include malicious code I will receive a phone call from someone asking about my confidential data (e.g. password, bank account details) I will click on a link in a SMS message or email from a source that I cannot verify its origin, whether it is trustworthy	

Median scores on these two components were calculated for each participant to investigate the relationships between these two major worry areas and experience with online threats, as measured by the number of threats they reported experiencing and how frequently they experience them, and self-reported computer and security knowledge and ability in identifying security threats (computer and security competencies).

There was no significant relationship between scores on either component and either self-reported computer or security knowledge. However, there was a significant relationship between Phishing Worries and self-reported confidence in the ability to identify security threats (Phishing Worry: rho = −0.27, p = 0.015). This showed that participants who were more confident in their ability to identify security threats were less worried about phishing attacks.

There were also interesting relationships between participants' scores on the components and their experience of online threats. In relation to whether participants reported having experienced threats at all, there was a positive relationship between both Worries component and the number of threats experienced (Theft Worries: rho = 0.27, p = 0.027; Phishing Worries: rho = 0.23, p = 0.036). This means the more online threats they said they had experienced, the higher their scores on both Worries components.

The relationship between the components and how frequently participants had experienced online threats was less clear. As there were 12 scenarios, linear regressions were conducted to predict Worries scores from the ratings of the frequency of experiencing each of the different scenarios. The overall result for Theft Worries scores was just short of significance ($F_{12, 80} = 1.80$, p = 0.067), however, Scenarios 1 and 4 were individually significant predictors (Scenario 1: p = 0.008; Scenario 4: p = 0.027). The overall result for the Phishing Worries scores was significant ($F_{12, 80} = 2.06$, p = 0.031), with Scenarios 1 and 10 being individually significant predictors (Scenario 1: p = 0.014, Scenario 10: p = 0.042). So, Scenario 1 is particularly predictive of being worried about online threats.

3.3.7 Participants' Self-Reported General Security Behaviour (SeBIS) and its Relationship to Their Experiences of Online Threats and Computer and Security Competencies

To explore how well the SeBIS subscales reflect participants' self-reported online security behaviours, their relationships with three self-rating questions: computer knowledge, security knowledge, and ability to identify online threats, were examined. In addition to the 81 UK participants who completed the initial questionnaire, an additional 126 participants were recruited via Prolific to provide a larger sample (N = 207) . A Principal Component Analysis (PCA) was conducted on this full sample to validate the SeBIS structure within the UK context (see Appendix E). However, further analysis needs to be undertaken for a validation which was not possible in the time scale of this thesis, therefore, the four subscales proposed by Egelman and Peer on the basis of data from the USA were used in the analysis.

The original SeBIS subscales were used to assess the participants' self-reported security behaviours. To understand how the UK sample's security behaviour intentions compared to previous research, the mean SeBIS subscale scores were compared against the normative values reported by Egelman and Peer (2015). The SeBIS normative values reported by Egelman and Peer (2015) were derived from a large sample of participants recruited primarily from the United States through online platform (Mechanical Turk). The sample had a relatively balanced gender distribution, a wide adult age range (19–71 years; mean age in the mid-30s), and a substantial proportion of participants with undergraduate or postgraduate education. The authors described this sample as broadly representative of the U.S. online population.

The adjusted means were calculated by rescaling the 7-point Likert responses to match the original 5-point SeBIS scale used by Egelman and Peer. As shown in Table 3.25, the Device Securement subscale was significantly higher than both the original SeBIS mean and the scale midpoint. In contrast, no significant differences were found for Password Generation or Proactive Awareness when compared to Egelman's norms. However, the Updating subscale was significantly lower than the original SeBIS mean and below the midpoint, suggesting weaker behaviours in applying security updates.

Table 3.25: Means of SeBIS subscales in the current sample, with statistical comparison with scores from Egelman and Peer (2015) and with the midpoints of each subscale.

Subscale	Egelman and Peer Mean[1]	Current sample Mean (SD)	Adjusted mean[2]	Comparison with Egelman and Peer	Comparison with midpoint
Device Securement	3.21	5.9 (1.01)	4.21	$Z = 11.8$, $p < 0.00$	$Z = 12.2$, $p < 0.00$
Password Generation	3.25	4.4 (1.22)	3.14	$Z = -0.95$, n.s.	$Z = 3.9$, $p < 0.00$
Proactive Awareness	3.73	5.0 (1.1)	3.57	$Z = -1.56$, n.s.	$Z = 10.0$, $p < 0.00$
Updating	3.47	3.6 (0.98)	2.57	$Z = -11.1$, $p < 0.00$	$Z = -4.9$, $p < 0.00$

[1.] Egelman and Peer (2015) only provide mean scores for individual items in SeBIS, not the subscales. So I calculated the mean score for each subscale, but this means I cannot calculate the SD for each subscale in their sample

[2.] I used a 1–7 scale; the original SeBIS used a 1–5 scale, therefore, these are the subscale scores adjusted to a 1–5 scale to allow comparison with the original SeBIS results by multiplying by 0.714.

To assess how these original SeBIS subscales relate to participants' self-rated computer and security competencies, Spearman's correlation was used.

Table 3.26. shows the result. It showed that there is a significant positive correlation between self-rated ability to identify the attack and these SeBIS subscales: Device Securement (r = .165, p = 0.01) and Proactive Awareness (r = .206, p = 0.003).

Security knowledge showed positive correlations with Password generation (r = .208, p = 0.00), Proactive Awareness (r = .207, p = 0.00) and Updating (r = .180, p = 0.01). While computer knowledge was only significantly associated with Proactive Awareness (r = .167, p = .016).

Table 3.26: Correlation between SeBIS subscales and computer and security competencies.

	Computer knowledge	**Security knowledge**	**Ability to identify the attack**
Device Securement			(r = .165, p = 0.01)
Password Generation		(r = .208, p = 0.00)	
Proactive Awareness	(r = .167, p = 0.01)	(r = .207, p = 0.00)	(r = .206, p = 0.00).
Updating		(r = .180, p = 0.01)	

A Spearman correlation was conducted to examine the relationship between participants' SeBIS scores and their experiences of online threats (see Table 3.27). There was a significant negative correlation between Proactive Awareness and experiences of online threats (r = -.327, p = 0.00). This suggests that participants with higher proactive security awareness were less likely to experience online threats. In terms of worry components, there is no correlation between participants' scores in SeBIS and either worry components.

Table 3.27: Correlation of SeBIS subscales with experience of online threats.

	Device Securement	**Password Generation**	**Proactive Awareness**	**Updating**
Experience of threats	n.s.	n.s.	r = -.327, p = 0.003	n.s.
Theft worries	n.s.	n.s.	n.s.	n.s.
Phishing worries	n.s.	n.s.	n.s.	n.s.

3.4 Discussion

This study investigated the experiences of a range of online threats and the frequency of those experiences by a sample of British young adults. This was achieved by creating a set of 12 short scenarios presenting a range of online threats from the user's perspective in non-technical language. Participants were asked not whether they had experienced exactly the scenario, but "something like" it, to allow for a range of similar experiences. This scenario-based approach differs from most earlier survey studies, such as those by Hewitt and White (2022) evaluated participants' experiences with security by asking general, subjective questions about frequency and impact (e.g. "How recently have you been affected by a computer security problem?"). In contrast, the current study employed specific, realistic scenarios to prompt participants to recall and evaluate particular threats.

To further support the development of these scenarios, elements from the MITRE ATT&CK and Cyber Kill Chain frameworks were integrated into the study design. These frameworks are commonly used in modelling threats targeted at organisations (Naik et al., 2022), but were adapted here to reflect the stages and tactics most relevant to individual users. For instance, the "Delivery" and "Exploitation" stages from the Kill Chain were particularly useful in understanding how threats are encountered and acted upon by individuals. Similarly, MITRE's categorisation of techniques, such as phishing or user execution, helped map participant experiences to structured patterns of attack. Applying these frameworks helped structure the threat scenarios in a way that reflected real-world attack stages and techniques. This mapping ensured that the scenarios were not only realistic but also grounded in recognised cybersecurity models typically applied in organisational settings. Their use here at the individual user level contributes a methodological innovation to studies examining personal experiences with online threats.

The results highlight several important findings regarding the experiences of online threats by a sample of younger adults, sometimes referred to as "Generation Z", in the UK, including how they recognise these threats and the solutions they used to mitigate them.

The sample used in this study can be considered well-educated, as more than half of the participants hold a degree. They rated themselves above average in terms of computer knowledge, online security knowledge, and ability to identify attacks. However, they had frequently reported experiences of online threats and had difficulties in effectively dealing with them. These difficulties may be explained by similar studies that focused on young adults and argued that growing up with technology does not necessarily equate to better security practices and knowledge (Furnell & Moore, 2014; Petrie & Merdenyan, 2016).

This finding raises the possibility that, if individuals within an educated sample who perceive themselves as capable of identifying cyberattacks encounter various types of threats, those who may not have the same level of education or perceived expertise may find more difficulties in recognising or dealing with them.

While the research questions for this study were designed to examine key aspects of younger adults' experiences with online threats, it is important to reflect on their scope and sufficiency. The questions do effectively capture what threats younger adults in the UK encounter, how they recognise and respond to them, and how these experiences relate to their behavioural intentions. However, the findings also suggest that focusing solely on experiences may not fully address how prepared or resilient British younger adults are when facing online threats. This reflection suggests that the RQs were necessary and appropriate for understanding exposure and response; however, future work should extend them to consider their levels of awareness and learning, and how these and other contextual factors influence their readiness and long-term digital resilience.

Turning to the results on each of the research questions:

RQ1: What are the types and frequency of online threats encountered by younger adults in the UK?

The first research question investigated the types and frequency of online threats experienced by this study sample. Phishing and spear phishing emerged as the most commonly encountered threats,

reported by over three-quarters of participants. This widespread exposure reflects their ongoing prominence in the online environment and aligns with reports suggesting that phishing remains one of the most persistent threats individuals face (APWG, 2024; Furnell, 2021).

Malware was also commonly encountered, with nearly three-quarters of participants reporting such experiences. Although new cyber threats are emerging, malware remains a widespread risk, as attackers continue to develop sophisticated variants such as ransomware, spyware, and Trojans (Furnell, 2021). This suggests that malware remains a persistent problem for individual users despite ongoing advancements in technical security measures.

In contrast, data and identity theft were reported less frequently than malware and phishing, even though they were addressed in three scenarios, one about stolen bank details and two focusing on the misuse of personal information. This is somewhat surprising, considering that Identity-based crimes, including both theft and fraud, have been increasing globally (Gies et al., 2020; Pascual et al., 2018). The relatively low number of participants in the UK sample reporting such experiences is also unexpected, as recent reports indicate that identity theft remains a significant threat in the UK. According to Cifas' Fraudscape 2025 report, there were over 249,000 cases in 2024 alone (Cifas, 2025). The low reporting rate in this sample may indicate a lack of recognition or underreporting of these issues. Supporting this observation, a study in the U.S. found that people often overlook identity theft protection practices, especially those that require ongoing effort from the user (Honolulu & Chi, 2020). These trends may also apply to participants in the UK.

Another interesting finding was that websites were the most frequently reported sources of malware and data theft, while social media and email were more commonly linked to phishing and spear phishing scenarios. This finding is consistent with the definition provided by the United States Computer Emergency Readiness Team (US-CERT), as cited in Alkhalil et al. (2021), which describes phishing as “a form of social engineering that uses email or malicious websites (among other channels) to solicit personal information from an individual or company by posing as a trustworthy organisation or entity”.

Ofcom’s 2023 report shows that UK users aged 16–24 engage with an average of nine online platforms, much more than older adults. Popular platforms like YouTube, WhatsApp, Facebook, and Instagram show year-on-year growth, which heightens young users' exposure to threats.

A phone calls emerged as a source of phishing attempts, particularly when attackers impersonated trusted parties, such as financial institutions or service providers (S10). This result agrees with an early study by Caldwell (2013), who expected that smartphones would become a source of attack in the future, as it was common that people respond to information requested over their mobile immediately.

RQ2: How do young UK adults detect and respond to online threats?

A key contribution of this study lies in the categorisation of cues participants reported using to detect online threats. Through a content analysis of their responses, five main categories of detection cues emerged: message content/design, device behaviour, suspicious activity, impersonation, and prior knowledge. Notably, cues related to message content and design, such as suspicious design or requests for personal information, were the most frequently cited (36.1%), particularly in phishing and malware scenarios. This finding agrees with previous work by Steves et

al. (2020), who identified “Language and Content” as a key cue category, including subcategories such as requests for sensitive information and the presence of urgent or suspicious language.

Similarly, device behaviour (e.g. device slowdown or crash) was reported frequently (26.2%) and it was often linked to Malware scenarios. These findings highlight how both technical symptoms and contextual content play critical roles in user threat recognition.

Suspicious activities were reported frequently in scenarios related to data and ID theft. These included noticing unauthorised transactions or suspicious notifications. Such cues reflect a more reactive form of threat detection, where users recognise something is wrong only after the attack has progressed or harm has occurred.

Impersonation was another cue that occurred in Data/identity theft scenarios as well as one Phishing scenario (which was mainly about impersonating the participants). Recognising the threat relying on impersonation as cues was mentioned in a previous study by Bera et al. (2023). The study highlighted that impersonation is an effective technique often seen in phishing and spear-phishing emails, where attackers impersonate authoritative entities to prompt the victim to reveal confidential information.

Interestingly, prior knowledge, such as having heard about the threat before or recognising the scam method as common, was also reported by participants as a detection cue. This finding agrees with earlier research showing that user experience and familiarity with threats can improve security behaviours (Algarni et al., 2017; Jeske & van Schaik, 2017).

Another important finding in this study was understanding the actions participants took in response to online threats. The analysis revealed that participants’ solutions fell into three main categories: Technical Actions, Account Management, and Support and Reporting.

Technical Actions were the most frequently reported type of response. The most common of these was deleting or uninstalling software, particularly in scenarios involving malware. Although using or updating antivirus software was reported, it was less frequent, possibly reflecting participants’ limited knowledge or confidence in technical tools.

Account Management strategies appeared prominently in response to identity theft or financial threats. In scenarios where participants reported stolen details or suspicious transactions, or cancelled cards or payments, to mitigate potential harm. Interestingly, blocking or confronting attackers was also reported in phishing-related scenarios.

Lastly, Support and Reporting actions were less common. Warning others, reporting incidents, and seeking advice were reported in Phishing and Data theft scenarios.

Only a few participants reported that they had reported the threats to the authorities as a solution. Despite certain governmental initiatives encouraging users to report phishing incidents, for example, the National Cyber Security Centre (NCSC) advises users to report suspicious emails and text messages to the Suspicious Email Reporting Service (SERS) via report@phishing.gov.uk. In addition, Action Fraud provides a national reporting service for fraud and cybercrime incidents. However, participants may not be aware of these services, or they might only adhere to the minimum actions regarding online security (Zwilling et al., 2022).

In terms of the adequacy of the solutions, participants reported adequate responses to phishing and spear phishing threats. For example, all participants who encountered spear phishing from someone impersonating a known contact reported taking appropriate action. This supports prior research showing that familiarity with specific threat types and past experience can enhance user security behaviour (Albladi & Weir, 2020). Similarly, Jeske and van Schaik (2017) found that frequent internet use among UK and US students was associated with improved threat recognition and security practices, indicating that exposure to common threats may improve response capabilities over time. Another study, targeting US students (Goel et al., 2017), suggested that many students are aware of common phishing detection techniques, about 60% reported hovering over links, and 22% searched for information online before clicking. However, even contextualised phishing messages can still deceive users, especially when cues such as URLs are hidden.

While these findings suggest that participants were reasonably prepared to handle familiar threats, it is also important to consider how well prepared they were for less familiar or more complex types of attacks. Participants did not report sufficient responses to ransomware, adware, and spoofed website scenarios. However, these threats were also among the least frequently reported in this study. This suggests that limited exposure or unfamiliarity contributed to participants' self-perception of their inability to respond appropriately when faced with these types of threats. Although participants rated themselves above average in their security knowledge and ability to identify online attacks, this confidence may not extend to less commonly encountered threats. This pattern reflects uneven preparedness, strong for well-known threats but weaker for new or sophisticated ones and aligns with Ofcom's Adults' Media Use and Attitudes Report (2023), which found that while UK internet users aged 16–24 are highly active online and confident in using digital platforms, they are less likely than average to identify online risks effectively. These findings highlight the need to strengthen young adults' readiness for emerging threats through broader awareness and continuous skill development.

RQ3: What are the levels of worry about online threats among young adults in the UK, and how are these levels related to their experiences of such threats?

The third research question investigated the level of worry among young adults about different online threats. This sample was more worried about data/identity theft than phishing threats. This can be due to the severity of the consequences of identity theft. In Data/Identity theft-related scenarios, the consequences reported by participants were lost money, annoying messages and calls, and stolen identity. These consequences might be considered more severe than those associated with threats in other scenarios, such as phishing and adware. This result is consistent with the result from a previous study conducted to measure risk perceptions for students from the UK and the US and found that students reported identity theft as the riskiest threat and severity of risk was one of the significant predictors of perceived risk (van Schaik et al., 2018).

An interesting relationship was observed between participants' level of worry and their reported experiences. Specifically, those who reported encountering a greater number of threats tended to score higher on both Theft Worries and Phishing Worries components. This suggests that direct experience with threats may increase individuals' concern about them.

Moreover, a significant relationship was identified between self-reported confidence in the ability to identify security attacks and the Phishing Worry component. Specifically, individuals who reported higher confidence in their ability to identify security threats had lower levels of worry about phishing

attacks. This relationship suggests that confidence in recognising phishing attempts may contribute to reduced concern regarding falling victim to such attacks. This result agrees with Algarni et al. (2017), who more cybersecurity knowledge decreases susceptibility to social engineering attacks.

RQ4: What are the online security behaviour intention scores of younger adults in the UK, and how are these scores related to their experience of online threats, computer and security knowledge?

The last research question investigated measuring participants' intentions in relation to their online security behaviours. SeBIS was one of the scales that has been widely used and validated across different contexts and populations (Ayyagari & Crowell, 2020;Egelman et al., 2016; Sawaya et al., 2017) to measure individuals' self-reported of these intentions. While SeBIS was originally developed and validated in a Western context (specifically participants from the US, e.g. Egelman et al., 2016; Gratian et al., 2018), it has also been validated in several studies in other countries such as China, France, Japan, Russia, South Korea (Sawaya et al., 2017). However, to the best of my knowledge, SeBIS has not been widely used to measure online security behaviour intentions among British young adults. One exception is a study conducted during the COVID-19 pandemic, which used SeBIS to examine how loneliness and quality of life influenced online security behaviour among UK home workers (Deutrom et al., 2022).

The findings from the SeBIS subscales offer insight into the self-reported intentions in relation to online security behaviours of British younger adults. In the current sample, participants scored significantly higher than the normative sample in the USA on the Device Securement subscale, suggesting strong behaviours in practices like locking devices. However, their scores on Password Generation and Proactive Awareness did not differ significantly from Egelman and Peer's means, indicating room for improvement in creating strong passwords or checking links and malicious websites. Most notably, scores on the Updating subscale were significantly lower than both Egelman and Peer's values and the scale midpoint, highlighting a persistent reluctance or delay in applying security updates.

Correlational analyses further support these interpretations. A significant positive relationship was found between participants' self-rated ability to identify online attacks and their scores on both Device Securement and Proactive Awareness. This suggests that those who feel more confident in spotting threats also tend to take practical precautions. Similarly, higher security knowledge was associated with better behaviours in password generation, proactive awareness, and updating, pointing to the role of knowledge in shaping secure practices. This agrees with a previous study that targeted students from four countries (Israel, Slovenia, Poland and Turkey) and found that higher security knowledge was linked to good security awareness and behaviours regardless of country and gender (Zwilling et al., 2022).

Interestingly, computer knowledge was only linked to proactive awareness, which may reflect that general digital competence does not necessarily translate into secure behaviours unless paired with specific security awareness.

Taken together, the findings offer insight into the factors that have likely shaped participants' current level of cybersecurity awareness and behaviour. Their relatively strong security practices, including device security and proactive awareness, may be due to the regular exposure to common online threats and a generally high level of digital literacy among younger adults. In contrast, poor

security practices in updating suggest that convenience, habit, or limited attention to maintenance practices in everyday digital education may reduce engagement with good security routines. Overconfidence might also play a role, as those who see themselves as skilled users could underestimate the need for consistent precautions. Overall, these patterns indicate that while participants demonstrate positive intentions toward cybersecurity, certain practical and psychological barriers continue to hinder the translation of secure intentions into secure behaviour.

In summary, the results show that although participants are aware of security threats and concerned about them, they still have difficulties finding the best appropriate solution in some situations.

3.4.1 Limitations of the Study

Participants were recruited through Prolific, which may introduce sampling bias, as Prolific users tend to be more digitally literate and accustomed to research participation than the general population. Also, the study focused on younger adults in the UK, so naturally the results will not generalise to broader age groups or demographic diversity.

Another limitation was that although the study used a scenario-based approach to improve the responses, the data are still self-reports of incidents from the past and may be affected by memory loss, recall bias or social desirability bias, as participants may have interpreted the scenarios differently based on personal experiences.

A similar scenario-based study was subsequently conducted with young adults in Saudi Arabia using the same method, which will be presented in the next chapter. Although no formal cross-cultural analysis was undertaken, the two studies provided an opportunity to explore whether similar patterns in threat types, recognition and response were observed in a different national context. The comparisons will be discussed in the final Discussion and Conclusions chapter.

Chapter 4 Experiences and Concerns of Online Threats among Younger Adults in the Kingdom of Saudi Arabia

4.1 Introduction

In the previous chapter, I used a scenario-based online questionnaire to investigate the types and frequency of online threats experienced by younger adults in the UK and their worries about online threats. The results revealed useful insights about the types of threats reported by participants, their sources and consequences, and how participants dealt with them.

This chapter expands the investigation to include a new participant group: younger adults in the KSA. By investigating a second population, I can assess whether the findings from the UK sample are applicable in a very different culture. Additionally, this chapter aims to explore whether younger adults in KSA encounter different types of threats due to variations in online security behaviours or specific local cybersecurity challenges.

Consistent with the overall research objectives outlined in Chapter 1, this study addresses the following research questions, which correspond to objectives 1–3 of the thesis (see Table 4.1 for the mapping between objectives and RQs):

RQ1: What are the types and frequency of online threats that younger adults in the KSA encounter?
RQ2: How do KSA younger adults detect and respond to online threats?
RQ3: What are the levels of worry about online threats among younger adults in the KSA, and how are these levels related to their experiences of such threats?
RQ4: What are the online security behaviour intention scores of younger adults in the KSA, and how are these scores related to their experience of online threats, computer and security knowledge?

Table 4.1: Mapping thesis objectives to Study 2 research questions.

Thesis objectives	**Study 2 (KSA Survey)**
Obj. 1**:** Identify online threat types and frequency	RQ1
Obj. 2**:** Examine how younger adults detect and respond to online threats	RQ2 and RQ3
Obj. 3: Investigate the effect of individual characteristics on online security experiences	RQ4

4.2 Method

4.2.1 Design

This study uses the same design as Study 1 (see section 3.2.1). The cultural suitability of the questionnaire for the KSA sample was carefully considered. In planning the study in KSA, reports from Saudi national sources, such as Saudi CERT, were reviewed to identify common online threats targeting younger users in the KSA. The selected types of threats are widely encountered and discussed within the KSA, particularly through social media, online banking, and messaging applications, and therefore did not require modification from the UK version of the questionnaire. Moreover, retaining the original scenario content and question structure enabled meaningful

comparisons with the UK sample. Only minor wording adjustments were made during translation and pilot testing to improve clarity, and no changes were made to the underlying threat contexts or response options.

4.2.2 Participants

The inclusion criteria for the study were to be a Saudi citizen currently living in KSA, aged between 18 and 30 years old.

Data collection took place between February and May 2022. Recruitment was conducted using repeated online invitations and reminders circulated through emails and social networks (e.g. WhatsApp) to increase participation. These efforts generated 130 recorded responses in Qualtrics. However, only 73 of these responses were complete, likely due to the length and cognitive demands of the questionnaire. The questionnaire consisted of four parts, including three sections that required participants to carefully read multiple scenarios, reflect on their experiences, and answer a standardised scale measuring security behavioural intentions. This structure required sustained attention and may have contributed to participant dropout before completion. A further screening of the 73 completed responses was then applied using attention check items placed at the end of the questionnaire, resulting in a final valid sample of 45 participants. Although small in size, this approach prioritised data quality and ensured that all included responses reflected meaningful and attentive engagement with the questionnaire content.

The demographic characteristics of the participants are summarised in Table 4.2. Due to an oversight, participants were not asked about their gender.

Table 4.2: Demographic characteristics of the participants in Study 2.

Category	**Range (Mean)**
Age	18–30 Years (27 years)
Highest educational level	
High school	7 (16 %)
Bachelor's degree	28 (62 %)
Postgraduate degree	10 (22 %)
Professional qualification	0
Prefer not to say	0
Self-reported computer expertise	
Median (Semi Interquartile range)	5.0 (1.5)
Z score (probability)	3.52 ($p < .001$)
Self-reported online computer security knowledge	
Median (Semi Interquartile range)	4.0 (1.0)
Z score (probability)	0.14, n.s.
Self-reported ability to identify online attack	
Median (Semi Interquartile range)	5.0 (1.5)
Z score (probability)	1.52, n.s.

Participants were asked to rate their computer knowledge, online security knowledge and confidence in identifying cybercriminal attacks on 7-point rating items. Participants rated their

computer expertise significantly above the midpoint of the rating scale. But on their security knowledge and their ability to identify online attacks, they rated themselves as not significantly different from the midpoint of the scale, so average in each case.

4.2.3 Materials

This study used the same scenarios as in Study 1 (see Table 3.4: The 12 scenarios used in Study 1, with codes, short names and categories.).

4.2.4 Online Questionnaire

The same questionnaire as in Study 1 was used (section 3.2.4).

The questionnaire was developed in English; however, many participants from KSA may have a better understanding of Arabic than English. In the Qualtrics platform, two versions of the questionnaire, one in English and one in Arabic, were developed. Participants were able to select their preferred language at the start of the questionnaire using a language icon located at the top of the first page. Although English was set as the default, participants could switch to Arabic at any time. This option was also clearly stated in the introduction of the questionnaire.

Providing a questionnaire in Arabic enhances accessibility and ensures that language barriers do not prevent their participation in the study. Also, it helps participants comprehend the questions more easily, which leads to more accurate responses.

To ensure the clarity and accuracy of the translation process, I used the following process

- I translated the questionnaire from English to Arabic.
- English–Arabic translation specialist reviewed my translation by comparing both the English and Arabic versions for consistency in meaning.
- The same specialist then translated the Arabic version back into English.
- The back-translated version was compared with the original English version to identify any changes in meaning.
- Finally, a separate reviewer, an Arabic language teacher, checked the Arabic version for grammar, spelling, and punctuation.

Participants were recruited by sending emails and messages through social media. The invitation message in Arabic explained the aim of the study, the expected time, and the requirements to complete it.

4.2.5 Procedure

A pilot study was conducted by asking one security expert, one academic and two students, all from the KSA, to complete the questionnaire. They were asked to check the time required to complete the questionnaire, the clarity of the questions, and spelling and grammar mistakes. A number of comments were received about the clarity of some wordings. The translations were checked and some corrections made.

At the beginning of the study, participants were introduced to the purpose of the study, their right to withdraw, data protection, and compensation for participating in this study. They were then

asked to complete the consent form before proceeding to the study. Participants were encouraged to participate by being offered a chance to enter a prize draw for one of 10 gift vouchers worth 50 Saudi Riyals (approximately GBP 10.00) each. The study was publicised in February 2022 and remained open for approximately four months**.**

The study was approved by the Physical Sciences Ethics Committee at the University of York with the approval code (Aldaraani20211216).

4.2.6 Data Analysis

SPSS statistical software is used to analyse the quantitative data. Data was cleaned by removing incomplete responses or responses for participants who failed to pass the attention check question.

The rating data frequently failed to meet the assumption of normality (as assessed by Shapiro-Wilk tests) (Field & Hole, 2002), so non-parametric statistics were used.

For the open-ended question, the categories and coding definitions used here are similar to those described in Study 3 (see sections 3.3.5.1 and 3.3.5.2) developed based on participants' responses to open-ended questions regarding threat recognition and response.

4.3 Results

4.3.1 Frequency of Encountering Different Types of Threats

Table 4.3 presents the results of the analysis of the 12 scenarios. It shows the percentage (and number) of participants who reported having encountered similar threats to those in the scenarios and the median rating and SIQR of the frequency of encountering such threats.

The results revealed variations in participants' encounters with different online threats. The most common online threats were Malware and Phishing. 87 % of the participants experienced at least one of the scenarios related to Malware, while 71 % experienced at least one of the scenarios related to Phishing and Spear phishing. Data/Identity theft was less commonly reported than Phishing and Malware, with 40 % of the participants encountering at least one related scenario.

For Phishing and Spear phishing, the most frequently reported threat was spear phishing from seemingly trusted sources, such as banks, with over half of the participants (56 %) encountering this (S10). In contrast, the least encountered threat was spear phishing in which participants were impersonated to deceive their friends (S9). This contrast highlights the prevalence of threats exploiting trust in familiar sources versus the relatively rare experience of highly targeted impersonation.

Nearly half of the participants (47 %) experienced malware-related scenarios, including adware and malware links. In contrast, ransomware (S4) was the least encountered Malware, experienced by only 11 % of participants.

Spear phishing messages or calls from trusted sources (S10) and impersonation-based spear phishing (S11) have particularly high median ratings (5.0 and 6.0, respectively), indicating that when participants encountered these threats, they were encountered so frequently.

Table 4.3: Percentage of participants reporting that they had encountered threats related to each scenario, median rating (SIQR) frequency of encountering it (from "never" scored as 1 to "many times" scored as 7).

Scenario type/Instance	N (%) Participants encountering [1]	Median rating of frequency (SIQR)[2]
Phishing/Spear phishing	**32 (71 %)**	**5.0 (2.0)**
S9. Spear Phishing, impersonating participant	5 (11 %)	5.0 (2.00)
S10. Phishing msg/call, from a Trusted party	25 (56 %)	5.0 (1.75)
S11. Spear Phishing msg/call, impersonating someone	19 (42 %)	6.0 (2.0)
Malware	**39 (87 %)**	**5.0 (2.0)**
1. Malware, Link	14 (31%)	4.0 (2.1)
2. Malware, Attachment	17 (38 %)	5.0 (1.5)
3. Malware, Free App	15 (33 %)	5.0 (2.0)
4. Malware, Ransomware	5 (11 %)	3.0 (1.00)
7. Malware, Adware	21 (47 %)	4.0 (1.75)
8. Malware, Link phone	21 (47 %)	5.0 (2.0)
Data/Identity theft	**18 (40 %)**	**4.0 (1.5)**
5. Theft Bank Details	11 (24 %)	2.0 (1.5)
6. Theft Personal Information	7 (16 %)	5.0 (2.00)
12. Theft personal information, spoofed website	9 (20 %)	4.0 (2.25)
ALL SCENARIOS	**43 (96 %)**	1.0 (1.5)

1. For Scenario category, the number of participants encountering at least one of the scenarios in the category.
2. For Scenario category, based on all ratings of individual scenarios.

The results of the subsequent questions answered by participants who encountered particular threats are presented below in Tables 4.4 to 4.13.

4.3.2 Devices Where Online Threats are Encountered

The device types that participants reported they were using when they encountered threats similar to those in the scenarios are summarised in Table 4.4.

Laptops were the most frequently reported device type in malware-related scenarios, accounting for 50 % of the total 93 responses. In contrast, Data/Identity theft was more frequently reported while using phones, which accounted for 63 % of the 27 reported cases.

Many participants reported encountering malware threats mainly while using laptops, especially in scenarios S1, S2, and S7. In S7 (Adware), for example, 67 % of participants experienced the threat on a laptop. In S5, which involved stolen bank details, 82 % experienced the threat on their phones.

Across both Malware and Data/Identity theft scenarios, desktop and tablet use was less commonly reported as the device in use when the threat was encountered.

Table 4.4: Device types on which participants encountered online threats (frequency and percentage).

Scenario	N	Desktop	Laptop	Tablet	Phone	Not sure
Malware	**93**	**13 (14 %)**	**46 (50 %)**	**9 (10 %)**	**25 (27 %)**	**0**
S1	14	4 (29 %)	6 (43 %)	0	4 (29 %)	0
S2	17	1(6 %)	10 (59 %)	2 (12 %)	4 (24 %)	0
S3	15	2 (13 %)	5 (33 %)	3 (20 %)	5 (33 %)	0
S4	5	0	3 (60 %)	1 (20 %)	1 (20 %)	0
S7	21	3 (14 %)	14 (67 %)	2 (10 %)	2 (10 %)	0
S8	21	3 (14 %)	8(38 %)	1 (5 %)	9 (43 %)	0
Data/ Identity theft	**27**	**3 (11 %)**	**5 (19 %)**	**0**	**17 (63 %)**	**2 (7 %)**
S5	11	1 (9 %)	0	0	9 (82 %)	1 (9 %)
S6	7	2 (29 %)	1 (14 %)	0	4 (57 %)	0
S12	9	0	4 (44 %)	0	4 (44 %)	1 (11 %)

*N in the main threat type rows (e.g. *Malware, Data/Identity Theft*) refers to the total number of reported instances, which may include multiple responses from the same participant. N in the scenario-specific rows (e.g. S1, S2...) refers to the number of unique participants who experienced the threat in that specific scenario.

The prevalence of laptops in malware exposure suggests that traditional browsing and downloading remain the primary methods for such incidents. The high rate of identity-theft incidents on phones reflects the growing use of mobile applications for financial transactions and messaging, which may increase users' vulnerability to deceptive mobile communications. These trends show that threat exposure is heavily influenced by device-specific usage habits.

4.3.3 Sources of online threats

For the source of threats for Malware (Table 4.5), websites were the most frequently reported source of threats across multiple Malware-related scenarios (S1, S2, S3, S7, and S8). Notably, 86 % of participants in S7 (Adware) identified websites as the source of the threat, reinforcing the role of websites in malware distribution.

For Data/Identity Theft scenarios, websites were also the most frequently reported source of threat, accounting for 57 % of instances, as shown in Table 4.6.

In phishing and spear phishing scenarios, social media was reported frequently as a source of threat, accounting for 37 % of reported incidents, followed by phone calls (25 %). These findings suggest that social media platforms and phone calls might be prominent sources for phishing attempts (Table 4.7).

The source of threats across all scenarios is presented in Table 4.8. Websites emerged as the primary source of threats, particularly in Malware and Data/Identity theft scenarios. Specifically, 70 % of malware cases and 57 % of data and identity theft cases were linked to websites, which together accounted for nearly half (46 %) of all reported threat sources. In contrast, phishing threats were most commonly associated with social media messages. Surprisingly, across all scenarios, emails accounted for only 5 % of reported phishing threats.

Websites are a common source of malware. This may be because malicious scripts or downloads can be easily embedded within sites that appear legitimate. Users may also rely on superficial design cues to assess trustworthiness, without verifying the URL, security certificate, or the legitimacy of the source. The prevalence of social media as a vector for phishing and spear phishing suggests a shift from traditional email-based deception to personal messaging platforms, where attackers exploit familiarity, informality, and interpersonal communication styles.

Table 4.5: Source of threats in malware scenarios.

Source	S1	S2	S3	S4	S7	S8	All Malware
Website	8(57%)	12 (71 %)	11 (73)	2 (40)	18 (86)	15 (71)	66 (70)
App	2 (14)	1 (6)	1 (7)	2 (40)	2 (10)	2 (10)	10 (12)
Social media message	1 (7)	4 (24)	2 (13)	0	1 (5)	4 (19)	12 (15)
SMS	1 (7)	0	0	0	0	0	1 (1)
Not sure/ Don't know	2 (14)	0	1 (7)	1 (20 %)	0	0	3 (4)

Table 4.6: Source of threats in data and identity theft scenarios.

Source	S5	S6	S12[1]	All Data/ID Theft
Website	7(64 %)	2(29)	4(44)	13(57 %)
App	2(18)	1(14)	0	3(13 %)
SM Message	1(9)	1(14)	0	2(9 %)
SMS	0	1(14)	1(11)	2(9%)
Not sure/Don't know	1	2	-	3(13 %)

1. In S12, there is no question about the source of threats; the answers in this table were found in participants' answers to the last open-ended question.

Table 4.7: Source of threats in phishing and spear phishing scenarios.

Source [1]	S9	S10	S11	All Phishing
Email	1 (20 %)	2 (8 %)	5 (26 %)	8 (16 %)
Social Media Message	1 (20.0%)	6 (24.0%)	11 (57.9%)	18 (37 %)
SMS	0	5 (20 %)	2 (2 %)	7 (14 %)
Phone call	0	12 (48 %)	0	12 (25 %)
Not sure/Don't know	3 (60)		1 (5.3)	4 (8 %)

1. Options offered but never selected: App and Online account

Table 4.8: All data for sources of threats across all scenarios.

Source	Malware	Data/ID Theft	Phishing	All
Email	0	0	8 (16)	8 (5 %)
Social Media Message	12 (15)	2 (9)	18 (37)	32 (21 %)
SMS	1 (1)	2 (9)	7 (14)	10 (7 %)
Phone call	0	0	12 (25)	12 (8 %)

Source	Malware	Data/ID Theft	Phishing	All
Website	66 (70)	13 (57)	0	70 (46 %)
App	10 (12)	3 (13)	0	13 (9 %)
Not sure/Don't know	0	3 (13)	4 (8)	7 (5 %)

4.3.4 Consequences of Online Threats

Participants were also asked to select from a list of possible consequences of encountering situations similar to those presented in the scenarios. Tables 4.9–4.13 show the list of consequences selected, along with the percentage of participants who identified each consequence.

A device running slowly was the most frequently reported consequence across Malware-related scenarios, mentioned in 46 % of the reported cases. Followed by pop-ups in 30 % instances (Table 4.9). Notably, over 70 % of participants in S7 and S8, which were about adware and malware through links, also reported experiencing frequent and intrusive pop-ups.

In the Data and Identity Theft, the most common consequences for Theft bank details (S5) (Table 4.10), were financial loss. Nearly half of the participants (46 %) reported that they had lost money.

While in scenarios about theft personal information S6, over half (57 %) received annoying SMS messages or calls after the incident (Table 4.11). Additionally, in S12, 44 % of participants shared their personal information with a fraudulent website, highlighting the effectiveness of such threat in capturing sensitive data.

Within the Phishing and Spear phishing scenarios, one notable finding in S9 is that 60 % of participants reported that someone responded to the attacker, believing it was them (Table 4.12). This suggests that spear phishing can have not only personal but also social consequences, damaging trust and relationships. Furthermore, in S10 and S11, a significant number of participants either did not remember their response or chose "other," reflecting the uncertainty and confusion that often accompany phishing attacks (Table 4.13).

Table 4.9: Consequences of malware-related scenarios.

	Screen frozen	Device slow down	Device crashed	Strange pop-up
S1 N = 14	4 (29 %)	10 (71)	1 (7)	N/A
S2 N = 17	6 (35 %)	14 (82)	2 (12)	1 (6)
S3 N = 15	6 (40)	11 (73)	4 (27)	N/A
S4 N = 5	N/A	N/A	N/A	N/A
S7 N = 21	0	12 (57)	2 (10)	15 (71)
S8 N = 21	0	0	0	15 (71)
Total $N_{mention}$= 103	16 (16 %)	47 (46 %)	9 (9 %)	31 (30 %)

Option in S4: I could not access any of my files selected by 2 (40%); Paid the requested ransom, selected by 1 (20%)
Option in S7: browser homepage changed, selected by 3 (14.3%)
Option in S8: unknown app/software installed, selected by 6 (28.6%)
Option Not sure/can't remember was selected by 5 participants across all Malware scenarios.

Table 4.10: Consequences of data/identity theft, S5 (theft of bank details).

	Lost money	**Could not use a credit card**	**Bank account was overdrawn**
S5 N = 11	5 (46 %)	2 (18 %)	1 (9 %)

*Not sure/can't remember was selected by 2 (18.2) in S5

Table 4.11: Consequences of data/identity theft-related scenarios, S6 and S12.

	Stolen identity	**Annoying SMS/calls**	**Handed over the data**	**Device infected**
S6 N = 7	2 (29 %)	4 (57 %)	N/A	N/A
S12 N = 9	1		4 (44 %)	3 (33 %)

*Not sure/can't remember was selected by 1 (14.3%) participant in S6

Table 4.12: Consequences of phishing/spear phishing-related scenarios, S9.

	Friend was upset	**Many received message**	**Someone responds without verifying**
S9 N = 5	1 (20 %)	1 (20 %)	3 (60 %)

* Not sure/can't remember was selected by 3 (60.0)

Table 4.13: Consequences of phishing/spear phishing-related scenarios, S10 and S11.

	Respond to the request	**Could not access account**	**Personal info. used**	**Malware was downloaded**
S10 N = 25	1 (4 %)	2 (8 %)	2 (8 %)	2 (8 %)
S11 N = 19	6(32 %)	0	0	0

* Option offered in S11 but never selected: I sent money to the fraudulent person
* Not sure/can't remember was selected by 18 (72) in S10 and 11 (58 %) in S11

These results show that some online threats, such as malware, result in temporary device disruption or inconvenience, whereas others, such as data or identity theft and spear phishing, and lead to financial or interpersonal impacts that extend beyond device-level harm.

4.3.5 Participants' Accounts of a Memorable/Recent Online Threat Incident

Participants were asked in an open-ended question to briefly explain a memorable/recent incident of the type of online threat, including what actions they took, how they realised something was wrong, and how they tried to solve the problem.

In all, 29 (64 %) out of 45 participants answered one or more of the open-ended questions in the 12 scenarios. In total, there were 60 answers out of 169 opportunities, so 36 % of relevant scenario reports included an answer to this question (Table 4.14).

Table 4.14: No. of answers provided by the participants to the open-ended question.

Scenario Type	Scenario No	N participants	N answers	% answers
Malware	S1	14	4	29
	S2	17	5	29
	S3	15	1	7
	S4	5	0	0
	S7	21	4	19
	S8	21	5	24
Data/Identity Theft	S5	11	5	46
	S6	7	3	43
	S12	9	5	56
Phishing/Spear Phishing	S9	5	2	40
	S10	25	15	60
	S11	19	11	58
Total No of Answers			60	

A code dictionary was created based on the participants' answers. The analysis was organised into three main topics: Threat detection, Solutions and adequacy of solutions. Tables 3.17 in Section 3.3.5.1 provide the definitions for all categories and subcategories of Threat Detection Cues used in this study.

4.3.5.1 Participants' Descriptions of Threat Detection Cues

Table 4.15 shows the coding results of participants' responses on how they detect threats, with some examples from participants' answers. Device performance was mentioned frequently across Malware-related scenarios, followed by a suspicious design. For Data/Identity Theft, unusual transactions were the most frequent cues mentioned in S5, which was about stolen bank details. The request type was another important cue used by the participants to detect phishing messages or calls and spoofed websites.

Table 4.15: Threat detection cues used by participants.

Scenario no. short name	Detection methods: N (%)	Example answers
Malware		
S1. Malware Link N = 4	Device performance: 3 (75%) Notification: 1 (25%)	Device performance: my device was slowed down because I downloaded some files from some websites (P4) Notification: A recruitment link, and when I clicked on it, it asked for my mobile number. After that, I received a notification from the telecom company saying I have an outstanding balance of 35 Saudi Riyals. (P37)
S2. Malware Attachment N = 5	Device performance: 3 (60%) Suspicious design: 2 (40%) Not clear: 1 (20%)	Device performance: "An Excel file sent to me by e-mail was downloaded, and when it was downloaded, the device was very slow until I removed the file (P44) Suspicious design: I clicked on a link that seemed to take me to a recent news article or information. After that, my device started displaying icons for annoying advertisements, and it began to operate very slowly (P29)
S3. Malware Free App N = 1	Device performance: 1	Device performance: I used to receive alert messages in the calendar saying that my device was at risk, had been infected with a virus, and that my data would be deleted and the device formatted within minutes. (P27)
S7. Malware/Adware N = 4	Suspicious design: 3 (75%) Device performance: 1 (25%)	Suspicious design: I had to install a protection program on the device but it did not prevent pop-ups for ads from appearing which continue to appear when logging in to the browser (P19) Device Performance: I downloaded antivirus software from a website and my device was negatively affected by those programs. (P41)

Scenario no. short name	Detection methods: N (%)	Example answers
S8. Malware Link (phone) N = 5	Suspicious design: 2 (40 %) Sending spam messages: 1 (20 %) Not clear: 2 (40 %)	Sending spam messages: "I found that users were added to my Twitter account and tweets were sent from my account (P25) Suspicious design: A movie website has shown frequent and disturbing ads (P41)
Data/Identity Theft		
S5. Theft Bank Details N = 5	Unusual purchases or transactions: 4 (80%) Not clear: 1 (20 %)	Unusual transactions: Someone contacted me for a working contract and asked to send a password that will be sent to my phone number, once I told him the password he was able to withdraw all the amount I have in my bank account (P43)
S6. Theft Personal Info N = 3	Being impersonated: 1 (33 %) Not clear: 2 (67 %)	Being impersonated: saved my national ID and my job-related information on the work device which was accessed by many employees, which made it easy to be compromised. (P29)
S12. Theft personal info. Spoofed website N = 5	Request for personal information: 2 (40 %) Wrong or suspicious content: 1 (20 %) Poorly constructed message: 1 (2 %) Suspicious design: 1 (20 %) Not clear: 1 (20 %)	Poorly constructed: I realised while entering my information that the site is not professional and has several spelling mistakes that made me doubt and realise it's fake (P29)
Phishing/Spear phishing		
S9. Spear Phishing (impersonating participant) N = 2	Not clear: 2	Not clear: Email has been hacked, I think the reason for this is that I use the same email to register on many different sites (P29)
S10. Phishing msg/call (from a Trusted party) N = 15	Request for personal information: 3 (20 %) Common threat type: 2 (13 %) Suspicious or Wrong content: 2 (13 %) Poorly constructed message: 1 (7 %) Being impersonated: 1 (7 %) Not clear: 6 (40 %)	Request for personal info.: A phone call claiming to be from one of the telecommunication companies with Internet offers and packages. She asked me to send her a password I received but I refused (P1) Common threat type: I received a message that looked like it was from a delivery company, but it was clearly fake, so I didn't enter my information. (P12) Being impersonated: received a job recruitment message, and when contacted the source of the message via WhatsApp, they requested some of her personal information. Using her details, they accessed *Absher* account (a Saudi government e-portal for managing personal and official services) and issued SIM cards. (P44)

Scenario no. short name	Detection methods: N (%)	Example answers
S11. Spear Phishing msg/call (impersonating someone) N = 11	Request for personal information: 2 (18 %) Common threat type: 1 (9 %) Not clear: 8 (73 %)	Request type: I received a message from someone requesting a money transfer, and I immediately realized it was a scam (P9) Common threat type: I am aware of the issue and act by deleting and blocking the sender. (P22)

* No answers to S4, which was about Malware, Ransomware

4.3.5.2 Participants' Descriptions of Solutions to Threats

The solutions that participants reported they used when they encountered threats are presented in Table 4.16. A small number of participants (ranging from 3 to 15 per scenario) provided answers describing the actions they took to resolve online threats. Table 4.16 presents the responses where participants described solutions. Notably, several participants in phishing-related scenarios (S10 and S11) stated that no action was needed because they recognised the threat early and chose not to interact with it, which aligns with best cybersecurity practice.

Table 4.16: Solutions followed by participants in the 12 scenarios.

Scenario	Solutions	Example
Malware		
S1 N = 4 (1 included one solution)	Seek human help /advice	A fake link to announce some fake prizes was clicked by mistake, so the device became slow and did not respond to commands. The problem was solved by a computer technician (P41)
S2 N = 5 (2 included one solution each)	Delete/uninstall: 1 Close/Quit/Restart: 1	Close/Quit/Restart: I tried to solve the problem by shutting it down completely and restarting it (P32)
S8 N = 5 (1 with one or more solutions)	Changed details on online accounts	Then I retrieve my Snapchat through email, and I change all accounts' passwords (P35)

Scenario	Solutions	Example
Data/Identity Theft		
S5 N = 5 (2 included one or more solutions)	Card/payment cancelled: 1 Changed details on online accounts: 1	Card cancelled: they withdrew a financial amount and renewed my subscription forcibly without my consent because they retained my banking card information. This led me to cancel my credit card and issue a new one (P29) Change details: The only solution I did was to remove the card and erase its information from all websites and applications (P9)
S6 N = 3 (1 with one solution)	Warn others/report	I tried to contact the app developers, but I didn't find an answer. (P41)
S12 N = 5 (2 with one or more solutions)	Card/payment cancelled: 1 Warn others/report: 1 Changed details on online accounts: 1	Change details: I realised at the time that my bank information had been hacked, so I changed my username and password immediately (P19) Card cancelled & Report problem: I immediately suspended all my cards and I contacted the bank immediately (P2)
Phishing/Spear phishing		
S10 N = 15 (2 with one or more solutions)	No solution as there is no interaction with threats: 11 Warns others/report: 1 Blocked Popups: 1 Changed details on online accounts: 1 Not clear: 2	Changed details on online accounts & Blocked pop ups: I realised that it was a fraud message I deleted my data and blocked the message (P27)
S11 N = 11 (6 with one or more solutions)	No solution as no interaction: 5 Blocked/confronted popups/attackers: 6 Delete or uninstall: 1 Warn others/report: 1	Blocked/confronted popups/attackers: Block the address and delete the email from the list. (P18) Warn others/report: I blocked and reported the sender (P30)

* Scenarios S3, S7, and S9 were excluded from the table, as the answers provided did not include any description of how the threat was addressed.
* No answer was given to S4.

4.3.5.3 Adequacy of Participants' Attempts and Solutions

Then the adequacy of participants' solutions was assessed by comparing them with the set of recommendations provided by security experts (See Section 3.3.5.3). Table 4.17 shows the number of adequate solutions in each scenario.

The adequacy of solutions provided to all scenarios was 78 % for all scenarios. This high percentage should be interpreted with caution due to the limited number of responses. only a small number of participants provided open-ended responses, with a small number of adequate solutions can result in a relatively high adequacy percentage. Additionally, this may be partly explained by the fact that for many online threats, there are multiple viable and appropriate responses**,** such as cancelling the card, changing details or contacting the service provider, all of which align with expert recommendations

The number of answers received from participants to this question in each scenario was limited, with no answer given to one scenario (S4). In other scenarios, participants wrote about the threats but did not include details about what they did to solve the problems (S3, S7 and S9).

In malware-related scenarios, particularly S1, S2, and S8, the majority of participants who responded did not report any clear solution, and where solutions were provided, only one or two were adequate. This pattern was similar in data and identity theft scenarios (S5, S6, S12), where the number of responses remained small, but a few participants provided appropriate responses, such as contacting banks or cancelling cards. Interestingly, phishing-related scenarios (S10, S11) showed a slightly higher number of responses, particularly in S11, where more than half of the participants who responded described actions that were considered adequate, such as blocking and reporting the sender.

For Phishing scenarios, in S10, although 25 participants encountered the threat, only two described how they solved it, both of which were adequate. Notably, 11 participants stated that they recognised the threat and chose not to engage, meaning that no further action was necessary. As one participant (P29) explained: *"I did not respond and I ended the call immediately".* A similar pattern appeared in S11**,** where five participants also reported recognising and avoiding the threat without needing to take further steps.

Table 4.17: Assessment of adequacy of participants' solutions addressing the security threats.

Scenario	N (%) of answers with and without solutions	Adequacy of the solution	Examples
Malware			
S1 N = 4	With solutions: 1 (25%) Without solution: 3 (75%)	Adequate solution: 1	The device became slow and unresponsive. The problem was solved by a computer technician (P41)
S2 N = 5	With solutions: 2 (40%) Without solution: 3 (60%)	No adequate solution	I realised something was wrong when the tablet did not respond. At first, it became slow, and then it did not respond to anything. I tried to solve the problem by shutting it down completely and restarting it. (P32)
S8 N = 5	With solutions: 1 (20%) Without solution: 4 (80%)	Adequate solution: 1	Then I retrieve my Snapchat through email, and I change all accounts' passwords (P35)
Data/Identity Theft			
S5 N = 5	With solutions: 2 (40%) Without solution: 3 (60%)	Adequate solutions: 2	They withdrew a financial amount and renewed my subscription without my consent because they retained my banking card information. This led me to cancel my credit card and issue a new one. (P29)
S6 N = 3	With solutions: 1 (33 %) Without solution: 2 (67 %)	Adequate solution: 1	Found out that a sum had been deducted from my account through the application, and I tried to contact the app developers (P41)
S12 N = 5	With solutions: 2 (40%) Without solution: 3	Adequate solution: 1	However, when it insisted on accessing my personal account and obtaining my password, I immediately cancelled all my cards and contacted the bank (P2)
Phishing			
S10 N = 15	With solutions: 2 (13 %) Without solution: 13 (87 %)	Adequate solutions: 2	They requested some of her personal information. Using her details, they accessed her *Absher* account (a Saudi government e-portal for managing personal services) and issued SIM cards in her name. A report was filed through the *Kulna Amn* App (App for reporting crimes) (P44)
S11	With solutions: 6 (55 %)	Adequate solution: 6	I immediately realised it was a scam. Nothing happened to my

Scenario	N (%) of answers with and without solutions	Adequacy of the solution	Examples
N = 11	Without solution: 5		device, and the solution I took was to block their number (P9) I ignored the message and I blocked and reported the sender (P30)

4.3.6 Participants' General Worries about Online Threats and their Relationship to their Experiences of Online Threats and Computer and Security Competencies

Table 4.18 presents participants' ratings of the level of worry on the 9 statements. The participants' level of worry ranged from slightly below the midpoint of the 7-point scale (with a median of 3.0 for two statements about phishing) to relatively high (median of 5.0 for statements about data and identity theft).

Only one statement about phishing ("I will receive a phone call from someone asking about my confidential data" e.g. password, bank account details) was significantly below the midpoint (4.0), indicating that participants reported significantly low worry level for this statement about phishing.

Table 4.18: The worry statements measuring the level of worry about online security threats.

Threat type/Statements	Median (SIQR)	Z Score	p-value
Malware			
Someone will lock me out of my device(s) and demand money to restore access	4.0 (3.00)	-0.14	0.88
Someone will access my device(s) or account(s), look at my information and use it to blackmail me	4.0 (2.75)	-0.30	0.75
Data/Identity Theft			
My device will be accessed by an attacker and my data will be destroyed	4.0 (2.50)	-0.10	0.92
Someone will steal my online identity and misuse it	5.0 (3.00)	0.42	0.67
Someone will access my device(s) or account(s), steal my data and use it for malicious purposes or to their advantage (e.g. make illegal purchases)	5.0 (2.25)	1.23	0.21
Phishing/Spear phishing			
I will receive an email with a link leading to a fake website	4.0 (2.00)	-1.21	0.22
I will receive an email with an attachment that may include malicious code	4.0 (2.00)	0.26	0.79
I will receive a phone call from someone asking about my confidential data (e.g. password, bank account details)	3.0 (1.75)	-3.28	0.001
I will click on a link in a SMS message or email from a source that I cannot verify its origin, whether it is trustworthy	3.0 (2.25)	-1.61	0.10

A principal components analysis (PCA[4]) was conducted on the ratings to investigate whether they formed meaningful groups for the participants. The PCA revealed two components that accounted for 73.7% of the variance (see Table 4.19). The first component was Theft Worry, accounting for 60.6% of the variance and included five statements. The second component was the Phishing Worry, which accounted for 13.3% of the variance and included three statements.

Table 4.19: Principal component analysis (PCA) of online threat worries.

[4] As there were nine statements, 45 participants constituted a sufficient sample for a PCA.

Component	% Variance
THEFT WORRIES	60.6%
My device will be accessed by an attacker and my data will be destroyed Someone will lock me out of my device(s) and demand money to restore access Someone will access my device(s) or account(s), look at my information and use it to blackmail me Someone will steal my online identity and misuse it Someone will access my device(s) or account(s), steal my data and use it for malicious purposes or to their advantage (e.g. make illegal purchases)	
PHISHING WORRIES	13.3%
I will receive an email with a link leading to a fake website I will receive a phone call from someone asking about my confidential data (e.g. password, bank account details) I will click on a link in a SMS message or email from a source that I cannot verify its origin, whether it is trustworthy	

The median scores on these components were calculated for each participant to investigate the relationship between the two major worry areas and experience with online threats, as measured by the number of threats they reported experiencing and how frequently they experience them, and self-reported computer and security knowledge and ability in identifying security threats (computer and security competencies).

There was no significant relationship between the scores on either component and their experience of online threats (Theft Worry: $r = 0.18$, $p = 0.24$; Phishing Worry: $r = 0.02$, $p = 0.88$). There was no significant relationship between Theft Worry and self-reported ratings (computer expertise: $r = -0.15$, $p = 0.34$; online security knowledge: $r = -0.17$, $p = 0.25$; identifying attacks: $r = -0.19$, $p = 0.20$). However, there was a significant relationship with Phishing Worry, which had significant, if small, negative correlations with Computer knowledge ($r = -0.33$, $p = 0.025$) and with online security knowledge ($r = -0.29$, $p = 0.05$) but no relationship with the ability to identify security attacks.

A linear regression was performed to predict worry scores from how frequently participants had experienced online threats**.** The result of the Theft Worry component was not significant **(**$F(1,43) = 2.481$, $p = .123$), indicating that the frequency of experiencing threat does not significantly predict worries about theft-related threats. The result for Phishing Worry Component was not statistically significant ($F(1,43) = 0.048$, $p = 0.828$), suggesting that the frequency of experienced attacks does not predict phishing-related worries**.**

Linear regressions were conducted to predict Worries scores from the ratings of the frequency of experiencing each of the different scenarios. The result for S4 (which is about malware/ransomware) was significant ($F(1,43) = 4.932$, $p = 0.032$), with participants who had experienced ransomware reporting higher Theft Worry scores. Similarly, the result of S6 (which is about theft of personal data) was also significant ($F(1,43) = 5.713$, $p = 0.021$).

The result for the Phishing Worry Scores were not significant in all scenarios.

4.3.7 Participants' Self-Reported General Security Behaviour (SeBIS) and its Relationship to their Experiences of Online Threats and Computer and Security Competencies

The original SeBIS subscales were used to assess the participants' self-reported security behaviours (Table 4.20).

A Wilcoxon signed-rank test was conducted to compare the SeBIS subscale scores of the current Saudi sample with the normative means reported by Egelman and Peer (2015). After adjusting for scale differences, participants in this sample scored significantly higher on Device Securement than the normative mean, and also significantly higher than the midpoint of the scale.

In contrast, scores for Password Generation were significantly lower than the normative mean but did not differ significantly from the scale midpoint. For Proactive Awareness, no significant difference was found compared to the normative mean, though the sample scored significantly higher than the midpoint. Finally, Updating scores were significantly lower than both the normative mean and the scale midpoint, indicating that this area may be a notable weakness among participants.

Table 4.20: Means for the SeBIS subscales, with comparison with the standard scores from Egelman and Peer (2015) and with the midpoints of the scale.

Subscale	Egelman and Peer Mean[1]	Current sample Mean (SD)	Adjusted mean[2]	Comparison with Egelman and Peer	Comparison with midpoint
Device Securement	3.21	5.7 (1.43)	4.1 (1.02)	$Z = 4.5$, $p < 0.00$	$Z = 5.2$, $p < 0.00$
Password Generation	3.25	3.9 (1.08)	2.8 (0.77)	$Z = -2.8$, $p = 0.005$	$Z = -0.33$, n.s.
Proactive Awareness	3.73	4.9 (1.20)	3.6 (0.86)	$Z = -0.51$, n.s.	$Z = 4.31$, $p < 0.00$
Updating	3.47	4.0 (1.56)	2.8 (1.11)	$Z = -3.1$, $p = 0.002$	$Z = -4.8$, n.s.

1. Egelman and Peer (2015) only provide mean scores for individual items in SeBIS, not the subscales. So I calculated the mean score for each subscale, but this means I cannot calculate the SD for each subscale in their sample
2. I used a 1–7 scale; the original SeBIS used a 1–5 scale, therefore, these are the subscale scores adjusted to a 1–5 scale to allow comparison with the original SeBIS results by multiplying by 0.714.

Table 4.21 presents the result of the correlation between participants' SeBIS scores and their self-rated computer and security competencies.

Password Generation was significantly correlated with all three self-rated competencies: computer knowledge, security knowledge, and the ability to identify attacks. Proactive Awareness was significantly related to both security knowledge and the ability to identify attacks, but not computer knowledge. Updating was significantly correlated only with computer knowledge.

Table 4.21: Correlation between SeBIS subscales and computer and security competencies.

	Computer knowledge	Security knowledge	Ability to identify the attack
Device Securement			
Password Generation	r = 0.43, p = 0.003	r = 0.49, p < 0.00	r = 0.35, p = 0.01
Proactive Awareness		r = 0.42, p = 0.003	r = 0.39, p = 0.008
Updating	r = 0.34, p = 0.02		

Table 4.22 presents the relationship between participants' SeBIS scores and their experiences of online threat in the 12 scenarios. The goal was to determine if higher self-reported security behaviour correlated with reduced exposure to online threats. A significant positive correlation was found between the Password Generation and threat experience (r = .503, p < .001), indicating that participants with high scores in secure password practices reported higher online threat experiences. No significant correlations were found between threat experiences and the other subscales.

Table 4.22: Correlation results of SeBIS subscales with experience of online threats.

	Device Securement	Password Generation	Proactive Awareness	Updating
Experience of threats	n.s	r = 0.50, p < 0.000	n.s	n.s

The correlation between SeBIS scores and both worry components was examined. Table 4.23 presents the result. Proactive Awareness was negatively correlated with both worry components. No significant correlations were observed between the worry components and the other SeBIS subscales.

Table 4.23: Correlation between the SeBIS scores and worry components.

	Device Securement	Password Generation	Proactive Awareness	Updating
Phish worry			r = -0.35, p = 0.01	
Theft worry			r = -0.34, p = 0.02	

4.4 Comparison of the UK and KSA Younger Adults' Experiences and Responses to Online Threats

This section provides a comparison between the UK and KSA samples, highlighting key similarities and differences observed across the two studies.

4.4.1 Sample Characteristics and Self-Rated Expertise

Although I tried to recruit very similar samples in the two countries, there are some differences were observed between the UK and KSA participants (see Table 4.24). The UK sample was larger, with a younger mean age, whereas the Saudi sample was somewhat better educated (with a higher percentage of participants with a degree or higher degree). This may be partly due to the difference in the age distribution between the two samples. However, the educational level difference was

considered to be an important difference, as some studies have shown educational level to be an important factor in this area (Lyon, 2023).

Both samples rated their computer expertise as above average. However, the UK sample rated their computer security expertise and their ability to identify online attacks as above average, whereas the Saudi sample rated these as only average. These differences in ratings may also be related to cultural differences in rating one's own skills (He et al., 2017).

Table 4.24: Participants' demographic characteristics for Studies 1 and 2.

	British sample	**Saudi sample**
Sample size	81	45
Mean age (18–30)	24	27
Highest Educational Level		
High school	35 %	16 %
Bachelor's degree	42 %	62 %
Postgrad degree	19 %	22 %
Other	5 %	-
Self-reported computer expertise Median (SIQR) Z score (probability)	 5.0 (0.5) 6.25 ($p < 0.001$)	 5.0 (1.5) 3.52 ($p < 0.001$)
Self-reported computer security knowledge Median (SIQR) Z score (probability)	 5.0 (1.0) 4.90 ($p < 0.001$)	 4.0 (1.0) 0.14 ($p = 0.89$)
Self-reported ability to identify online attacks Median (SIQR) Z score (probability)	 5.0 (1.0) 1.52 ($p < 0.001$)	 5.0 (1.5) 1.52 ($p = .129$)

4.4.2 Frequency and Types of Online Threats Encountered

For the frequency of encountering threats, nearly all participants in both countries experienced at least one security threat (95 % and 96 %). The Saudi sample reported higher encounters with Malware (87 %) compared to the British sample (74 %). Phishing encounters were slightly higher in the UK (77 %) than in KSA (71 %).

Interestingly, Data/Identity Theft was reported more frequently in the KSA (40 %) compared to the UK sample (30 %). A chi-square test was conducted to test if the difference between the two samples was significant, but this was not the case χ^2 (1, N = 126) = 1.07, p = .30), indicating no meaningful difference in reported Data/Identity Theft between the two groups.

4.4.3 Worry and Perceived Severity of Threats

Participants in both the UK and KSA reported higher levels of worry about data and identity theft than about phishing, despite phishing being more frequently encountered. This pattern suggests a shared perception that data and identity-related threats are associated with more severe or long-lasting consequences. Although phishing was reported more often, it appeared to generate lower

levels of concern, whereas less frequent threats involving personal data or identity were perceived as more consequential. Taken together, these patterns suggest that worry may be influenced not only by the frequency of threats encountered but also by users' perceptions of potential impact.

4.4.4 Detection, Response and Reporting Behaviours

In both countries, participants demonstrated greater confidence in recognising and avoiding phishing and spear phishing than in identifying technical threats such as malware. Avoidance, such as ignoring suspicious messages, was commonly reported as an effective response to phishing in both samples. However, malware and identity-related threats were more likely to be recognised after negative consequences had occurred. Reporting behaviour was limited in both contexts, with relatively few participants escalating incidents to service providers or official authorities. These similarities suggest shared challenges in recognising some online threats early and in engaging with formal reporting mechanisms.

4.4.5 Security Behaviour Intentions (SeBIS)

Comparison of self-reported security behaviour intentions revealed both similarities and differences between the two samples. Participants in both countries reported relatively strong intentions in areas such as device securement, suggesting engagement with basic protective practices. In contrast, weaker intentions were observed for behaviours requiring ongoing effort, such as updating and strong password practices, particularly in the KSA sample. In both samples, self-reported security knowledge was associated with stronger security behaviour intentions, highlighting the role of perceived knowledge and confidence in shaping intended secure behaviour. Overall, these findings suggest that while younger adults in both contexts express intentions to engage in some protective practices, gaps remain in some technical or maintenance related aspects of security.

4.5 Discussion

This study investigated the types of online threats experienced by younger adults in KSA, how these individuals detect and respond to such threats, their levels of worry, and their self-assessed computer and cybersecurity competencies. The same online scenario-based survey was used to explore these issues in depth as had been used in the UK study reported in the last chapter. Participants were presented with a range of threat scenarios, asked to reflect on similar experiences, and report how they recognised and dealt with those threats. The study also included a standardised scale to measure security behavioural intentions (SeBIS) and examined how these related to threat experience and knowledge.

The findings indicated that malware, phishing, and spear phishing were the most frequently reported threats, particularly in scenarios involving deceptive messages or calls from seemingly trustworthy sources, and adware.

While participants generally rated themselves highly in computer knowledge, their ratings for security expertise and threat identification were more moderate. No significant correlation was found between threat experience and self-rated competencies, but higher security knowledge was correlated with lower worry about phishing. Participants often detected malware and identity theft reactively, usually after experiencing negative consequences, whereas phishing was more likely to be proactively recognised and avoided before any harm occurred. Online security behavioural intention

scores on the SeBIS were highest for Proactive Awareness (e.g. avoiding suspicious links), but weakest for keeping device Updating, suggesting an uneven adoption of good security practices.

Reflecting on the scope of the research questions in this phase, it is clear that they effectively captured the types and frequency of online threats encountered by younger adults in the KSA. The inclusion of self-reported measures of computer and security knowledge offered insight into participants' perceived awareness. However, the findings suggest that focusing on experience and self-assessment alone may not fully reveal how prepared or resilient Saudi younger adults feel when facing these threats. While the RQs were appropriate for investigating exposure and behavioural responses, future research should extend them to include dimensions of security capability and the contextual factors that enable or hinder digital resilience, such as educational background, cultural norms, and access to cybersecurity support services. This broader approach would provide a more comprehensive understanding of how younger adults build and maintain readiness to deal with online threats.

Turning to the research questions:

RQ1: What are the types and frequency of online threats experienced by young adults in Saudi Arabia?

In this sample, nearly all participants reported experiencing at least one malware-related scenario, while nearly three-quarters encountered at least one phishing-related scenario, including spear phishing. These figures indicate that malware and phishing remain prevalent threats among young Saudi users. This agrees with broader threat landscape reports. For instance, McAfee data presented in a study by Alhashim and Hafizur Rahman (2021) showed that malware accounted for 35% of all reported cyberattack vectors**,** making it the most prevalent threat category. This supports the high frequency of malware-related scenarios reported by participants in the current study. Another study by Alzubaidi (2021) conducted an online survey with 1,230 Saudi participants aged 18 and over found that over 500 participants had experienced malware threats, suggesting widespread exposure among Saudi users.

Phishing-related scenarios were among the most frequently reported in this sample, consistent with global trends that identify phishing as a dominant cyber threat. According to the Anti-Phishing Working Group (APWG), 877,536 phishing attacks were observed worldwide in just the second quarter of 2024. Also, many studies found that phishing is still one of the most prominent attacks targeting users in KSA (Aljeaid et al., 2020; Alyahya & Weir, 2021).

Previous studies have also highlighted the prominence of phishing in KSA, although often across broader age ranges. For example, the study by Alzubaidi (2021) also reported that more than half of the participants had received phishing emails. Similarly, Alotibi (2016) reported that many Saudi users received phishing emails, suggesting persistent exposure to such threats. However, both of these studies included participants beyond the young adult age range, making the current findings particularly valuable in highlighting threat exposure within a younger demographic. In particular, over half of the participants reported experiencing phishing messages that appeared to come from trusted sources. This supports previous research showing that phishing tactics have shifted from mass emails sent to random targets to more personalised attacks that specifically target individuals (Alkhalil et al., 2021).

The next key area of analysis for RQ1 was the source of threats. Participants frequently reported websites as a primary source of online threats, particularly for Malware and Data/Identity Theft-related scenarios. For example, websites were the most common source for adware and stolen bank details. This trend underscores the pervasive risk that websites pose as a source for malware, potentially due to the ease with which malicious content can be embedded or shared on trusted-looking sites (Peng et al., 2019; Samarasinghe & Mannan, 2021).

Social media was commonly reported by the participants as a source for Phishing and Spear phishing. This agrees with what was found by the APWG (Phishing Activity Trends Report 2nd Quarter 2024, 2024) that social media has become the most frequent attack sector.

In relation to the type of device that was being used during the threat experience, laptops and phones were the most commonly used devices, especially when participants encountered Malware and Data/ID theft. This result is supported by a report from KSA, which found that 82% of individuals aged 12–59 use the Internet, with 92% accessing it via mobile phones (General Authority for Statistics, 2018). The high prevalence of mobile device usage suggests that users may be particularly vulnerable to phone-based spear phishing. In this study, participants reported that calls or messages from what seemed familiar were very common. Phone fraud was also found to be reported as common in the UAE, reflecting a trend in the region. This shows that attackers are increasingly using mobile communication channels in this region (Shah et al., 2023).

RQ2: How do younger KSA adults detect and respond to online threats?

Moving to the second research question, which investigated the detection methods and responses followed by younger KSA adults. Participants reported different cues to recognise phishing and malware threats. In malware-related scenarios, participants often reported recognising the threat only after experiencing its negative effects, such as device slowdowns, crashes, or pop-up messages. Similarly, in data and identity theft scenarios, participants typically reported becoming aware of the threat after observing consequences like suspicious transactions. This suggests a generally reactive approach to these types of threats, where detection is driven by visible impact rather than early recognition (Onyewuchi Ofoegbu et al., 2024).

In contrast, participants showed a more proactive approach in their reports of recognising phishing and spear phishing threats. Some participants reported identifying common cues, such as requests for personal information. These findings agree with prior research indicating that the presence of sensitive information requests is a common cue for phishing emails (Downs et al., 2006; Furnell, 2007; Steves et al., 2020).

The distinction between reactive and proactive approaches was particularly evident in Scenarios 10 and 11, where many participants reported not interacting with that kind of threat and therefore took no further action. In Scenario 10, for example, 11 out of 15 participants who responded said in a situation like that, they ignored the phishing message because they recognised it as fraudulent. Similarly, in Scenario 11, several participants reported recognising and avoiding that kind of threat. While this may appear as a lack of action, it actually reflects an effective way to respond to phishing threats, which is in line with security best practices that recommend not clicking, responding, or engaging with suspicious content.

These findings highlight that while participants may struggle to detect technical threats such as malware without visible consequences, they are better equipped to recognise social engineering threats like phishing, which present more familiar and accessible warning signs. However, as previous research has shown, non-experts still often lack the deeper knowledge required to fully understand or mitigate threats (Nthala & Wash, 2021) and may prioritise returning to their tasks over taking appropriate security measures.

One possible reason for participants' inaction after encountering some types of online threats, such as malware, may be the difficulty of accessing security-related information. Previous research highlights the fact that many online platforms provide their security and privacy policies only in English and often at a literacy level that can be challenging for non-native English speakers to understand (Vashistha et al., 2018). Although the participants in this study are not necessarily low-literate, language barriers and the complexity of technical jargon may still hinder their ability to fully understand online security guidelines. However, as there were few responses to this question, this may need further exploration.

Another notable finding is that only in four responses, participants reported threats to service providers, with only one of them mentioned reporting threats to cybersecurity authorities. Despite the existence of official reporting channels for individuals, which enable users to report cyber incidents confidentially via email or government portals. However, prior research indicates that such reporting mechanisms may not be widely known to the public (Rashed Albediwi & Sadaf, 2023). Similarly, Alotaibi et al. (2016) found that many of the individuals who had been targeted by cybercrime did not report the incident.

Although many participants demonstrated the ability to recognise and ignore phishing or spear phishing attempts, which reflects a practical level of security capability, the reported consequences also suggest that this preparedness is uneven. Some participants still experienced financial loss, impersonation, or account compromise, indicating that not all younger adults were equipped to protect themselves effectively when facing threats that required more than avoidance or basic troubleshooting. Moreover, the very limited reporting behaviour highlights a lack of confidence or awareness regarding formal escalation channels, suggesting that resilience is shaped not only by the ability to detect threats but also by familiarity with support mechanisms and security procedures. Future work could therefore explore preparedness, examining not just behavioural responses, but also users' confidence, knowledge, and access to effective support when threats occur.

RQ3: What are the levels of worry about online threats among young adults in the KSA, and how are these levels related to their experiences of such threats?

The third research question investigated the levels of worry younger KSA adults had about threats. Participants were more worried about data and identity theft than phishing, even though phishing was experienced more frequently. This suggests that the participants did not fully understand the consequences of phishing attacks, or they may believe that the consequences of data or identity theft are more severe or long-lasting compared to those of phishing attacks. Previous studies have indicated that the perceived severity of a risk is a strong predictor of how individuals perceive that risk (van Schaik et al., 2017).

The relationship between worry and the experience of threats was not consistent across threat types. For example, participants reported high levels of worry about identity theft, even though it

was encountered less frequently than phishing, suggesting that worry may be influenced more by the perceived severity of consequences than by actual exposure.

Interestingly, participants who rated their security and computer knowledge higher were less worried about phishing attacks. This result supports previous research that found cybersecurity expertise helps individuals to detect social engineering attacks (Albladi & Weir, 2020) and may explain why participants with high levels of cybersecurity knowledge did not worry about phishing attacks compared to those with lower levels. A similar study by Alanazi et al. (2022) with a KSA sample and similar age group (18–30 years) found that knowledge of potential cyber threats influenced participants' online security awareness.

RQ4: What are the security behaviour intentions of younger adults in the KSA, and how are these scores related to their experience of online threats, computer and security knowledge?
The final research question investigated participants' security behaviour intentions, as measured by the SeBIS. While some researchers have pointed out that SeBIS may not fully capture smartphone-specific behaviours (Huang et al., 2023), it remains a well-established tool for measuring common security intentions, such as intended password creation, software updates, and awareness. Notably, SeBIS has been applied across various cultural contexts. For instance, a recent study involving over 3,500 participants from seven countries, including the United Arab Emirates, demonstrated its suitability for the Arab context (Sawaya et al., 2017). Although there is limited research using SeBIS specifically with Saudi participants, one recent study employed the scale to explore the relationship between security behaviour and perceptions of facial recognition technology, comparing Saudi and American users (Alqarni et al., 2023). This underscores its relevance and appropriateness for the current study.

A comparative analysis with the original SeBIS normative scores (Egelman & Peer, 2015) revealed some differences in the behavioural intentions of this Saudi sample. Participants demonstrated significantly higher security intentions in Device Securement, suggesting greater engagement in protective behaviours such as screen locking. This may reflect increased awareness about device protection and privacy and is potentially influenced by growing smartphone use. However, Password Generation scores in this sample were significantly lower than the normative data. This indicates weak practices in creating strong and unique passwords. Similar concerns have been raised in previous research, which reported that Saudi students may lack good password security (Alqahtani, 2022), and reuse passwords across accounts (Alkhaiwani & Almalki, 2021). Moreover, cultural factors may also play a role: one study found that some Saudi participants shared passwords to banking accounts with their spouses as a sign of trust, despite this practice being against official cybersecurity regulations (Flechais et al., 2013).

Additionally, Updating intentions scored significantly lower, both compared to the original SeBIS sample and the scale midpoint, indicating this as a particular area of weakness. The relatively low score on the Updating subscale suggests that this may represent a gap in secure behaviour. Notably, this pattern is not unique to this sample; prior research with American participants has also shown that users often delay or ignore software updates (Rajivan et al., 2020).

Interestingly, while Proactive Awareness scores were not significantly different from the normative sample, they were significantly above the scale midpoint. This suggests that participants exhibit moderate awareness, such as avoiding suspicious links or verifying sources. Overall, these results

highlight that while younger adults in the KSA show strong intentions in some security behaviours, there remain notable gaps, particularly in updating and password practices, which are consistent with previous findings (Alqarni et al., 2023; Alzubaidi, 2021).

When examining the relationship between SeBIS and participants' level of worry, higher levels of worry about phishing and identity theft were associated with lower scores on proactive security. This pattern implies that greater worry may inhibit rather than encourage action in some users, possibly due to a lack of efficacy. This agrees with prior research suggesting that self-efficacy or confidence plays a more critical role in driving secure behaviours than knowledge alone (Sawaya et al., 2017). In this context, even users who are aware of risks may fail to act securely if they do not feel capable of protecting themselves.

Participants who reported higher levels of computer knowledge**,** security knowledge, and ability to identify attacks were more likely to score higher on the Password Generation subscale of SeBIS. Similarly, both security knowledge and the ability to identify attacks were associated with higher scores on the Proactive Awareness subscale. This agrees with the SeBIS validation study by Egelman et al. (2016) which found that those who scored high in Proactive Awareness were more able to identify phishing websites. Another study examined the relationship between knowledge and security behaviour among students from two Saudi universities (Aldossary & Zeki, 2016) and found that students' knowledge was linked to their security behaviours. However, the study did not provide clear details about the questionnaire or methods used. It mainly assessed security knowledge by focusing on students' awareness of viruses, as interpreted from the results. This limited approach might not cover all aspects of security knowledge that are important for understanding users' security behaviours.

4.5.1 Limitations of the Study

The study had a number of limitations which need to be discussed. First, while the scenario-based survey provided useful insights into the types of online threats experienced by participants, the sample size in this study (N = 45) was relatively small. Although 130 responses were received, many were excluded due to incompleteness or failure to pass the attention checks (explained in 3.2.6). This limits the generalisability of the findings.

Notably, a relatively high proportion of completed responses in the KSA sample failed the attention checks (28 out of 73 completed responses; 38 %), which is substantially higher than in the UK survey, where only 3 out of 84 participants (4 %) failed the attention check questions.

Several factors may have contributed to this. First, the attention check items were created by reversing three existing SeBIS statements (e.g. changing "I use different passwords for different accounts" to "I use the same password for different accounts"). This required participants to notice a subtle change in meaning, and when such items were translated into Arabic, the combination of reversal and translation may have made them even harder to interpret accurately than they were in English. Secondly, the attention check questions were placed near the end of a relatively long and cognitively demanding questionnaire. Although this was also the case for the UK sample, it did not appear to affect UK participants to the same extent. However, by this point, some participants may have been tired or less focused, increasing the likelihood of mistakes. Thirdly, although the survey was offered in both Arabic and English, the technical wording of some items may still have been

challenging for some respondents. Together, these factors may help to explain the higher failure rate in attention checks in this phase compared with the UK sample. Finally, and perhaps most importantly, UK participants were recruited through the Prolific platform, The KSA sample was recruited through messages on various email lists, so participants may have been much less familiar with completing online questionnaires. This difference in familiarity with the type of task may have contributed to the lower failure rate observed in the UK sample compared with the KSA sample. Together, these factors may help to explain the higher failure rate in attention checks in the KSA sample

Another limitation of this study that the responses to the optional open-ended questions were limited, especially in describing threat detection or solutions. Although the survey was offered in both Arabic and English, language complexity or digital literacy may have still affected comprehension or response rate. In addition, the fact that the KSA participants may not have been used to completing questionnaires, as noted above, may have meant they were less likely to answer open-ended questions or provided shorter answers. This reduced the depth of insight into behavioural responses.

4.6 Conclusions

One key feature of this study was that the threat scenarios were pre-defined, based on what I found in the existing literature and cybersecurity reports. While this allowed for comparison across known threat types, it also meant that participants could only respond to the situations presented, in spite of the fact that participants were told not to react to the specific scenario but to a situation like that.

To address the limitations that participants were given a pre-defined set of scenarios and that they were reporting from memory on incidents which may have been a long time ago and mis-remembered, the next two studies adopt a diary-based design. This allowed me to gain richer insights into how individuals recognise and respond to online threats in real-life contexts, and with close to real-time reporting. This approach shifts the focus from researcher-defined threats to incidents reported directly by the participant, allowing them to record actual encounters with security threats as they occur. This method provides an opportunity to explore the emergent threat landscape and better understand users' detection strategies and behavioural responses in their own context. The next study, reported in Chapter 5, was conducted in KSA. Then in Chapter 6, the diary method I initially used was refined and improved, for a study conducted in the UK.

Chapter 5 Diary Study of Experiences of Online Threats for Saudi Younger Adults

5.1 Introduction

The previous chapters provided initial findings of the types of online threats encountered by younger adults in the KSA and UK, as well as how they recognised and responded to these threats. However, these findings were based primarily on retrospective survey data. To build on this work, this chapter presents findings from a diary study with younger adults in the KSA, which focuses on documenting online threat encounters in more detail as they occurred in near real time. The following study will present a subsequent diary study conducted with younger adults in the UK.

The main aim of this phase of the program of research was to complement the earlier survey studies by moving beyond retrospective reports and capturing information about specific encounters, asking participants to report on the cues they used to detect possible attacks, and their responses during their daily digital activities. This method was particularly suitable for understanding how online threats are experienced in practice, rather than how participants recall or anticipate such events.

This diary study was designed to address limitations in survey method such as: (1) it avoids reliance on memory by capturing experiences closer to when they occur; (2) it focuses on specific, real-life threat events, allowing for more detailed insights into participants' perceptions and reactions; and (3) it is longitudinal, so gives more accurate estimate of the frequency of encountering threats.

The results of the earlier studies in this programme of research indicated that phishing, spear phishing, and malware were among the most frequently encountered threats, and highlighted a range of cues used by participants to detect and respond to these threats. This diary study extends these findings by examining participants' threat experiences in greater detail and with more immediate reporting.

The diary study was conducted with participants in the KSA before being extended to the UK sample. Although the earlier survey phase was carried out in parallel for both samples, the original research design planned to follow the survey with an in-lab experimental study involving UK participants. While the diary study was being conducted in the KSA, the experimental study was developed in parallel. However, due to time and ethical constraints given the PhD timeframe, conducting the experimental study was no longer feasible. As a result, the research design was adapted, and the diary method was subsequently used with the UK sample instead.

The study contributes to Objectives 1–3 outlined in Chapter 1 by offering more detailed and immediate accounts of threat encounters and behaviours.

The following research questions are specific to this study:

RQ1: How frequently do Saudi younger adults encounter different types of online threats?
RQ2: What are the purposes of online threats that Saudi younger adults encounter?
RQ3: What cues do Saudi younger adults use to detect online threats?
RQ4: How do Saudi younger adults respond to online threats?
RQ5: What is the relationship between Saudi younger adults' individual characteristics (risk taking,

unrealistic optimism, consideration of future consequences, online security behaviours) and their experiences of online threats?

Table 5.1: Mapping thesis objectives to the KSA diary study RQs.

Thesis objectives	KSA diary study
Obj. 1: Identify the type and frequency of online threat encountered by younger adults	RQ1, RQ2
Obj. 2: Examine how younger adults detect and response to threats	RQ3, RQ4
Obj. 3: Investigate how individual characteristics affect online experiences	RQ5

The diary method directly supports the research questions addressed in this chapter. Daily reporting enabled the examination of how frequently different types of online threats were encountered (RQ1) and the perceived purposes of those threats (RQ2). By asking participants to describe the cues they relied on to identify threats and the actions they took in response, the diary entries also provided insight into threat detection (RQ3) and response behaviour (RQ4). Linking diary-reported experiences with individual characteristics measured through standardised scales allowed the examination of how risk-taking, unrealistic optimism, consideration of future consequences, and online security behaviours related to real-world exposure and responses to online threats (RQ5).

Several recruitment considerations also shaped this phase of the research. The upper age limit for participation was extended from 30 to 40 years, as recruitment and continued participation were more challenging during the diary phase due to the extended time commitment required. The diary study did not have a fixed target sample size; however, based on initial responses to the study invitation, recruitment aimed to enrol approximately 30 participants. However, fewer participants agreed to take part after receiving full study details. Recruitment and continued participation also influenced the final sample, including the observed gender balance, which is discussed further in the Participants and Limitations of the Study sections.

The daily questions did not directly ask participants about their emotional reactions to the threats or their perceived impact (e.g. whether the encounter caused harm). These were not the focus of the study which aimed to record the frequency and types of threats and participants' behavioural responses, while keeping the daily reporting brief to encourage continued participation for 30 days. Emotional impact and coping confidence could be explored more directly in future diary studies by adding a small number of short follow-up items after each reported threat.

5.2 Method

5.2.1 Design

An online diary study was conducted to collect detailed information about the online threats received by young Saudi adults. The study was designed to allow participants to report their experience of online threats as they occur over time. This method was chosen to provide contextual insights into actual threats and behaviours, aiming to understand the specific threats encountered by individual adults over an extended period.

Structured surveys (e.g. Alotaibi et al., 2016; Alyahya & Weir, 2021; Alzubaidi, 2021) often ask participants about particular types of threats that have been selected and defined by survey authors or identified as frequent in the literature. By contrast, the diary method allows the participants to

monitor the actual threats they encounter during the study period. This method is also useful in determining the frequency of online threats targeting young adults in Saudi Arabia. The study involved asking participants to note the online threats they encountered during the day and complete a short diary entry about the threats at the end of each day. If they encountered no threats on a particular day, they would simply report that. Those who reported receiving an online threat were ask to upload screenshots of it if possible and explain briefly what happened and how they decided whether it was a security threat or not.

Screenshots provided more objective information about the threats, which could be analysed further and compared with participants' answers to identify any details they may have missed.

Participants were asked to take screenshots of the threat once they encountered it and upload them to the link of the diary when they received it at the end of the day. Each day, participants were allowed to enter up to three threats.

Participants were asked to complete the diary for 30 days. This time period was chosen to collect sufficient data suitable for analysis, considering the possibility that participants may not encounter online threats every day, and to gather more detailed information about young Saudi adults' experiences with online threats.

The diary study consisted of three main parts: an initial questionnaire, a 30-day diary period, and a final questionnaire.

The study employed a number of measures to investigate the relationship between participants' individual characteristics and behaviours in relation to online threats. This approach is consistent with past research efforts described in Chapter 2 (Section 2.8).

The measures used were:

- The Security Behaviour Intention Scale (SeBIS) (Egelman & Peer, 2015b) was used to measure online security behaviour. SeBIS was selected as it has been validated in previous studies across several different cultures, especially Western countries (see section 2.6.1).
- The Domain-Specific Risk-Taking Scale (DOSPERT) (Blais & Weber, 2006), a well-established scale, has been used in previous studies to measure risk perception and taking for participants in Western cultures (see section 2.8.1). There is a lack of scales developed to measure the risk perception and taking among Arab populations, However, the DOSPERT has been successfully adapted in other cultural contexts. Moreover, DOSPERT measures domain-specific risk-taking, making it suitable to examine the likelihood of engaging in risky behaviours in the online security context. Egelman and Peer (2015) investigated its correlation with SeBIS to understand how risk-taking tendencies relate to security behaviours. DOSPERT was adapted and used in this study to address the gap in using a standardised scale for risk-taking in the Arab world.
- The Consideration of Future Consequences Scale (CFC) (Strathman et al., 1994) was used to understand how considering future consequences affects online security behaviours, as previously explored in the development of SeBIS (Egelman & Peer, 2015b).
- Unrealistic optimism (UO) was measured with six questions that asked participants to rate:
    - Their vulnerability to online threats compared to a friend and a typical person of their age.

- Their ability to detect online threats that come from different sources, such as messages, links or websites, compared to a friend or typical person in their age.
- Their ability to deal with threats if they received them compared to a friend or a typical person of their age.

This measure was included as it is common that people believe they are less likely to experience negative events, which may lead them to take more risks. This bias has also been examined in previous works related to factors affecting online security (Hewitt & White, 2021; Rhee et al., 2012).

To spread the workload, participants were asked to complete the SeBIS and DOSPERT as part of the initial questionnaire and the CFC and UO questions as part of the final questionnaire.

The three parts of the diary study are illustrated in Figure 5.1.

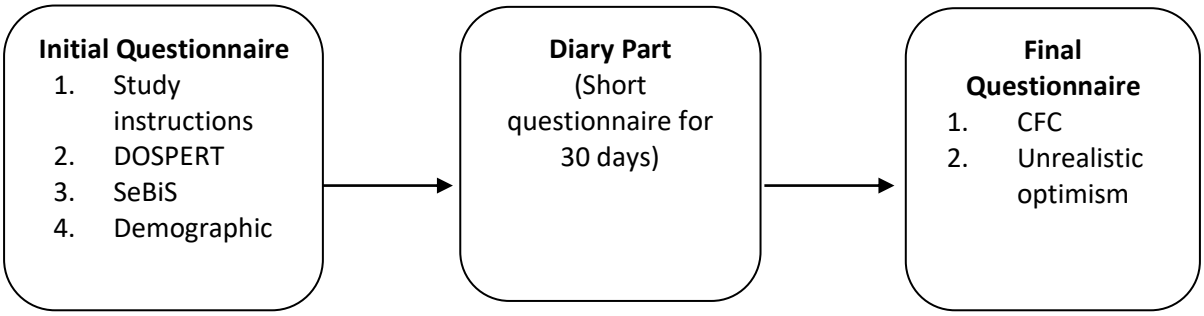


Figure 5.1: Three parts of the diary study.

5.2.2 Participants

For participation, the inclusion criteria were to be a regular Internet user living in Saudi Arabia, aged between 18–40 years old. 16 participants were recruited. Table 5.2 summarises the demographics of the sample. Compensation of 200 Saudi Riyals (approximately GBP42 or USD 53) was offered for participation in the study.

Table 5.2: Demographic characteristics of the participants in Study 3.

Gender	
Male	4 (25 %)
Female	12 (75 %)
Age	
Range	18–40 years
Mean	24
Educational background	
High school	5 (31 %)
Bachelor's degree	10 (63 %)
Postgraduate degree	1 (6 %)
Self-rating of computer knowledge	Median: 6.5, SIQR: 1.0 Range: 3–7 T = -2.55 p = 0.011

Self-rating of online security knowledge	Median: 5.0, SIQR:1.5 Range: 3–7 T = -2.96 P = 0.003

Participants were asked to rate their general computer knowledge and their online security knowledge on 7-point Likert items (ranging from 1 = not at all knowledgeable to 7 = very knowledgeable). Participants rated significantly above the midpoint of the scale (One-Sample Wilcoxon Signed Rank Tests) on their computer knowledge. Participants also rated their online security knowledge significantly above the midpoint. They rated their general computer knowledge significantly higher than their online security knowledge (Related Samples Wilcoxon Signed Rank Test, T = -2.59, p = 0.01). Thus, participants considered themselves knowledgeable about both computers and online security, but less so about online security.

Participants were also asked if they had attended any online security courses or training. 14 (88 %) participants reported having taken such courses or training. While the question did not specify the type or content of training, this high percentage may suggest a general interest or awareness of online security issues among the sample.

5.2.3 Materials

5.2.3.1 Initial Questionnaire

The diary study was implemented as an online questionnaire using Qualtrics survey software (Qualtrics.com). The study consisted of three main parts. The first part of the study involved an initial questionnaire. Participants were presented with an introduction to the study, followed by detailed instructions and information about data protection and the consent form. Also, participants were asked to select or create an email address for this study and share it with the researchers. Email addresses were used to link participants' answers in the three parts of the study. Also, it was used to send their compensation at the end of the study.

The DOSPERT scale was used in this study to measure the likelihood of engaging in various risky behaviours across five domains: Health/safety (H/S), Financial (F), Recreational (R), Ethical (E) and Social (S). Participants were asked to rate their risk taking as measured by (DOSPERT) for 26 items ranging from extremely unlikely (1) to extremely likely (7).

To the best of my knowledge, DOSPERT has not been used in Arabic countries nor has it been translated into Arabic, except for one study by Rogers (2017) (see section 2.8.1). However, it was not specified whether the scale translated into Arabic.

Therefore, I adapted the DOSPERT scale to suit the Saudi context. I removed four items due to cultural and contextual inappropriateness for the Saudi sample. One from the Ethical domain and three from the Financial domain, making a 26-item scale.

In addition, some items in the Financial and Ethical sub-scales were adjusted to measure similar risks, but in a way that is more appropriate for the Saudi context. For example, in the Ethical subscale, the item "Drinking heavily at a social function" was replaced with "Taking certain medications that may affect your behaviour before a social event". Some words were changed to be

more understandable to Saudi participants. For example, in the Recreational domain, one of the items “Going whitewater rafting at high water in the spring” was replaced with “Going jet skiing in surging sea waves”.

The DOSPERT scale consists of subscales: Social, Health/Safety, and Recreational, each consisting of 6 items with possible scores ranging from 6 to 42. The Financial subscale, which has 3 items, offers possible scores from 3 to 21. The Ethical subscale contains 5 items, with possible scores ranging from 5 to 35. Higher scores in the subscale of DOSPERT indicate greater willingness to take risks in that subscale.

Both original and modified scales can be found in Appendix F: Original and Modified DOSPERT scale.

The SeBIS scale measures participants' intentions to engage in security behaviours across four sub-scales: Device Securement, Password Generation, Proactive Awareness, and Updating. The original SeBIS scale was used without any modification. Due to an oversight, I did not use the adapted version of the SeBIS scale which I used in Studies 1 and 2. Participants were asked to rate their online security behaviours (SeBIS), 16 items with a 7-point Likert scale from Never (1) to Always (7).

The Device Securement and Password Generation subscales have four items each, with scores ranging from 4 to 28. For Proactive Awareness, there are 5 items and scores ranging from 5 to 35. Updating subscale has 3 items and scores ranging from 3 to 21.

At the end of the initial questionnaire, participants were asked about their demographics: age, gender, and educational background. Finally, there were three questions about computer and online security knowledge and whether they attended any online security training or courses.

5.2.3.2 Diary Questionnaire

This online questionnaire was sent via email to the participants every day at the same time. The daily short questionnaire consisted of four questions. The first question asked if they had encountered any online threat that day, followed by an optional question to upload a screenshot of the threat if they were able to capture one. The third and fourth questions were open-ended, asking the participants to briefly explain what happened and how they determined whether it was a security threat. Lastly, they were asked if they wanted to report another threat for that day. Participants were permitted to enter up to three threats per day. Table 5.3 shows the main structure of the questions in the diary questionnaire.

Table 5.3: Diary questions.

Have you received any possible online threats today?	Yes/No
If Yes for the first/second/third possible threat,	
Please upload the screenshot of the threat if you were able to take one.	
Please briefly explain what happened	Open-ended
Did you respond to the threat?	Yes/No
How did you decide whether it was a security threat or not?	Open-ended

5.2.3.3 Final Questionnaire

The final questionnaire consisted of the CFC scale and the UO questions. The original unidimensional CFC scale by Strathman et al. (1994) was used, which has 12 items. Initially, the original unidimensional CFC scale by Strathman et al. (1994) was considered for this study. However, later research has revised the scale into a two-dimensional structure, distinguishing between Consideration of Immediate Consequences and Consideration of Future Consequences. Based on this, the 10-item version validated by She et al. (2021) was selected. I chose to use this validated scale because it is relevant to my research, as it focuses on evaluating the CFC scale among Malaysian young adults, similar to my target sample age group. Additionally, Malaysia and Saudi Arabia have some cultural and religious similarities, which may affect how people make their decisions. This makes the scale more suitable for my population than those validated in Western countries.

Participants were asked to rate 12 statements about CFC on a 5-point Likert scale ranging from extremely uncharacteristic (1) to extremely characteristic (5).

UO was measured with six questions that asked participants to compare themselves either to their friends or to a typical person of their age. The questions were as follows:

1. Compared to your friends, how likely do you think you are to receive online threats and attacks?
2. Compared to a typical person of your age, how likely do you think you are to receive online threats and attacks?
3. Compared to your friends, how capable do you feel in detecting whether a message, link, or website is an online threat?
4. Compared to a typical person of your age, how capable do you feel in detecting whether a message, link, or website is an online threat?
5. Compared to a typical person of your age, do you think you know how to handle online attacks?
6. Compared to your friends, do you think you know how to handle online attacks?

For Questions 1 and 2, participants responded on a 5-point scale ranging from “Much less likely than others” (1), through “About the same” (3), to “Much more likely than others” (5). For Questions 4 to 6, responses were also on a 5-point scale, ranging from “Much less able” (1), through “About the same” (3), to “Much more able” (5).

All questionnaires were made available in both Arabic and English. On the first page of each questionnaire, participants were given the option to select their preferred language before beginning the study. All translations were carefully reviewed to ensure clarity and consistency across both versions.

Participants received a file containing some examples with clarification images of the most common and current online threats that have targeted individuals. They were asked to keep this file during the study period and refer to it when needed (see Appendix G: The Information Sheet Shared with Saudi Participants before the Diary Study).

5.2.4 Procedure

The inclusion criteria were designed to ensure that participants were likely to encounter online threats in their everyday digital activities. Focusing on younger adults who regularly used the Internet increased the likelihood of capturing naturally occurring, real-world threat experiences during the diary period. No additional restrictions were placed on participants' technical expertise or prior security knowledge, as the aim of the diary study was to observe how general users experience and respond to online threats, rather than to compare predefined user groups.

Participants were recruited using a combination of snowball sampling and open online recruitment. Initial invitations were shared through my social network and further circulated through social network groups (e.g. Telegram). This approach was chosen to reach a broad range of younger adults with diverse levels of online usage and security knowledge, reflecting everyday Internet use rather than a specific or expert group. A more targeted recruitment strategy was therefore not adopted, as it may have narrowed the range of naturally occurring experiences captured in the diary study.

Potential participants were first contacted via email and informed about the purpose of the study, its duration, and what participation would involve. Those who expressed interest received a follow-up email with further details, including the official start date of the study, the time commitment required for each part (e.g. the initial questionnaire, the 30-day diary, and the final questionnaire), and instructions for completing each part. They were told they would receive email reminders for each phase, with links to complete the relevant questionnaires.

Each evening during the diary period, participants received an email with a link to a short questionnaire to report any threats experienced that day. They could report up to three threats per day. If no threats occurred, they could simply indicate that. Screenshots, if available, could be uploaded through the same diary link.

Participants were informed that they could capture screenshots of any type of online threat or attack, regardless of the device they were using at the time (smartphone, tablet, laptop, or desktop). Lastly, to ensure privacy, participants were asked to obscure the other party's (sender's) information before sharing screenshots. This includes their name, profile picture, and any other identifying information.

To encourage daily completion of the diary questionnaires, participants received daily email reminders with a link to the day's diary questionnaire, prompting them to report any online threats encountered that day. At the end of each week, participants received a follow-up email acknowledging their participation and encouraging them to keep making diary entries. These emails also reminded participants that they could contact me at any time if they had questions or needed support.

At the end of the study, participants were sent an email of thanks and arrangements were made to send them the gift voucher.

The study was reviewed and approved by the Physical Sciences Ethics Committee at the University of York (reference: Aldaraani20230711).

5.2.5 Data Analysis

The rating data from the scales were not normally distributed, so non-parametric statistics were appropriate. Non-parametric tests are also preferred for small sample sizes (Siegel & Castellan, 1988).

Content analysis was used to analyse the open-ended questions that asked participants to explain what happened and how they recognised the threats and the screenshots (if provided). I coded the following information:

- the threat type,
- cue/s used to recognise the threats
- purpose of threat
- response to the threats.

Threat Type

The types of threats that emerged from the analysis of participants' responses are presented in Table 5.4.

Table 5.4: Threat type definitions.

Type/subtype	Definition
Phishing	Messages from unknown sources (email) that are designed to deceive or manipulate recipients into disclosing sensitive information or taking harmful actions. Phishing from other than emails categorised separately.
Spear phishing	Messages that often come from familiar or trusted sources, such as a bank, shipping company, or store
Smishing	Phishing via SMS text message
Vishing	Phishing via online voice channel
WhatsApp phishing	Phishing via WhatsApp message
Social media phishing	Phishing via a message on social media sites
Spoofed website	A fraudulent website that closely resembles a legitimate one
Not clear	Threat type could not be identified

Cues used to identify a threat

I started with the cue categories from the Phish Scale (Steves et al., 2020), listed in Table 5.4. While the Phish Scale was created to rate the difficulty of detecting phishing emails, I realised that I needed to categorise cues for threats coming from a wider range of sources, including phone calls, SMS, and social media platforms (see items with an asterisk in Table 5.5). Therefore, I expanded the Phish Scale categories in the following ways: "Technical Indicators" was expanded to include unknown phone or SMS numbers. Similarly, "Language and Content" was expanded to include incorrect and not applicable information. In addition, a new category was added, named "Prior Knowledge", to cover cases where participants identified a threat based on past experience or warnings from external sources (e.g. friends, social media, or the news). For example, if participants were previously aware of the threat, prior knowledge from sources such as friends, family, social media, news, or popular scam methods served as cues in this context.

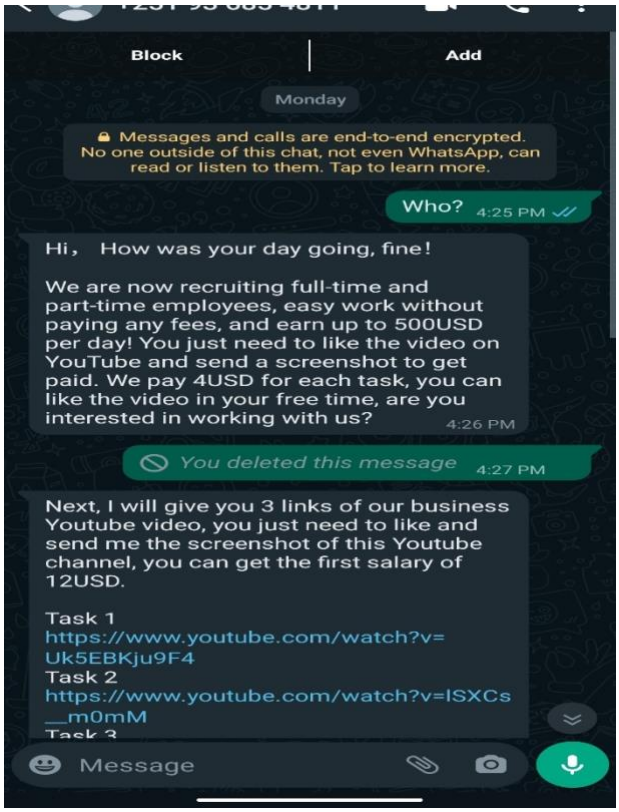
Table 5.5: List of cues used to identify threats (adapted and expanded version of the NIST Phish Scale cues [Steves et al., 2020]).

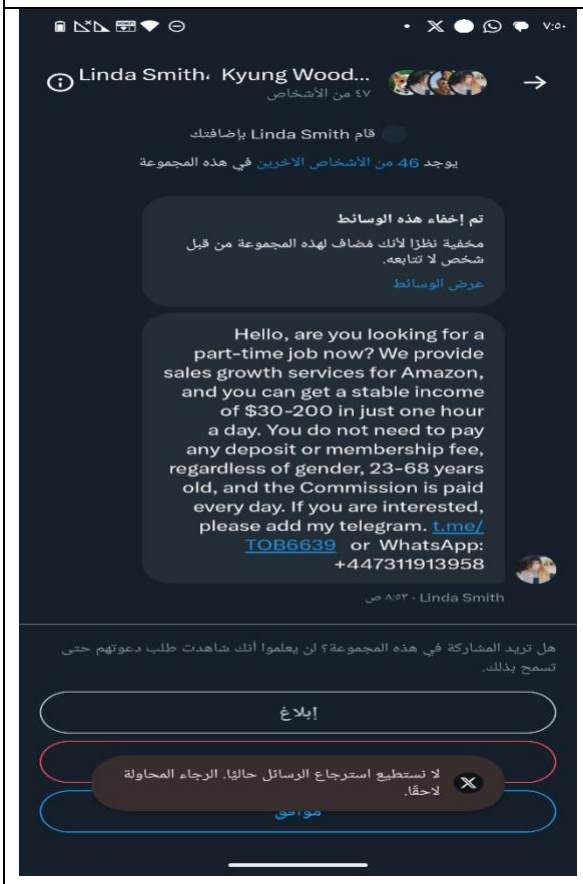
Cue type	Cue name	Criteria for counting
Error	Spelling and grammar irregularities	Does the message contain Inaccurate spelling or grammar use,including mismatched plurality?
	Inconsistency	Are there inconsistencies contained in the email message?
Technical indicator	Attachment type	Is there a potentially dangerous attachment?
	Sender display name and email address	Does a display name hide the real sender or reply-to emailaddresses?
	URL hyperlinking	Is there text that hides the true URL behind the text?
	Domain spoofing	Is a domain name used in addresses or links plausibly similar to alegitimate entity's domain?
	Unknown (phone/SMS) number*	Is the number for the phone call or message unknown?
Visual presentation indicator	No/minimal branding andlogos	Are appropriately branded labeling, symbols, or insigniasmissing?
	Logo imitation or out-of-date branding/logos	Do any branding elements appear to be an imitation or out-of-date?
	Unprofessional lookingdesign or formatting	Does the design and formatting violate any conventional professional practices? Do the design elements appear to beunprofessionally generated?
	Security indicators and icons	Are any markers, images, or logos that imply the security of theemail present?
Language and content	Legal language/copyright info/disclaimers	Does the message contain any legal-type language such ascopyright information, disclaimers, or tax information?
	Distracting detail	Does the message contain any detailed aspects that are not central to the content?
	Requests for sensitiveinformation	Does the message contain a request for any sensitive information,including personally identifying information or credentials?
	Sense of urgency	Does the message contain time pressure to get users to quicklycomply with the request, including implied pressure?
	Threatening language	Does the message contain a threat, including an implied threat,such as legal ramifications for inaction?
	Generic greeting	Does the message lack a greeting or lack personalisation in the message?
	Lack of sender details	Does the message lack detail about the sender, such as contact information?

Cue type	Cue name	Criteria for counting
	Incorrect information*	Does a message or call have something wrong, inaccurate or deceptive? For example, false notifications about parcel deliveries when there is no expected shipment, or requests from a bank using unusual communication methods, such as personal calls requesting sensitive information.
	Not Applicable information*	Is the information not relevant or applicable to the participant's circumstances, interests, or context at the time of receipt? For example, receiving a job offer based on a CV when no CV has been submitted
Commontactic	Humanitarian appeals	Does the message make an appeal to help others in need?
	Too good to be true offers	Does the message offer anything that is too good to be true, suchhaving won a contest, lottery, free vacation and so on?
	You're special	Does the email offer anything just for you, such as a valentine e-card from a secret admirer?
	Limited time offer	Does the email offer anything that won't last long or for a finitelength of time?
	Mimics a work or businessprocess	Does the message appear to be a work or business-relatedprocess, such as a new voicemail, package delivery, order confirmation, notice of invoice?
	Poses as friend, colleague, supervisor, authority figure	Does the message appear to be from a friend, colleague, boss orother authority entity?
Prior knowledge*	Friends or family	Does the participant already know something about this threat from their family and friends?
	Social media	Does the participant already know something about this threat from social media?
	Official websites and news streams	Does the participant already know something about this threat type from official websites (e.g. bank or governmental sites) or news streams.
	Common scam	Does the participant already know something about this threat because it is commonly known scam method? (no source of knowledge given)

Any cues in the screenshot which the participant had not reported (and therefore potentially not noticed) were also coded. Table 5.6 shows some examples of the screenshots and cues extracted from it.

Table 5.6: Examples of images attached by participants.

Example screenshots	Cues found by participants	Unmentioned cues
	Prior knowledge (Official), Mimics a work or business process, Incorrect info. (phone number)	Spelling mistake, grammar mistake
	Request for sensitive information	Too good to be true, Lack of sender details

Example screenshots	Cues found by participants	Unmentioned cues
	Prior knowledge (Family and Friends), URL	Too good to be true

Purpose of Threat

The main purpose of the threats was determined from participants' responses, with data theft or financial fraud identified as the primary purposes. The definitions and examples can be found in Section 5.3.2, Table 5.8.

Categories for Interaction with Threats

Participants have been classified based on their interaction with the threats. The interaction with threats was found in their answers to the open-ended questions about how they recognised threats. Two groups were created: Interactors, referred to participants who interacted with at least one threat, and non-interactors, referred to participants who did not interact with any threats.

I acted as first coder. My supervisor, the second coder, then reviewed my coding. Problem areas in the coding were discussed, and adjustments were made as needed. Any problematic cases were assessed by the two coders together. Often, the information provided by the participant was ambiguous, which made coding difficult.

The coding process involved the following steps:

1. The first coder began the coding procedure by reviewing all participant responses.
2. Categories were initially extracted from participants' responses, including threat type, source of threat, purpose of the attack, and cues used by participants to recognise the threat and actions taken in response to the threats.
3. The first coder wrote the definitions for the categories and subcategories.

4. A meeting was conducted between the first and second coders to review the categories and their definitions. The definitions of each category and its subcategories were clarified and finalised to ensure that coders had a common understanding.
5. The second coder independently reviewed all participants' responses and assigned each response to the appropriate categories based on the refined definitions established previously.
6. Any disagreements in the coding between the first and second coders were discussed and resolved.

Participant quotes are labelled using the format "P#–R#", where "P" refers to the participant number and "R" indicates the response number, as participants could submit multiple entries throughout the study period.

5.3 Results

5.3.1 Encountering Online Threats: Frequency and Types of Threats

Participants monitored for threats for between 17 and 35 days each. In total, there were 431 monitored days in the study. Participants reported 58 online threats in total, between 1 and 14 threats per participant. Thus, on average, participants reported having encountered only 0.13 threats per day, which means 4.04 threats per month. 13 participants provided a total of 47 screenshots of a threat.

The types and frequencies of the different threats reported are summarised in Table 5.7. The most frequently reported threat type was phishing, accounting for nearly 70% of all reported threats. This category was further divided into different types of phishing, with general phishing being the most common, representing 17 % of threats. Spear phishing was also common, making up 16 %, followed by phishing via WhatsApp at 12 %. The other phishing types each accounted for less than 10% of the threats. Only 7 % of threats involved a spoofed website. Additionally, a considerable number of reported threats (24 %) could not be determined due to insufficient information.

The results suggest that while participants encountered relatively low threats during the monitoring period, phishing remains the dominant threat type experienced in everyday digital life. The wide range of phishing channels reported (email, SMS, WhatsApp, social media, and voice calls) indicates that threats are not confined to a single platform but are embedded across participants' routine communication channels.

5.3.2 Purpose of the Online Threats Reported

Table 5.8 summarises the frequency of the purpose of the threat as understood by the participants.

In 22 % of cases, participants believed the threat was intended to steal data, and 27 % aimed at financial fraud. However, the purpose of 51 % of the threats could not be specified because participants did not provide enough information in their responses to identify the purpose of the threat.

Table 5.7: Threat types reported with examples and frequencies (N = 58).

Type/Subtype	Examples	Frequency (%)
Phishing		**40 (69 %)**
Phishing	"An advertisement arrived via email for jobs, and it contained a link that led to a strange website requesting personal information" (P10-R2) "I received an email claiming that they have a profitable business project that requires collaboration" (P12-12)	10 (17)
Spear phishing	"A scam involving a group impersonating "SPL," a shipping company. The scammers use WhatsApp to send messages claiming that you have a shipment and need to pay for the shipping" (P1-R1)	9 (16)
Smishing	"I received messages on my number claiming that they found my resume and liked it" (P15-R1) "I received a text message claiming to be from Saudi Post" (P5-R3)	7 (12)
Vishing	"Deceptive call claiming to suspend the bank account" (P13-R5)	4 (7)
WhatsApp phishing	"An international number contacted me through WhatsApp and informed me that they have a remote job I can do in my spare time" (P11-R1)	7 (12)
Social Media phishing	"Message on Twitter attempted to persuade to click on the link" (P13-R2)	3 (5)
Spoofed website	"I was searching for the Ministry of Commerce to report an illegal sale. The website that appeared first on my search results was the one I clicked on, it was a fake website that did not have the ministry logo or contact information" (P1-R3)	**4 (7 %)**
Not clear		**14 (24 %)**

Table 5.8: Purposes of the threats and examples of participants' explanations (N = 59[1]).

Category	Definition	Example	Frequency (%)
Data theft	Attempts to obtain victims' personal or sensitive data such as name, date of birth, phone number, email, credit card number, or bank details	An international number with no available information is requesting sensitive information (P12-R3)	13 (22 %)
Financial fraud	Attempts to engage the victims in financial transactions or make payments	Received an email from a shipping company and they asked to complete the payment (P2-R3)	16 (27 %)
Could not be specified	The purpose of the attack cannot be specified from the participant's response and screenshot.	A message containing a link from an unknown source has been received (P4-R3)	30 (51 %)

[1.] One threat report included both data theft and financial fraud as purposes

These findings indicate that when participants were able to infer the purpose of a threat, it was most commonly understood in terms of financial fraud or data theft. However, the fact that the purpose could not be identified in over half of the reported threats highlights the ambiguity of many real-world online attacks. In many cases, participants' descriptions and screenshots did not provide sufficient detail to clearly infer attacker intent, suggesting that users often encounter threats without fully understanding their underlying goals. This uncertainty reflects the everyday conditions under which online threats are experienced and the challenge individual users face in accurately interpreting attacker motives during threats encounters.

5.3.3 Cues Used to Detect Online Threats

A total of 98 cues were identified by participants as having been used to detect the online threats, 1.69 per threat. Additionally, from the screenshots or explanations of the threats, I identified 25 cues that were not mentioned by the participants, so 0.43 unmentioned cues per threat. This might be either because they did not notice them or did not consider them important enough to mention in their reports. This resulted in a total of 123 cues, 2.1 cues per threat. Table 5.9 lists the cues participants mentioned and the cues which I identified in the screenshots provided by the participants.

The most frequently mentioned cue category was Language and Content (37 %), with common sub-cues including requests for sensitive information (13 %) and incorrect information (9 %). This was followed by Technical Indicators (28 %), with Hidden or shortened URL hyperlinks and Lack of/Suspicious sender name or email both accounting for 9.4% of cues. The categories of Prior knowledge (15 %) and Common Tactic (15 %) were somewhat less frequently reported by participants. Finally, participants reported a few cues in the Visual presentation indicator category (4 %) or the Errors category (2 %).

These findings highlight that participants mainly relied on content-based cues, technical signs, and prior experience to identify threats.

In terms of cues that were not reported by participants but identified by the researcher from the screenshots, Common tactic was the most frequently identified category (41 %), followed by Technical Indicator (26 %) and Language and content (19 %).

All the categories provided in the Phish scale are included in Table 5.9.

Table 5.9: Cues used by participants (N = 98) and cues found by researcher (N = 25).

Category/Sub-category	Participants N (%)	Researcher N (%)
Error	**2 (2 %)**	**2 (8 %)**
Spelling and grammar irregularities	1 (1)	2 (7)
Inconsistency	1 (1)	0
Technical indicator	**27 (28 %)**	**7 (26 %)**
Attachment type	0	0
Sender display name, email address	9 (9)	2 (8)
Unknown phone/SMS number	6 (6)	0
Hidden/shortened URL hyperlink	9 (9)	5 (20)
Domain spoofing	3 (3)	0
Visual presentation indicator	**4 (4 %)**	**0**
No/minimal branding and logos	1 (1)	0
Logo imitation or out-of-datebranding/logos	0	0
Unprofessional-looking design or formatting	2 (2)	0
Security indicators and icons	1 (1)	0
Language and content	**36 (37 %)**	**5 (19 %)**
Legal language/copyrightinfo/disclaimers	0	0
Distracting detail	1 (1)	0
Requests for sensitiveinformation	12 (13)	1 (4)
Sense of urgency	2 (2)	0
Threatening language	1 (1)	0
Generic greeting	3 (3)	1 (4)
Lack of sender details	4 (4.2)	3 (12.0)
Incorrect information	9 (9 %)	0
Not applicable information	4 (4 %)	0
Common tactic	**14 (15 %)**	**11 (41 %)**
Humanitarian appeals	2 (2)	2 (8)
Too good to be true offers	5 (5)	5 (20)
You're special	0	1 (4)
Limited time offer	0	1 (4)
Mimics work or business process	7 (7)	1 (4)
Poses as friend, colleague, supervisor, authority figure	0	1 (4)
Prior knowledge	**15 (15 %)**	**0**
Family or friends	4 (4)	0
Social media	2 (2)	0
Official websites and news streams	2 (2)	0
Common scam	6 (7)	0

Six of the Phish Scale cues were not used by any participant to detect threats. These cues are:

- Attachment Type
- Logo Imitation or Out-of-date branding/logos
- Legal Language/Copyrightinfo/Disclaimers
- You're Special
- Limited Time Offer

- Poses as a Friend, Colleague, Supervisor, Authority Figure.

However, three cue instances in the Common Tactic category were detected by me. In particular, 5 instances of the Common Tactic sub-category of Too good to be True Offers were not reported by the participants, as well as 5 instances of the Technical Indicator subcategory of Hidden/shortened URL hyperlinks. It is not known whether the participants simply forgot to include these cues in their report or whether they actually failed to notice them.

The threat detection cues shows that participants primarily relied on content-based and technical indicators, such as requests for sensitive information rather than visual design cues. The frequent reliance on prior knowledge and past experience further suggests that threat detection is shaped by learning and familiarity, rather than by evaluation of all available cues. At the same time, the presence of unreported cues identified through screenshots indicates that participants may overlook or under-report some warning signs, even when these cues are present in the threat.

5.3.4 Participants' Behavioural Patterns in Experiencing Online Threats

Based on the analysis of participants' descriptions of how they encountered and reacted to possible threats, I identified six distinct behavioural patterns. These patterns represent different ways participants navigated the threat experience, from initial perception to action or inaction, and eventual outcome. This section refers to these patterns collectively as the Behavioural Patterns in Experiencing Online Threats.

The patterns involve when the participants suspect something they receive (such as an email) is a threat, whether they take any action and whether it turns out to be a threat. Participants are considered to take action if they clicked on a link, opened a file or link or replied to a request in a call or SMS. In some cases, participants clicked on a link and then recognised the threat from the cues. In this case, they counted as having taken action, as they clicked before checking. These patterns are:

1. **Suspected Threat → Action Taken → Was a Threat:** Participants who recognised or suspected a threat based on one or more cues, took action, and confirmed their suspicion as valid.
2. **Suspected Threat → Action Taken → Was Not a Threat:** Participants who suspected a threat, took action, but their suspicion was incorrect, and no actual threat was present.
3. **Suspected Threat → No Action Taken → Was a Threat:** Participants who suspected a threat but did not take any action, and the situation ultimately revealed an actual threat.
4. **Suspected Threat → No Action Taken → Was Not Clear:** Participants who suspected a threat but chose not to act, which left the true type of threat undetermined.
5. **Did not Suspect Threat → Action Taken → Was a Threat:** Participants who did not initially suspect a threat but proceeded with an action, then found out that a threat was present.
6. **Did not Suspect Threat → No Action Taken → Was a Threat:** Participants who neither suspected the threat nor acted upon a potential threat, then found that it was a threat.

The most common pattern was suspected threat, no action taken, and it turned out to be a threat, where about 61% of responses follow this pattern.

Figure 5.2 presents a conceptual overview of the six patterns. Examples of each pattern are summarised in Table 5.10, drawn from participants' diary responses.

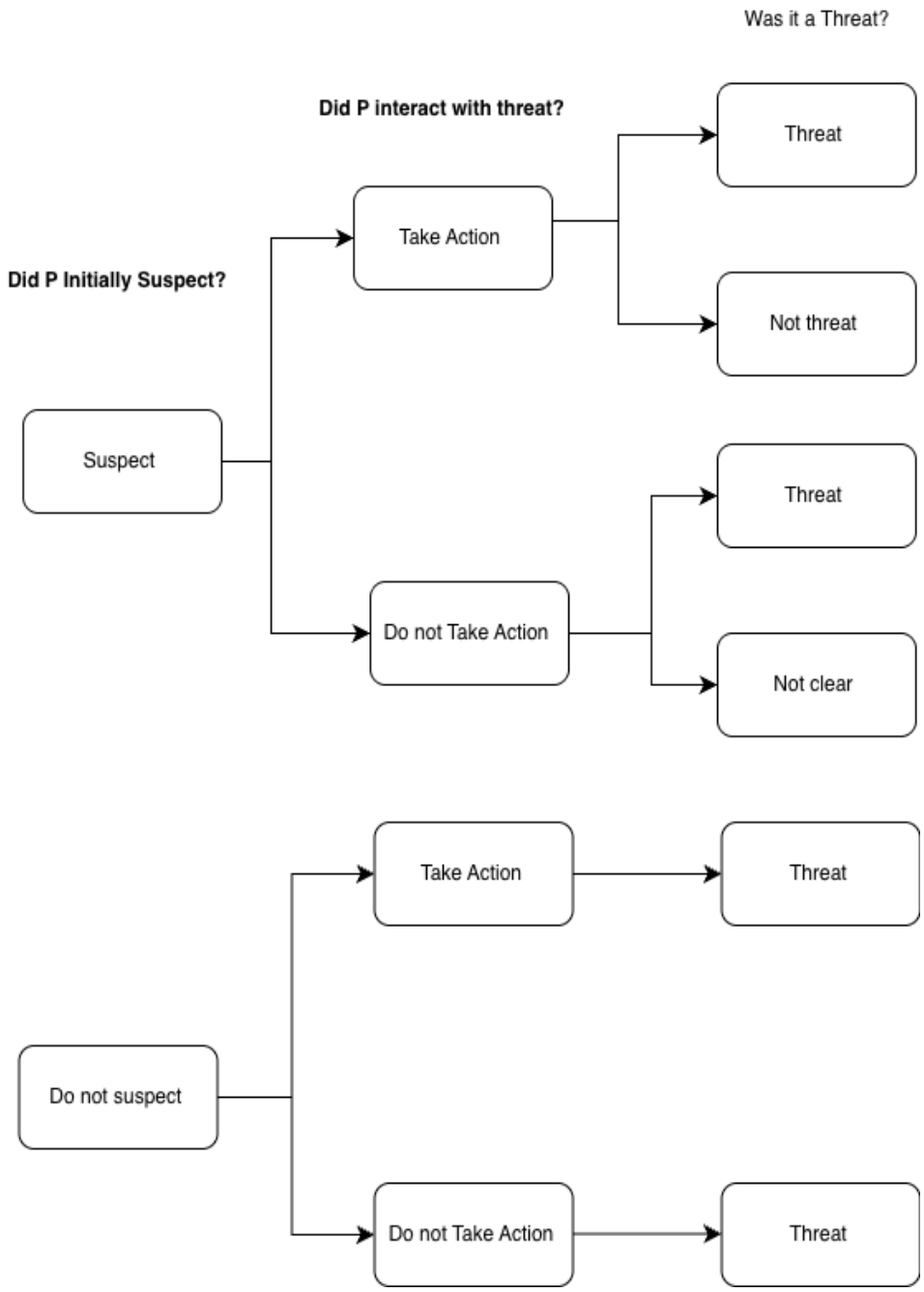


Figure 5.2: Participants' behavioural patterns in experiencing online threats.

Table 5.10: Frequencies of the six patterns of experiencing online threat, with examples of answers and explanations from participants (N = 57).

Patterns N (%)	Example answer	Explanation of how participant decided it was a threat
Suspected Threat → Action Taken → Was a Threat N = 2 (3.5%)	**P2-R1**: **"**I wanted to book a movie, and when I wrote Fox Cinema. An advertisement for Fox appeared to me as the first link after I completed the booking and selected Apple Pay, it was rejected. And only the bank card number was allowed to be used. A verifying message for payment was not received (which is the usual verifying option), but I received a call, the voice was different from Al Rajhi Bank calls so I cancelled it. Also, the movie was available at all times which is not usual"	**P2-R1: "**Because an amount of money will be withdrawn from my card"
Suspected Threat → Action Taken → Was Not a Threat N= 2 (3.5%)	**P1-R1: "**I saw numerous Twitter posts discussing a scam involving a group impersonating "SPL," a shipping company in my country. The scammers use WhatsApp to send messages claiming that you have a shipment and need to pay the shipping fee to receive it. Their website closely resembles the real one, and when you enter your credit card information, they steal everything in your bank account. Today, I received a message from them, and I carefully inspected it to see if they were asking me to click on any links. However, they did not, so I sent my location and discovered that it was the real shipping company"	**P1-R1: "**by carefully inspecting the message and reviewing the requirements they asked for"
Suspected Threat → No Action Taken → Was a Threat N = 35 (61.4%)	**P15-R1: "**I'm receiving messages on my number claiming that they found my resume and liked it, even though I haven't posted my CV anywhere. They also sent me strange links, and their method of communication is also unusual" **P13-R5**: "A deceptive Call claiming to suspend the bank account"	**P15-R1: "**The attached link is not trustworthy, and the source is unknown. The email or number they sent it from is clearly fake and not organised at all" **P13-R5: "**My account is not suspended, and there is no reason for it to be suspended"

Patterns N (%)	Example answer	Explanation of how participant decided it was a threat
Suspected Threat → No Action Taken → Was Not Clear N= 9 (15.7%)	**P5-R2**: "An international number called me via WhatsApp video call" **P14-R1**: "A PIN code was sent from a website I did not register with"	**P5-R2:** No answer given **P14-R1: "**I did not register on this website"
Did not Suspect Threat → Action Taken → Was a Threat N = 7 (12.3%)	**P11-R1: "**An international number contacted me through WhatsApp and informed me that they have a remote job I can do in my spare time, in exchange for an attractive amount of money" **P10-R2**: "An advertisement arrived via email for jobs, and it contained a link that led to a strange website requesting personal information"	**P11-R1:"** After completing the required task, they asked me to download a money transfer application and instructed me to take screenshots of certain information from the app after creating an account" **P10-R2**: "The website looks suspicious and requests unusual information. For example, it says, "Enter your email to access your database!"
Did not Suspect Threat → No Action Taken → Was a Threat N = 2 (3.5%)	**P12-R1**: "Mail delivery company" **P8-R2: "**On my Instagram account, I received a message from someone offering to buy artwork in exchange for virtual currency. The message included a link to a website where paintings could supposedly be purchased with this currency. When I looked up the website, I realised it was untrustworthy."	**P12-R1:** "Inquire about the shipment and its destination" **P8-R2:** "through the suspicious link"

5.3.5 Appropriateness of Participants' Responses to Threats

To explore how participants responded to online threats, I analysed the appropriateness of their actions**.** Responses were assessed based on whether the participant took a protective step (e.g. verifying request, checking link) or not. Table 5.11 provides examples of both appropriate and inappropriate responses, along with their frequency. Most responses (77 %) were appropriate. However, 18 % involved risky actions that could expose participants to harm.

Further analysis of the six patterns (in section 5.3.4) and how they may be linked to the appropriateness showed that all participants who interacted with threats without initially suspecting them provided inappropriate responses. In contrast, only three cases involved participants who did suspect a threat but still responded inappropriately. This suggests that a lack of suspicion, combined with interaction, was most strongly associated with inappropriate threat responses**.**

Table 5.11: Examples of appropriate and inappropriate responses to online threats.

Response type	Example from participant answers	Appropriateness assessment	Frequency (%)
Appropriate Response	P12-R10: "Track the shipment No. on the real website of the shipping company"	Verifying the request with the legitimate source before responding	44 (77 %)
Not appropriate Response	P12-R5:" opened the link but did not enter the banking info."	Click on the link before checking the security indicators.	10 (18 %)
Not clear	P5-R1:" Unfortunately, my bank account was hacked"	Could not be assessed	3 (5 %)

5.3.6 Participants' Individual Characteristics Related to Online Security

5.3.6.1 Participants' Risk-Taking Behaviour: DOSPERT

Table 5.12 presents the mean scores for each DOSPERT subscale. Mean scores were calculated to allow comparison with the normative scores presented by Blais and Weber (2006).

Participants in the current study reported significantly lower willingness to engage in Ethical, Health/Safety, and Social risk-taking behaviours when compared with the Blais and Weber (2006) scores, indicating more cautious attitudes in these domains. No significant differences were found for the Financial and Recreational subscales.

When compared to the scale midpoint (4 on a 7-point likelihood scale), participants scored significantly below the midpoint on all subscales except Social, suggesting that participants were generally unwilling to engage in most types of risky behaviours. The Social domain was not significantly different from the midpoint, indicating a moderate willingness to take social risks.

Table 5.12: Mean scores for the DOSPERT subscales, with comparison with the standard scores from Blais and Weber (2006) and with the midpoints of the scale.

DOSPERT Subscale	Blais and Weber Mean[1,2]	Current sample Mean (SD)	Comparison with Blais and Weber	Comparison with midpoint
Ethical	2.82	1.35 (0.56)	T = 1.00, p < 0.001	T = 0.00, p < 0.001
Financial	3.27	2.73 (0.88)	T = 33.00, n.s.	T = 0.0, p <0.001
Health/Safety	3.44	2.48 (0.93)	T = 11.00, p = .003	T = 2.5, p < 0.001
Recreational	3.74	3.22 (1.05)	T = 37.00, n.s.	T = 17.0, p = 0.014
Social	5.43	4.34 (0.97)	T = 2.00, p < 0.001	T = 71.5, n.s.

1. Means were calculated from Blais and Weber (2006) to allow comparison, as the number of items in each subscale was different in the version of the scale used here.
2. SD could not be calculated as I did not have access to the raw data of Blais and Weber (2006)

5.3.6.2 Participants' Online Security Behaviour: SeBIS

Table 5.13 presents the mean scores for each SeBIS subscale. Mean scores were calculated to allow comparison with the scores presented by Egelman and Peer (2015) and adjusted as Egelman and Peer used 5-point ratings, whereas I used 7-point ratings.

Compared to the SeBIS means, participants in this study reported significantly higher scores in Device Securement, suggesting stronger engagement with Device Securement.

No significant differences were found for the Password Generation, Proactive Awareness, or Updating subscales.

When comparing subscale scores to the midpoint of the scale, participants scored significantly above the midpoint on Device Securement, Password Generation, and Proactive Awareness, indicating generally strong security behaviours in these areas. The Updating subscale did not differ significantly from the midpoint, suggesting only moderately secure habits in this domain.

Table 5.13: Mean scores for the SeBIS subscales, with comparison with the scores from Egelman and Peer (2015) and with the midpoints of the subscale.

Subscale	Egelman and Peer Mean	Current sample Mean (SD)	Adjusted mean[1]	Comparison with Egelman and Peer	Comparison with midpoint
Device Securement	3.21	5.50 (1.28)	3.93	T = 119.0, p = 0.008	T = 127.5, p = 0.002
Password Generation	3.25	4.85 (1.42)	3.46	T = 93.0, n.s.	T = 75.0, p = 0.039
Proactive Awareness	3.73	5.44 (0.92)	3.89	T = 98.0, n.s.	T = 133.5, p < 0.001
Updating	3.47	4.52 (1.62)	3.23	T = 60.0, n.s.	T = 82.0, n.s.

1. I used a 1–7 scale; the original SeBIS used a 1–5 scale, therefore, these are the subscale scores adjusted to a 1–5 scale to allow comparison with the original SeBIS results by multiplying by 0.714.

5.3.6.3 Participants' Concern about the Future: Consideration of Future Consequences Scale (CFC)

Table 5.14 shows the median scores for the two subscales of the CFC, CFC-Future and CFC-Immediate. She et al (2021) did not report the median or mean scores on the two CFC subscales, so I could not compare my findings statistically with theirs.

Participants' responses on the (CFC) scale showed a preference for future-oriented thinking. One-sample Wilcoxon signed-rank tests indicated that the median scores for both the CFC-F and CFC-I subscales were significantly above the scale midpoint. However, a related-samples Wilcoxon signed-rank test revealed that participants scored significantly higher on the CFC-F subscale than on the CFC-I subscale ($T = 0.0$, $p < .001$), suggesting that they prioritised long-term consequences over short-term outcomes when making decisions.

Table 5.14: Median scores on the two CFC components, with comparison with the midpoint of the scale.

	Median (SIQR)	**Comparison with "extremely uncharacteristic"**	**Comparison with midpoint of the scale**
CFC-Future	3.50 (1.00)	$T = 136.0$, $p < 0.001$	$T = 66.0$, $p = 0.003$
CFC-Immediate	1.25 (0.50)	$T = 36.0$, $p = 0.010$	$T = 0.0$, $p < 0.001$

5.3.6.4 Participants' Unrealistic Optimism

To assess unrealistic optimism, participants were asked to make six ratings, to compare themselves to their friends and another to a typical person of their age, on three stages: likelihood of encountering online threats, ability to detect them, and ability to deal with them. Table 5.15 summarises the median scores on each rating, with the Spearman correlations between the pairs of questions about "your friends" and "a typical person". There were significant positive correlations between each pair, showing that participants were probably drawing on the same concept. Therefore, I decided to use just the "your friends" questions for subsequent analysis.

On the other hand, there was no clear pattern in the correlations between the three stages of receiving, detecting and dealing with threats, with one significant negative correlation (Receiving – Detecting: $r = -0.69$, $p = 0.003$), one no correlation at all (Receiving – Dealing with: $r = 0.02$, n.s.) and one significant positive correlation (Detecting – Dealing with: $r = 0.66$, $p = 0.006$), so these were treated as three separate measures.

Table 5.15: Median scores for the six unrealistic optimism questions, with Spearman correlations between the "your friends" and "a typical person" pairs.

Compared to …	Median (SIQR)	Spearman Correlation (r) Friends – Typical person
your friends, do you think you are more or less likely to receive online threats and attacks?	1.0 (1.0)	r = 0.81 p < 0.001
a typical person of your age, do you think you are more or less likely to receive online threats and attacks	1.0 (0.5)	
your friends, do you think you are more or less able to detect whether a call, message, link, or website is an online threat?	4.5 (0.5)	r = 0.52 p = 0.037
a typical person of your age, do you think you are more or less able to detect whether a call, message, link, or website is an online threat?	4.0 (1.0)	
your friends, do you think you know how to deal with online attacks?	3.5 (1.50)	r = 0.52 p < 0.038
a typical person of your age, do you think you know how to deal with online attacks?	4.0 (1.0)	

Table 5.16 shows participants' ratings of the three Unrealistic Optimism questions in relation to their friends, with the comparison to the midpoint of the scales. Participants' ratings showed that they perceived themselves as less likely than average to receive online threats, and significantly better than average at detecting them and but only average at dealing with them. These findings show participants are unrealistically optimistic in two of the three stages of dealing with online threats.

Table 5.16: Participants' ratings of unrealistic optimism questions in comparison to friends (1 = much less likely, 3 = about the same, 5 = much more likely … than my friends).

UO dimension	Median (SIQR)	Comparison with neutral midpoint
Receiving threats	1.0 (1.0)	T = 12.5, p = 0.015
Detecting threats	4.5 (0.5)	T = 105.0, p < 0.001
Dealing with threats	3.5 (1.5)	T = 62.0, n.s.

5.3.6.5 Threat Interaction and Its Relationship with DOSPERT and SeBIS Scores

Using the behavioural patterns identified in section 5.3.4, participants were categorised based on their interaction with the threats into those who interacted with a threat (whether they suspected or did not suspect it was a threat) as Interactors and those who did not interact with the threats were categorised as Non-Interactors. Then, the differences in DOSPERT and SeBIS scores between these two groups were investigated.

A Mann-Whitney U test indicated a significant difference in DOSPERT Ethical subscale scores between Interactors and Non-Interactors (U = 12.000, p = .042). Median scores showed that Non-Interactors reported higher ethical risk-taking (Median = 6.00) compared to Interactors (Median = 5.00), suggesting that a greater willingness to take ethical risks did not correspond with more

interactions with online threats. No significant differences were found for the other DOSPERT subscales.

There were no statistically significant differences on the SeBIS subscale scores between the two groups.

5.3.6.6 Regression Analyses of Threat Interaction and Security Response Behaviours

A linear regression was conducted to examine whether individual differences predicted the percentage of appropriate responses to online threats. Predictors included SeBIS subscales, CFC-I and CFC-F, DOSPERT subscales, and Unrealistic Optimism items. The overall regression did not reach statistical significance, and none of the individual predictors significantly explained variation in participants' appropriate threat responses.

To explore whether participants' propensity to interact with online threats could be predicted by individual characteristics, binary logistic regression was conducted using different sets of predictors. First, none of the SeBIS subscales significantly predicted interaction behaviour (all $p > .05$). Similarly, the CFC subscales did not significantly predict interaction.

None of the UO items significantly predicted interaction behaviour. A separate model that included the five DOSPERT subscales produced unstable estimates and extremely large coefficients, suggesting issues such as multicollinearity or quasi-complete separation due to the small sample size ($N = 16$). Consequently, no reliable predictors of interaction behaviour were identified in the current analysis.

5.3.7 Comparison of the Results from the Survey and Diary Studies with Younger Saudi Adults

This section compares findings from the KSA survey study (Chapter 4) and the KSA diary study (Chapter 5). The diary findings reinforce several key patterns identified in the earlier survey, while also providing additional insights that were not fully captured through retrospective self-reported responses.

In terms of threat types, both the survey and the diary study indicate that phishing-related threats and malware are among the most frequently encountered online threats for younger adults in the KSA. This consistency suggests that the threats reported in the survey reflect real experiences in participants' everyday online activity.

The diary study provided a more detailed account of threat detection than the survey findings. In the survey, participants described detecting threats through negative consequences, such as device performance problems, unusual financial transactions, or account misuse, particularly in cases of malware and identity theft. For phishing and spear-phishing scenarios, participants reported content-based cues, such as requests for personal information and recognition of common scams. The diary study confirmed that participants primarily relied on content-based cues, including requests for sensitive information and incorrect information, to identify threats in real-world encounters. However, the diary data also revealed gaps in cue awareness, particularly with respect to technical indicators and common tactics, which were identified only through screenshot analysis. These insights into unreported cues were not accessible through the survey data and highlight the

value of the diary method in revealing both what users notice and what they overlook when detecting online threats.

The diary study also provides a more systematic and detailed evaluation of the appropriateness of participants' responses to online threats than was possible in the survey phase. In the survey, appropriateness was inferred from a small number of open-ended responses, which may have contributed to a relatively high apparent level of appropriate solutions. In contrast, the diary study explicitly assessed appropriateness based on whether participants took protective steps, such as verifying requests or checking links, rather than relying solely on the outcome. The diary findings show that most responses were appropriate; however, the results also reveal important patterns underlying inappropriate behaviour. Further analysis demonstrated that inappropriate responses were associated with situations in which participants interacted with a threat without initially suspecting it. By contrast, cases in which participants suspected a threat but still responded inappropriately were relatively rare. This pattern-based analysis was not accessible in the survey data and highlights the role of early suspicion in shaping responses.

The diary study also provides context for the survey results related to participants' perceived ability to detect and handle online threats. In the survey study, participants rated their computer and security knowledge, as well as their ability to identify online attacks, as average to above average. This pattern aligns with findings from the unrealistic optimism measures, which show that participants tended to view themselves as less likely than their friends to encounter online threats and more capable of detecting them, while expressing less confidence in their ability to handle such threats effectively. Both the survey and diary phases measured intended security behaviour using the SeBIS scale. In both studies, participants showed stronger intentions for basic security behaviours, such as device securement. They were less likely to engage in behaviours requiring ongoing effort, including software updating or password management.

Collectively, the survey and diary findings indicate that while younger adults in the KSA are frequently exposed to online threats and generally confident in their ability to detect them, real-world responses are often reactive and limited. This highlights a gap between perceived capability, intended security behaviour, and enacted responses in everyday online contexts.

5.4 Discussion

This study used a diary-based approach to investigate how younger Saudi adults experience online threats. The diary method is still relatively uncommon in cybersecurity research, but it is well established in Human-Computer Interaction (HCI) (Lazar et al., 2015).

Unlike traditional surveys that rely on predefined threat categories (e.g. asking whether participants have encountered phishing or malware) and memory for past events, the diary method allowed participants to monitor and report incidents as they occurred, in their own terms. This participant-led approach provided richer, more contextualised insights into the actual threats they experienced and how they reported shortly after the threats occurred. To encourage daily participation and reduce fatigue, the diary entries were kept short. Each entry started with a yes/no question and included only two open-ended questions. The questions asked participants to explain what happened and how they recognised the threat. This simple structure helped participants stay

engaged and reflect on their experiences without needing a lot of time or effort. The method also allowed me to ask participants to take screenshots of the threats they received, providing objective evidence of the threats and the potential for further analysis of them.

To turn to the research questions addressed in this study:

RQ1: How frequently do younger Saudi adults encounter different types of online threats?
The first research question investigated the frequency with which younger Saudis encounter different types of threats. The diary entries revealed that phishing was the most frequent threat reported by the participants during the study period. This finding supports the findings from the previous survey study with KSA younger adults presented in Chapter 4. It also agrees with the findings of Aljeaid et al. (2020), who studied phishing susceptibility among Saudi university students. In one experiment they conducted, an email imitating an urgent message from the university's IT department was sent to 165 students, and 27% clicked a malicious link within the email. In another phishing experiment, they shared a fake car rental site via social media platforms such as WhatsApp, Facebook, and Telegram, resulting in 47% of participants engaging with the phishing content, particularly among higher education students.

However, about a quarter of the reported threats in the current study did not have enough details to identify the specific type. Some responses were vague or incomplete, making it difficult for me to determine the threats accurately. This highlights an issue of using open-ended questions to make the questionnaire easy for participants. While the question format allows participants to express themselves in any manner they choose, the quality of the data relies heavily on how well the participants describe the incidents.

The number of threats participants reported equates to an average of approximately 4.04 threats per month. While this may appear to reflect a relatively low rate, participants may not have reported every incident they experienced. So, this rate of receiving threats may well underestimate the number of threats younger Saudis encounter. I could not find any information about how many online threats a typical younger Saudi user might encounter in a given period, or indeed any user anywhere. As such, this reported frequency should be taken with caution. It may represent not the actual threats participants faced but what they noticed, decided to report, or thought were important to share. Since this is a small exploratory study, the findings provide some initial insights but not generalisable rates of online threat encounters.

RQ2: What purposes do these threats serve?
The second research question investigated the purposes of the threats that younger Saudis encounter. This was measured by their perceptions of the purposes of the threats. However, the purpose of the threats in over half of the responses could not be determined due to limited information provided in participant responses. Again, this was due to the use of the open-ended question format in the diary. Instead, purposes were determined from participants' responses and screenshots.

Participants identified two main purposes for the threats they encountered: financial fraud and data theft. This agrees with a study that investigated cybercrime awareness among Saudi students, which found that financial gain was one of the main motivations behind cybercrimes (Ismail & Farah,

2017). Similarly, a study by Bera et al. (2023) analysed thousands of phishing emails from publicly available datasets to identify common patterns in phishing email content. Using computational techniques, they found that data theft and financial fraud were recurring themes, highlighting how phishing attacks are often designed to extract personal or financial information from recipients.

RQ3: How do younger Saudi adults recognise and respond to online threats?

The third research question investigated how younger Saudis recognise and respond to online threats. An important finding that emerged from the study was the identification of six distinct behavioural patterns based on how participants recognised, responded to, and later verified online threats. These patterns were constructed from three key stages: whether the participants initially suspected the incident was a threat, whether they interacted with it, and whether they ultimately identified it as a real threat. The most common pattern involved suspicion followed by no interaction, and then realisation that the threat was real. Other patterns included no suspicion followed by interaction with the threat (often leading to inappropriate responses), and cases where suspicion was present but participants still engaged with the threat.

These patterns offer valuable insight into the steps users follow in real-world contexts when facing online threats. In particular, they reflect behavioural vulnerabilities such as carelessness, cognitive fatigue, or habitual actions that may lead to interaction with suspicious content despite some awareness. This supports prior work by Wang et al. (2021), who identified behaviours such as carelessness, where users fail to notice the security issue, and thoughtlessness, when they overlook potential risks or consequences, as common pathways to exploitation.

The patterns also highlight the critical role of suspicion in user responses to online threats. When participants expressed suspicion but chose not to interact, they generally avoided negative consequences, suggesting that suspicion can serve as a protective factor. This observation is consistent with the concept of Generalised State Suspicion (GSS), introduced by Levine and McCornack (1991), which refers to a cognitive state where individuals are more alert to potential deception. GSS is central to the Suspicion, Cognition, and Automaticity Model (SCAM) developed by Vishwanath et al. (2018). In their study, undergraduate students at an American university were sent simulated phishing emails as part of an experiment. The researchers then conducted a follow-up survey to assess students' levels of suspicion, cognitive effort, and automaticity in processing the emails. The findings showed that students who experienced higher suspicion were more likely to detect phishing attempts and avoid falling for them. This reinforces the idea that fostering user suspicion can be an important strategy for enhancing online threat detection and response.

A study by Nthala and Wash (2021) provides further support for the behavioural patterns observed in this research. Their study involved 31 non-IT university staff members, aged between 18 and 45, who were interviewed to explore how they process phishing emails. The researchers identified a four-stage process through which participants handled suspicious emails: getting context (deciding whether the email was relevant), reading the message (noticing cues or inconsistencies), enacting the request (e.g. clicking a link or replying), and seeking closure (verifying the message with others or reporting it). Importantly, suspicion could emerge at any stage, usually triggered by discrepancies during this sense-making process.

The relationship between suspicion and response appropriateness offers further insight into the behavioural patterns identified in the diary data. Specifically, participants who fell into the pattern of not suspecting and interacting consistently responded inappropriately, for example, by clicking on suspicious links, demonstrating clear engagement with the threat. By contrast, in the pattern where participants suspected a threat but still interacted, responses tended to be more cautious, and inappropriate actions were much less common. This suggests that the presence of suspicion not only supports initial threat detection but also influences the quality of user responses, even when engagement with the threat occurs.

RQ4: What cues do participants use to detect threats?

The fourth research question investigated the cues that younger Saudis use to detect threats. Participants most frequently used cues from the "Language and Content" category, including requests for sensitive information and incorrect information. Technical indicators, such as suspicious URLs or unknown phone numbers, were also commonly mentioned. A third key category was "Prior Knowledge," reflecting the role of previous experience and warnings from friends or the media (Nthala & Wash, 2021; Rader et al., 2012). Interestingly, I identified a number of cues that participants did not report, such as suspicious or hidden URLs, “too good to be true” offers, and limited time offers, suggesting that users may miss some important cues.

During the analysis of cues, I adapted the Phish Scale (Steves et al., 2020), a tool originally developed to assess the difficulty of detecting phishing emails. While the Phish Scale provides a useful framework for categorising detection cues, it was designed specifically for email-based threats. Therefore, it was necessary to expand the categories to account for other threat vectors encountered by participants, such as SMS, phone calls, and social media platforms. This adaptation highlights the flexibility and practical relevance of the Phish Scale but also acknowledges the developers’ own recognition that their classification of threat cues is not exhaustive and would benefit from further refinement:

“We recognise this list is not exhaustive and will be expanded… we anticipate some form of weighting may be useful to reflect cue saliency” (Steves et al., 2020, p. 4).

As the authors suggest, assigning weight to cues based on their importance is a complex task, given the variation in how different individuals perceive and respond to threats. This challenge was evident in the current study, where some important cues (e.g. suspicious links or too good to be true) were missed by the participants.

RQ5: What is the relationship between younger Saudi adults’ individual characteristics (risk taking, unrealistic optimism, consideration of future consequences, online security behaviours) and their experiences of online threats?

The final research question investigated a number of individual characteristics of younger Saudis (risk taking, unrealistic optimism, consideration of future consequences, online security behaviours) and their experiences of online threats.

To explore the relationship between participants' experiences with online threats and their self-reported online security behaviours, the SeBIS scale was used. Based on diary entries, participants were categorised into two groups: those who interacted with threats (Interactors) and those who

did not (Non-Interactors). In contrast to what Egelman et al. (2016) reported, that SeBIS scores were found to be predictive of actual behaviours, this sample showed no difference on their SeBIS scores between those who interacted with the threats and those who did not.

This result suggests that participants' self-reported behaviours may not strongly predict whether they will interact with online threats in real-life sitiuations. However, the small sample size (N = 16) may affect the statistical power of this analysis, and it is possible that real effects were not detected due to this constraint.

Comparisons were also made with normative data reported by Egelman and Peer (2015), who sampled American participants nearly a decade earlier. The current sample of younger Saudi adults scored significantly higher only on the Device Securement subscale. Scores on other subscales, such as Password Generation and Proactive Awareness, did not show significant differences compared to the earlier American norms. These findings may reflect not only changes over time in how online security is understood and implemented by individuals but also cultural and demographic differences. For instance, Egelman and Peer's sample included a broader range of ages and came from a Western context, while the current study was conducted with on younger adults in KSA. Such cultural and generational differences may shape users' security attitudes and exposure to security-related guidance.

Additionally, the higher Device Securement scores in the current sample compared to the previous norms might be influenced by technological advances over the last decade. Since 2015, features such as biometric authentication and automatic screen locking have become common in smartphones, which likely promote better security habits. This issue was discussed in a recent study by Huang et al. (2023), who noted that some of these features are not included in the original SeBIS items.

To explore how participants' risk-taking related to their interaction with threats, the two groups (interactors and non-interactors) were compared, and I found that interactors had significantly higher Ethical DOSPERT scores. This is contrary to the assumption that higher risk-taking would lead to more interaction with potential threats. This counterintuitive pattern may be understood in light of Blais and Weber's perspective on domain-specific risk-taking**,** which argues that individuals may take risks in one domain (e.g. ethical, financial) but behave cautiously in others (e.g. in this instance, online security). Thus, being more willing to engage in ethical actions does not necessarily translate into careless or impulsive behaviours in online threat situations. Supporting this, Ayyagari and Crowell (2020) argued that while DOSPERT covers various domains (e.g. ethical, recreational), it does not effectively capture information security risks. Their study involved developing a new Information Security Risk Scale tailored to cyber-related behaviours, arguing that DOSPERT's existing domains are not representative of real-world cybersecurity threats.

Despite expectations that individual characteristics might influence whether participants interacted with online threats, the regression analyses found no significant predictors of interaction behaviour or appropriate responses. Neither self-reported online security behaviours (as measured by SeBIS) nor psychological traits such as risk-taking (DOSPERT), consideration of future consequences (CFC) or Unrealistic Optimism were associated with participants' likelihood of interacting with threats or

responding appropriately. These results contrast with prior research that has linked such traits to security outcomes (e.g. Egelman & Peer, 2015). Again, the small sample size may account for this.

5.4.1 Limitations of the Study

As has already been mentioned, this study involved a small sample, limiting generalisability. Recruitment challenges were the main reason for the small sample size. Although over 30 individuals initially responded to the study invitation, only 16 agreed to participate after receiving full details. Many did not respond further, which may be due to the level of commitment required, specifically, the need to monitor and report online threats over a 30-day period.

There was a notable gender imbalance in the sample, with more women completing the diary study than men. This pattern is consistent with prior research showing gender differences in online survey participation, with women often demonstrating higher response rates (Wu et al., 2022).

Even though this study used a diary format, which was designed to provide more detailed and accurate information because it was reporting on events experienced the same day, it still relied on self-reported data that may have been subject to bias or inaccuracies. As discussed above, the dependence on daily reporting might have resulted in the under-reporting of threats. Additionally, participants sometimes provided data that was not directly relevant to the topic. A similar issue was noted by Turner et al. (2022) in their diary study on smart home security, where participants occasionally reported unrelated digital experiences. This was particularly common when participants were asked to reflect on concepts they did not fully understand, such as cybersecurity.

To address these limitations, particularly the ambiguity in identifying threat types and cues used due to the open-ended question format, the next study employed a more structured diary design. It was conducted with younger adults in the UK and aimed to recruit a larger sample of participants and to improve the clarity of information collected, enabling a more detailed analysis of participants' experiences.

Chapter 6 Diary Study of the Experience of Online Threats for UK Younger Adults

6.1 Introduction

This chapter presents findings from a diary study conducted with younger adults in the UK. The study was designed to examine the type and frequency of online threats and how participants detect and respond to them.

Building on the insights from the previous diary study with younger adults in the KSA, this study refines the design by including structured multiple-choice questions in the diary questionnaire. This change aims to reduce the ambiguity in participants' responses and facilitate the analysis.

This study builds on the overall research Objectives 1–4 outlined in Chapter 1. It focuses on examining younger British adults' experiences with online threats, including their frequency, detection, and behavioural responses, as well as the influence of individual characteristics.

This study will answer the following Research Questions:

RQ1: How frequently do younger British adults encounter different types of online threats?

RQ2: What cues do younger British adults use to detect online threats?

RQ3: How do younger British adults respond to online threats?

RQ4: What is the relationship between younger British adults' individual characteristics (risk taking, unrealistic optimism, consideration of future consequences, online security behaviours) and their experiences of online threats?

In addition, the findings are compared with those from the Saudi sample to address Objective 4, which explores cultural similarities and differences between the two groups.

Table 6.1 below presents the mapping between the overall research objectives and the study-specific research questions.

Table 6.1: Mapping of thesis objectives to UK diary study research questions.

Thesis objectives	**UK diary study research questions**
Obj. 1: Identify online threat types and frequency	RQ1
Obj. 2: Examine how younger adults detect and respond to online threats	RQ2 and RQ3
Obj. 3: Investigate the effect of individual characteristics on online security experiences	RQ4
Obj. 4: Compare cultural similarities and differences between UK and KSA participants	Addressed through the cross-national comparison section

6.2 Method

6.2.1 Design

The longitudinal format of this study would allow for examining the threat types that a sample of UK younger adults have encountered and how they detect them. The design of this study has been refined and modified in response to the challenges encountered in the Saudi diary study reported in Chapter 5.

One of the challenges that was encountered during the analysis of the Saudi study arose from using open-ended responses for all questions. This resulted in vague and ambiguous answers, making the analysis process challenging and leading to a number of reported threats being categorised as unclear. Additionally, some participants may have missed some important details or provided unclear answers about threats, particularly about how they detected the threats and the purpose of threats, which did not help in identifying and analysing the cues they used to recognise the threats.

To address these limitations, the design of this study was refined while keeping the main goal, which is to have participants report their experiences with online threats over an extended period.

The online diary questionnaire used as many multiple-choice questions as possible to improve clarity and ease of reporting, ensuring that participants could provide structured and consistent responses.

In a previous diary study, recruiting participants proved challenging, with only 16 participants taking part despite considerable effort. To address this in the current study, the diary structure was modified to improve engagement and data quality. Also, the diary period was shortened, and participant numbers increased to collect sufficient data without overburdening participants.

This study was conducted in two phases:

- **Phase 1** involved a pre-diary questionnaire that collected some information about participants' prior experiences with online threats.
- **Phase 2** was the longitudinal diary phase, carried out in two rounds of different durations:
    - **Round 1** (14 days, 14 participants): Conducted in early October 2024, participants were asked to monitor and report any online threats they encountered each day. A total of 60 threat reports were submitted. The number of reports was roughly equivalent to what was collected over a full month in the previous study with a similar number of participants (N = 16). However, participant engagement declined slightly during the second week, indicating possible fatigue.
    - **Round 2 (**7 days, 31 participants): To further increase data collection while reducing participant fatigue, a second round was conducted with a larger sample over a shorter period. This round yielded 61 threat reports. Although some decline in engagement was still observed toward the end, the shorter duration appeared to reduce fatigue compared to the first round.

Similar to the previous diary study, this study consisted of three main parts: an initial questionnaire, a diary part, and a final questionnaire.

The initial questionnaire included a new section that was not present in the previous study, which focused on participants' familiarity with phishing and their past experiences with phishing attacks. These questions aimed to assess participants' initial awareness of the term and their previous experiences with phishing attacks. Participants were first asked if they were familiar with the term "phishing," followed by an open-ended question to describe what it meant to them. This was used to explore their understanding in their own words. Afterwards, all participants were shown a brief definition of phishing to ensure consistent understanding across the sample. They were then asked whether they had ever experienced phishing attacks, whether they had ever been caught out by such messages, and if any serious consequences had occurred. I deliberately did not use phrasing such as "being a victim of a phishing attack" as this could be interpreted as judgmental by participants. However, "caught out" was further explained as "taking action because you thought it was a genuine message/email". This questionnaire was of interest in itself to give a general idea of how often young British people believe they experience phishing attacks. It also facilitated the recruitment of a sample of participants for the diary part.

The rest of the questionnaire (e.g. demographic questions and scales such as SEBIS, DOSPERT) was similar to the previous study.

The diary part retained the same initial screening question about threats. The changes from the previous diary included questions that asked about the device on which the threat occurred, the channel through which it was received, and the type of threat. There was also a question asked to select from a list of cues they used to suspect it was a threat, whether they were aware of this type of threat, and whether it turned out to be a threat. Most questions were multiple choice to make the questionnaire very quick to answer.

Four open-ended questions were asked for further information, one about the cues used to suspect a threat, two about how the participant interacted and dealt with the threat and one about what they thought the purpose of the threat was.

To better understand how participants identified threats, they were asked to select from a list of possible detection cues. The most frequent cues that have been used by Saudi participants (based on the Phish Scale and the expansion I did to the scale to cover new cues) were provided in a list, which allowed multiple answers, to help participants select and remember all the cues that drew their attention to the threats when they encountered it.

One adaptation was the cue "suspicious email/phone number/username," which was derived from the Phish Scale's original item "sender display name and email address". The wording was intentionally broadened to reflect the wider range of communication platforms used in this study, including SMS, voice calls, and social media applications. For the full list of cues, see Section 5.2.5.

Similar to the previous study (Section 5.2.1), the study employed a number of measures to investigate the relationship between individual characteristics and online security behaviours.

An additional section was included at the end of the study asking participants to reflect on their experience of the diary. In the final questionnaire, participants were asked whether they felt the study period was typical in terms of the number of online threats they usually receive**.** They were

also asked if their attitude toward online threats had changed as a result of participating in the study and whether they believed they would be more vigilant about monitoring online threats in the future**.** Additionally, participants reflected on whether they felt they would be better at detecting online threats**,** as well as whether they believed they had improved in dealing with such threats.

6.2.2 Participants

Inclusion criteria to participate in the study were to be aged 18 to 40 years, living in the UK and fluent in English. 66 people responded to the advertisement on the Prolific platform and answered the initial questionnaire in full. Their demographics are described in the Initial Group column of Table 6.1. Of these participants, 50 were invited to participate in the diary phase to create a sample reasonably balanced for age and gender and randomly chosen with respect to how frequently they reported encountering online threats. 45 people accepted the invitation to the diary phase and completed the whole phase and the final questionnaire. Their demographics are described in the Diary Group column of Table 6.2.

Various analyses were undertaken to compare participants in rounds 1 and 2 of the diary study, but there were no notable differences, so the two rounds were combined.

Table 6.2: Demographic characteristics of the participants**.**

	Initial Group N = 66	**Round 1**	**Round 2**	**Diary Group Total N = 45**
Age				
Range	18–40	22–40	18–40	18–40
Mean	29	31	30	31
Gender				
Men	35 (53 %)	6 (40 %)	17 (57 %)	23 (51 %)
Women	28 (42 %)	9 (60 %)	11 (37 %)	20 (44 %)
Non-binary	3 (5 %)	0	2 (7 %)	2 (4 %)
Education level				
High School	28 (42 %)	3 (10 %)	16 (53 %)	19 (42 %)
Bachelor's	25 (38 %)	8 (27 %)	8 (27 %)	16 (36 %)
Master's/PhD	13 (20 %)	4 (13 %)	6 (20 %)	10 (22 %)
Employment status				
Working (f/t or p/t)	51 (77 %)	12 (80 %)	22 (73 %)	34 (76 %)
Not currently working	9 (14 %)	3 (20 %)	5 (17 %)	8 (18 %)
Students (f/t)	6 (9 %)	0	3 (10 %)	3 (7 %)
Studied or worked related to online security	4 (6 %)	1 (7 %)	1 (3 %)	2 (4 %)
Knowledge of the internet ("Not at all knowledgeable" scored as 1 to "Very Knowledgeable" scored as 7)	Median: 6.0 SIQR: 1.0 Z = 6.27 p < 0.001	Median: 5.0 SIQR: 1.0 T = 101.00 p = 0.002	Median: 6.0 SIQR: 1.0 T = 333.00 p < 0.001	Median: 6.0 SIQR: 1.0 Z = 5.08 p < 0.001
Knowledge of online security ("Not at all knowledgeable" scored as 1 to "Very Knowledgeable" scored as 7)	Median: 5.0 SIQR: 1.0 Z = 4.23 p < 0.001	Median: 5.0 SIQR: 0.5 T = 94.00 p = 0.007	Median: 5.0 SIQR: 1.0 T = 296.00 p = 0.009	Median: 5.0 SIQR: 1.0 Z = 3.62 p < 0.001

Both the Initial and Diary Groups covered the full age range of interest and had a mean age approximately in the middle of that range. The gender balance was reasonable, with slightly more men than women in both groups, but some representation of non-binary individuals. The educational level of both groups was skewed towards people with higher education, with 58 % of the Initial Group and the Diary Group having a degree. This means the participants were more qualified than the overall UK population, in which in 2021, 33.8% of people had a bachelor or higher degree (Office for National Statistics, 2023). Most participants in both groups were in full-time or part-time employment, with small numbers not currently working or students. Occupations were very varied, from security guard to research consultant.

Participants were asked whether they had ever studied or worked in an area related to online security. Small numbers of participants reported that they had, but only four in the Initial Group and two in the Diary Group were thought to have any detailed knowledge relevant to the study.

Participants were asked to rate their knowledge of the internet and online security issues on Likert items from “not at all knowledgeable” to “very knowledgeable”. In all cases, ratings were significantly above the midpoint of the scale (measured using the Wilcoxon one-sample signed ranks test, with Z approximation as the sample size is greater than 30 in both cases) (Siegel & Castellan, 2000).

6.2.3 Materials

Participants completed three online questionnaires throughout the study: an initial questionnaire, a diary questionnaire, and a final questionnaire. All questionnaires were administered via Qualtrics (qualtrics.com) and distributed to participants through the Prolific platform. Full versions of these questionnaires are in Appendix H: UK Diary Study Questionnaire , Appendix I: Pre-study Questionnaire for the Diary Studies and Appendix J: Post-study for the UK diary study.

6.2.3.1 Initial Questionnaire

The initial questionnaire started with an information screen and a consent form**.** It then assessed familiarity with the term **"**phishing"**,** asking whether participants had heard of it and, if so, how they would define it.

To ensure that participants understood the rest of the questionnaire, the following explanation was then offered:

> "Phishing" is when an online attacker tries to trick you into providing sensitive information (such as your login or bank details) or downloading damaging software to your device. This usually happens by sending you an email or online message that you are asked to respond to or click on a link. A very common "phish" these days is a message saying you have a parcel, but that you need to log into a website or pay an extra charge before it can be delivered. The most serious attacks are when the software takes over your device and you are asked for money to restore access (this is ransomware and it's what happened to a number of NHS hospitals in London recently)”.

Participants were asked whether they had ever encountered phishing attacks, using a 7-point Likert scale with responses ranging from “never” (scored as 1) to “from time to time” (scored as 4) to “very often” (scored as 7)**.**

They were also asked whether they had ever been caught out by a phishing attack (same rating scale), and if so, whether the incident had led to serious consequences (response options: “yes,” “no,” or “don’t remember”). Those who answered “yes” were prompted to describe the consequences briefly.

Following this, participants completed the 26-item DOSPERT scale to assess their risk taking, presented on two screens (13 statements per screen). As in the Saudi diary study, some modifications were made to ensure the scale was suitable for the British young adult sample. The scale words were updated to be more understandable. For example, in the Recreational domain, one of the items is: “Going whitewater rafting at high water in the spring” was replaced with: Going jet ski-ing in very rough waves. Additionally, some items from the Financial and Ethical domains were removed. See Appendix F for a table with original and modified versions of the scale.

Next, participants were asked to complete the SeBIS scales, with the original 16 items. These items were presented on two screens with 8 statements per screen.

At the end of this initial questionnaire, participants were asked a set of demographic questions about their age, gender, educational level, and whether they had studied or worked in an online-related security field. They were also asked to rate their general knowledge of the Internet and their online security on a scale from “not at all knowledgeable” (1) to “very knowledgeable” (7).

6.2.3.2 Diary Questionnaire

As in the previous diary study, participants were asked to report any online security threats they encountered each day during the study period.

The changes in this version were that if participants reported that they encountered a threat, they were asked about the number of threats they encountered that day, and then they were able to enter up to three entries every day of reporting.

For each reported threat, participants were asked to provide further details by answering a series of questions. Specifically, they were asked to:

1. Indicate the device type they were using when they encountered the threat (Desktop, laptop, tablet, smartphone).
2. Specify the channel through which the threat was received (email, text message, voice message, social media, website, app).
3. Upload a screenshot of the threat, if possible.
4. Classify the type of threat from a predefined list, including phishing, spear phishing, malware/virus, ransomware, and spoofed websites. An additional option allowed participants to describe other threat types, and a "not sure" option was provided for uncertain cases.
5. Identify how they detected the potential threat by selecting from a list of common cues, such as requests for sensitive information, incorrect details (e.g. false parcel delivery notification),

suspicious or unknown email addresses, lack of sender/business information, too good to be true, suspicious links, attempts to impersonate well-known companies, spelling or grammatical errors, and unprofessional presentation. An open-ended option, "other", was also available for participants to describe additional cues.

6. Indicate whether they were already aware of this type of threat by selecting one of three options: 1 (Yes), 2 (I think so), or 3 (No).
7. Select from a set of options to indicate how they became aware of the threat (their awareness source). The available options were: television/newspaper, social media, family or friends, or previous personal encounters.
8. Report whether they had interacted with the threat and, if so, describe their interaction in an open-ended response.
9. Whether they interacted with the possible threats by responding to a yes/no question
   9.1 If they selected yes, they interacted with the threat, they were asked to describe how they interacted.
10. Whether they did anything to figure out or resolve the issue (e.g. delete the account, report it to www.actionfraud.police.uk)
11. Indicate whether they understood the purpose of the threat using a 5-point scale, ranging from 1 "I have no idea", 3 "I have some idea" to 5 "I am sure about the purpose of the threat".
    11.1 If they selected any score from 2 to 5, they were asked to describe what they believed the purpose of the threat was.
12. Indicate whether they thought it was a threat using a 5-point scale ranging from 1" definitely not a threat", 3 "still not sure" to 5" definitely a threat".

6.2.3.3 Final Questionnaire

The final questionnaire consisted of the same questions about the CFC scale and the UO questions that have been used in the KSA diary study (see Section 5.2.3.3).

However, in contrast to the modified version of the CFC scale used in the KSA sample, the current study employed the revised, two-factor CFC-14 scale (Joireman et al., 2012), with subscales assessing concern with future consequences (CFC-F) and concern with immediate consequences (CFC-I). CFC-14 used 7-point Likert items, ranging from 1 (extremely uncharacteristic of me) to 7 (extremely characteristic of me)**,** to indicate the extent to which each statement described participants, with higher scores reflecting a greater alignment with the described behaviour.

A section of the final questionnaire was added to gather more information about participants' experience of being in the study:

- A question sked to rate how typical the study period was in terms of the number of online threats they encountered, using a 7-point scale (from 1 = "I probably received a lot fewer threats in this period" to 7 = "I probably received a lot more threats/scams in this period", with 4 indicating "Fairly typical"). With an optional open-ended response to explain the rating.
- Describe any threats they found particularly interesting or problematic during the study (open-ended).

- a rating of whether participants' attitude toward online threats had changed as a result of the study ("not at all" scored as 1 to "a great deal" scored as 7)**,** with an optional open-ended response for further explanation.
- Questions asking whether participants expected to be more or less vigilant about online threats in the future and whether they believed they would be better at detecting and handling threats moving forward (7-point rating times) from "much less" to "much more") with an optional follow up open-ended questions for elaboration.

- An invitation to share any additional comments about experience in the study.

6.2.4 Procedure

Participants were recruited through a brief advertisement on the Prolific website, which provided a brief explanation of the study's objectives and procedures. The eligibility criteria required them to be between 18 and 40 years old and regular users of the internet and smartphones.

Upon signing up, Participants received a file containing examples with clarification images of the most common and current online threats that have targeted individuals. This included non-technical descriptions of all the major online threat types, gathered from a number of sources. They were also told not to worry about whether something turned out to be a threat or not, as the researchers were interested in how people generally monitored for online threats, whether they turned out to be threats or not. They were asked to keep this file during the study period and refer to it when needed.

In the Initial questionnaire, participants completed an initial survey (5–10 minutes) assessing their online security experiences, risk perceptions, and demographics**.** Of the 66 who completed the initial questionnaire**,** 45 participants completed the diary part, while 21 participants completed only the initial questionnaire

During the Diary questionnaire period, each evening at 8 PM, they received a questionnaire to report any threats encountered that day. If they had no encounters, they could simply report "none". They could report up to three threats per day.

Final questionnaire: Participants completed a final questionnaire (5–10 minutes).

If participants missed several days, they were sent a reminder message, which prompted them to catch up. They were also offered the possibility to add days at the end of the initial period, if they were not able to complete a diary questionnaire on some days, for example, because they were away.

Participants were encouraged to contact the researchers through the Prolific online messaging service (researchers are not allowed access to Prolific participants' email addresses, so must communicate through Prolific) at any point during the study and for any reason, but particularly if they had any queries or worries about threats.

As participants on Prolific are reimbursed per task, participants were offered GBP1.50 for the initial and final questionnaires, GBP1.00 for each threat diary questionnaire, plus a GBP3.00 bonus for

completing all the questionnaires. That meant that in total, participants received GBP 20.00 for the 14-day version of the study.

The study was reviewed and approved by the Physical Sciences Ethics Committee at the University of York. (reference: Aldaraani20230711)

6.2.5 Data Analysis

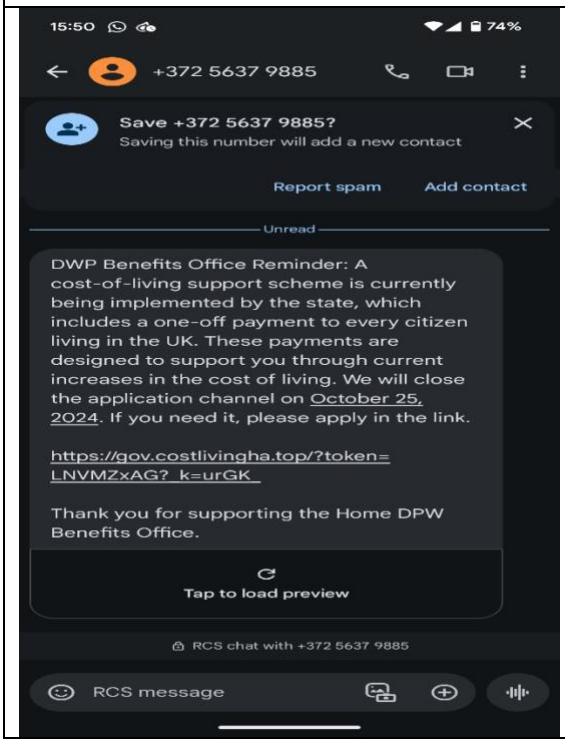
The rating data were often not normally distributed, so non-parametric tests were used.

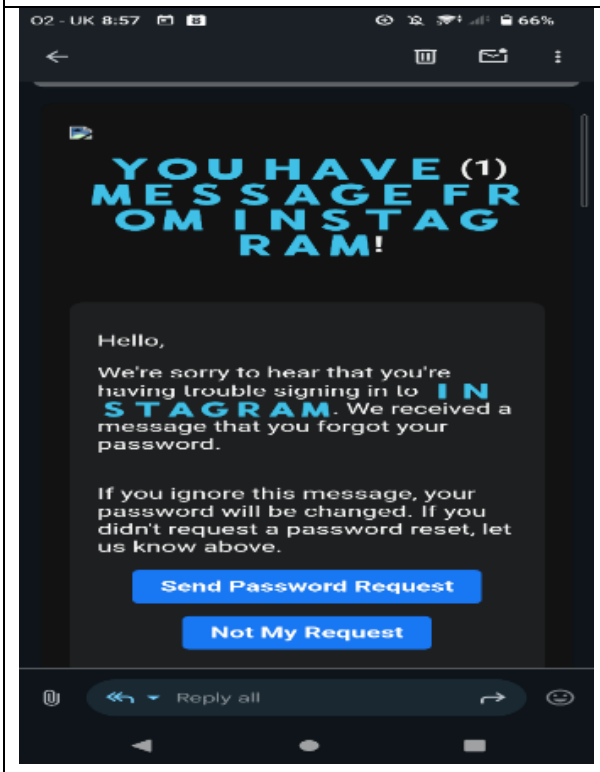
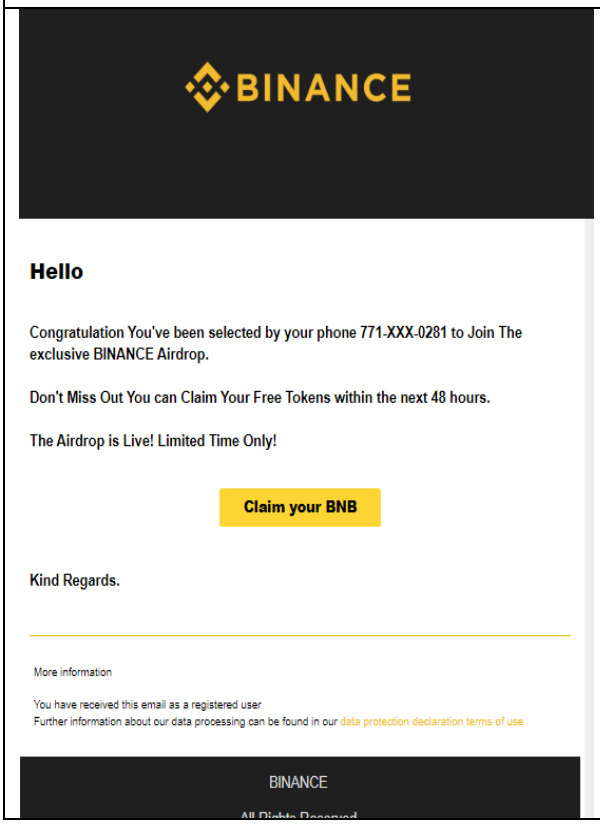
To assess how the sample's risk-taking (DOSPERT), security behaviour (SeBIS), and CFC scores compared to established normative values from the original validation studies, using one-sample Wilcoxon signed-rank tests**.**

Responses to open-ended questions were analysed using separate content analyses for each question. All responses for a particular question were carefully read and a set of appropriate categories was created, with appropriate sub-categories if needed.

I reviewed screenshots of online threats submitted by participants in conjunction with the cues they listed as having been used to identify it as a potential threat. Any cues which participants had not mentioned were identified. All the screenshots were also reviewed by a second researcher (one of my supervisors) and a small number of additional cues not identified by the participants were noted. Three examples of this analysis are given in Table 6.3.

Table 6.3: Examples of Screenshots of online threats submitted by participants with cues identified by the participant and those identified by the researchers

Screenshot	Cues identified by the participant	Cues identified by the researchers
	Requesting sensitive information Suspicious link	Unknown number Mimics a work or business process Spelling mistake (DWP, then DPW) Incorrect information (use of "the state", incorrect in the UK)

Screenshot	Cues identified by the participant	Cues identified by the researchers
	Suspicious email address	Unprofessional layout/presentation Grammatical error (“let us know above” when the link is below)
	Incorrect information Suspicious email address	Sense of urgency

6.3 Results

6.3.1 Initial Questionnaire

6.3.1.1 Participants' Understanding of Phishing

To ensure that participants understood the terminology in the questionnaire and to explore their understanding of current online threats, participants were asked whether they were familiar with the term "phishing", as it is the most common type of online threat individuals are likely to encounter.

In all, 62 (94 %) participants said they were familiar with the term, 3 (5 %) were not sure, and one participant (2 %) did not know the term. They were asked to explain what the term meant to them and then provided with an explanation. Five participants either did not answer the question or provided incorrect definitions, so a content analysis was conducted on 61 responses. The main categories were the attacker, the channel the phish was received through, the purpose of the phish and what the phish was targeting (Table 6.4).

Participants' identified by codes indicating their study phase: "P" codes (e.g. P7) for diary participants and "I" codes (e.g. I2) for initial questionnaire participants.

In general, participants had a good understanding of at least the most common aspects of phishing. In terms of the attacker, nearly a third of participants (33 %) mentioned someone impersonating another individual or organisation, and a further fifth (21 %) mentioned more general terms such as "hackers" or "scammers". The remainder of the participants concentrated on describing the phish itself without mentioning who the attackers might be (e.g. "receiving scam emails that usually have dodgy links in them" I41).

In terms of the channels participants mentioned that they received phishing attacks through, email was the most frequently mentioned channel (by 61 % of participants), but numerous other channels were mentioned, including links, which might be within emails or webpages, text, voice or simply messages and through attachments. Very few participants mentioned channels in terms of devices, so no coding was undertaken for devices on which phishing is received.

Often the purpose of the phish was described in rather benign terms (these were not specifically coded) such as to "get" or "obtain" information (e.g. "in order to get your details" P2; "to obtain personal data" P19), but a minority of participants used stronger terms such as "deception", "compromise", "steal" or "use information maliciously".

Finally, many participants mentioned what was being targeted by the phishing attack, with personal information being the most frequently mentioned target (nearly three-quarters of participants, 72%), followed by financial data or money (21 %). A few participants (13 %) mentioned specific types of information, such as passwords or bank account details.

Table 6.4: Definitions of "phishing" given by participants (N = 61).

Category/subcategory	Examples	N (%)
Attacker		
Someone impersonating an individual or organisation	Pretending to be a legitimate company or individual (P7) Someone sends a fake email pretending to be someone else/a company (I2)	20 (33 %)
General terms	Cybercriminals (I5) Hackers (I19) Scammers (P17)	13 (21 %)
Channel of the phish		
Email	Emails that pretend to be from Amazon etc (P34)	37 (61 %)
Link	Hoping to get you to click a malicious link (P36)	16 (26 %)
(Text) message	Emails or other messages (I18)	14 (23 %)
Website	A fake website that looks like the real deal (P32)	9 (15 %)
Voice message	Scam emails, texts or phone calls (P43)	5 (8 %)
Attachment	Encouraging recipients to … download an attachment (I5)	5 (8 %)
Purpose of the phish		
Deception	Often through deception (P41)	9 (15 %)
Compromise/hack/ account, use information maliciously	Compromise your data. (I11) so they can be used maliciously (P33)	7 (12 %)
Steal/theft	To steal your data or personal information (P11)	6 (10 %)
Fraud	In an attempt to commit fraud (P7)	3 (5 %)
Target of the phish		
Personal /sensitive information	Something scammers use to trick you in revealing sensitive information (P17) Personal details (I21)	44 (72 %)
Financial information	Might pretend to be a bank in order to gain account information (P35) Entering personal details like passwords to gain access to their online accounts (P29) Convince you to send them money (P13)	13 (21 %)
Specific types of information	To get you to insert your logins (P32) such as passwords, credit card numbers (P18)	8 (13 %)

These findings suggest that participants had a generally accurate understanding of phishing, particularly in terms of its purpose and delivery methods. However, their descriptions often lacked technical depth or conceptual clarity, indicating that their knowledge was shaped more by personal experience than by formal education or training in cybersecurity.

6.3.1.2 Frequency of Experience Phishing Attacks

Participants were asked whether they experienced phishing attacks. Nine participants (14 %) reported never experiencing any, and the other 57 participants (86 %) reported having experienced them. The median rating of frequency (rated as “never” scored as 1 to “very often” scored as 7) was 4.0 (SIQR: 1.0), not significantly different from the midpoint of the scale ($Z = 0.47$, n.s.), meaning “from time to time”

The 57 participants who reported experiencing phishing attacks rated whether they were ever caught out by a phishing attack (also rated as “never” to “very often”). 28 participants (49 %) reported they had never been caught out, but 29 (51 %) had, although the frequency was very low, with a median of 2.0 (SIQR: 0.5), significantly below the midpoint of the rating scale ($Z = -6.27$, $p < .001$).

The 29 participants who had been caught out were asked whether there were serious consequences of being caught out, six (21 %, which is also 9 % of the whole sample of 66 participants) said it did have serious consequences, 20 (69 %) said it did not, and 3 (10 %) could not remember (which suggests it did not have serious consequences).

Of the 29 participants who had previously been caught out by a phishing attack, six (21 %) reported experiencing serious consequences. These participants were asked to briefly describe those consequences. Three out of the six responses were relevant to the question and provided specific details, while others gave general descriptions of what typically happens in such cases. It seems that the question may not have been phrased clearly enough, which likely resulted in more general answers. The three responses included severe consequences such as malware being installed, falling victim to a sophisticated fraud and transferring an amount of money.

6.3.2 Diary Part

6.3.2.1 Encountering Online Threats: Frequency and Types of Threats

Each day participants were asked to report how many possible threats they had encountered. Seven participants never reported encountering a threat; the remaining 38 participants reported between 1 and 11 threats in a single diary entry. While it is possible that the report of 11 threats in one day reflected a retrospective entry covering multiple days, rather than actual daily encounters, it was retained as reported, since it did not significantly affect the overall results. 121 reports were completed, including 102 threats (as in 19 reports the threat type was not clear).

The total number of monitoring days was 413 from 38 participants. Participants reported an average of 8.5 threats per month, which means 0.29 threats per day.

Participants were asked to complete a short questionnaire on up to three threats each day. Almost always, only one report was completed (91.7% of the time). 51 screenshots were submitted (for 42.1% of threats).

6.3.2.2 Types of Threats

Participants were asked to classify the type of threat if they could. Approximately more than half were phishing threats (69 %), with spear phishing the next most common (17 %). Malware, viruses, ransomware, and spoof websites also occurred, but each of these types accounted for less than 6% of threats, making them relatively uncommon.

Table 6.5: Threat types N = 102 (%)

Threat type	N (%) of participants encountered the threat
Phishing	70 (69 %)
Spear phishing	18 (17 %)
Malware/virus	6 (5 %)
Ransomware	2 (2 %)
Spoofed website	6 (6 %)
Not sure/other	19 (16 %) [1]

[1.] Not sure/other percentage was found by dividing it by 121, which was the total number of reports

6.3.2.3 Device Type

If participants reported that they encountered a threat, they were asked subsequent questions for further details. First, they were asked about the device type they were using while they encountered the threats. Nearly three-quarters (72 %) of possible threats were encountered on mobile phones, with much smaller numbers on desktop computers (15 %) or laptops (13 %).

As the result showed most threats were encountered on mobile phones, which shows how much younger adults now rely on their phones for daily online activity. This also suggests that users might be more at risk when using their mobile phones, possibly because it is harder to spot warning signs on small screens or when multitasking.

6.3.2.4 Source of Threats

Participants were asked about the channel of threats from which they received the threats. Approximately half the threats were received via emails (51 %), with smaller numbers via social media sites (14 %), which might include the messaging services on these sites, and text messages (13%). While 10 % of the participants received threats through voice messages, only 4 % received the threats through phone calls.

This suggests that while email remains the primary delivery channel for online threats, attackers are adapting to users' broader digital habits. The presence of threats via social media, text messages, and voice calls highlights a shift toward more diverse platforms. This cross-platform spread may reduce user vigilance, especially in informal or trusted spaces like messaging apps.

6.3.2.5 Threat Detection Cues

Participants were asked to identify the cues that led them to suspect a potential threat. They could choose as many cues as they wanted from the options provided. For the 121 threats reported,

participants selected 299 cues in total from the list. This results in a mean of 2.5 cues identified for each reported threat (Table 6.6).

The most frequently selected cues were suspicious or unknown email addresses, phone numbers, or usernames, which were reported as key indicators of a potential threat. Suspicious email addresses accounted for 19 % of selections, while suspicious phone numbers or usernames were chosen 16.4% of the time. These were closely followed by suspicious links (16 %), highlighting the importance of URL analysis in online threat detection.

Interestingly, spelling and grammar errors were the least frequently selected cue, with only 2 % of participants identifying them as an indicator of a potential threat.

Table 6.6: Cues used by participants to detect potential threats (N = 299).

Cues	**N (%) of instances**
Suspicious email/phone number/username	56 (19)
*Unknown email/phone number/username	49 (16)
Suspicious link	47 (16)
Too good to be true offers	33 (11)
*Incorrect information (e.g. parcel delivery, but you are not expecting a parcel)	27 (9)
Unprofessional layout/presentation	22 (7)
Mimics a work or business process	20 (7)
Request for sensitive information (e.g. bank details)	18 (6)
Lack of sender/business information	12 (4)
Spelling/grammar errors	5 (2)
Other	10 (3)

In addition to the predefined cues listed in Table 6.6, participants were given the option to select “Other” and describe any additional cues that made them suspect a threat. Ten participants selected this option and provided brief descriptions of cues that were not included in the predefined list offered to them. Although they were relatively infrequent, they highlight how individuals use a range of cues to identify potential threats. These responses are summarised in Table 6.7.

Table 6.7: Additional detection cues provided by participants (selected "Other").

Cue name	Definition	Participants' answers
Newly created profile	Participants noted that fraudulent profiles were often newly created	P3: "Dummy profile, always created within a couple of months."
Money- requested	Participants identified the threats as involving demands for money	P4:" Demanding money saying phone has been hacked"
System warning	Participants relied on the warning generated by their systems or devices	P4: "Outlook blocked the content"
		P13: "Phone flagged as a potential scam"
Sense of urgency	Participants recognise the threat from the use of time pressure	P11: Sense of urgency
Suspicious download	Participants reported that they recognised threats when prompted to download something	P23: Ask to download something
Unnatural or unexpected response	Participants recognise the threat because of the non-human or unexpected speech/accent in the response	P34: Robotic responses to the question
		P17: The accent
Known threats	Participants recognised the threats as it was a commonly known scam	P33: I received a phone call and after googling it is a known scam

In addition to participants' reported cues**,** either from selecting the list or their responses to other option, a third source of detection cues came from screenshot analysis. This involved reviewing the content of the uploaded screenshots to identify threat cues that were present but not explicitly mentioned by participants**.**

Table 6.8 presents the cues identified by the researcher during this analysis. A total of 33 threats were examined, and in many cases, cues included both predefined cues (e.g. unprofessional layout*,* suspicious sender address) and new cues that were not offered in the original list, such as Known threat**,** Sense of urgency**,** and Threatening language**.**

This finding suggests that participants may notice certain cues or may not report all cues of what informed their suspicion.

Table 6.8: Threat cues observed in screenshots but not reported by participants (N = 33).

Cue	N (%)
Suspicious email/phone number/username	5 (15)
Unprofessional layout/presentation	5 (15)
*Sense of urgency	5 (15)
Unknown email/phone number/username	4 (12)
Making an offer too good to be true	3 (9)
Mimics a work or business process	2 (6)
Incorrect information (e.g. parcel delivery, not expecting a parcel)	2 (6)
Spelling/grammar errors	2 (6)
*Threatening language	2 (6)
Lack of sender/business information	1 (3)
*Common scam	1 (3)
Suspicious link	1 (3)

* Cues that were found during analysis but not offered in the list

These results suggest that participants relied on the most obvious cues to detect threats, such as strange links or unknown senders, rather than more subtle details as layout. This focus may reflect how individual users learn to spot threats through everyday experience or media advice. However, the missed cues found in screenshots analysed suggest that users may not always pay close attention or may overlook cue they do not fully understand. This highlights a potential gap in their ability to fully assess online threats, even when warning cues are present.

6.3.2.6 Awareness of Encountered Online Threats

Participants were then asked whether they were aware of this type of threat. Out of the 121 responses, the majority 80 cases (66 %) selected that they were already aware of this kind of threat they encountered. Further, 23 (19 %) selected “I think so”, suggesting that they had some familiarity with the threat. Only 18 cases (15 %) reported that they were not aware of this type of threat, which means that their encounter during the study may have been their first exposure to it.

For the 103 cases for which participants were aware or thought they were aware, they were asked how they were aware of this kind of threat. Participants could pick multiple sources of awareness from a set of options (142 instances chosen), see Table 6.9. The most frequently mentioned source was that they had encountered this type of threat before (86 mentions, 61 %), and the least one with only 4 mentions (3 %) that they had learnt about it on television or in newspapers.

For those who selected social media, they were allowed to specify which social media service or application, four participants reported Facebook, three Reddit, two YouTube, one Instagram, and one TikTok.

As the findings show, most participants reported being aware of the threats they encountered, often through previous personal experience. This suggests that their awareness was shaped mainly by repeated exposure rather than formal education. Friends, family, and social media also played a role, showing that informal, everyday sources are important methods for how younger adults learn about online threats.

Table 6.9: Reported sources of participants' awareness of online threats.

Source of awareness	Frequency of mention	Percentage (N = 142)
Encountered it before	86	61
Family or friend	31	22
Social media	21	15
TV or newspaper	4	3
Can't remember	7	-

6.3.2.7 Interaction with Threats

In 25 (21 %) of the participants' responses, they reported that they interacted with the threat. Those who interacted with threats asked how they interacted. Five of them reported that they did this only to take a screenshot for the study, so these responses were removed, leaving 20 (17 %) instances in which participants interacted with the possible threats. In most cases, 16 (80 %) the interaction was minimal, meaning participants opened the email or message (and in some cases, they stated that they did not click on any links or do anything further). In one case, a participant did click on a notification, which took them unexpectedly to an online financial site (it is not clear what happened after that) (P39). The most detailed interaction was by two participants who reported interacting with the attackers to investigate the threat (P10, P34). The other two responses (P38 and P39) reported their interaction with the threats but without providing details. Table 6.10 shows the participants' answers to the open-ended question "How did you interact with the threat?"

Table 6.10: Participants' reported interactions with online threats with examples and frequency.

Categories	Examples	N (%)
Limited interaction	I opened the email to view it, but did not access the link it provided. (P16)	16 (80 %)
Interacted to investigate	I asked further probing questions to understand how it works and if they were going to demand certain funds from me, to which they said £100 or £50 monthly, depending on the package (P10) I messaged a couple of times to see what kind of scam it was going to be (P34)	2 (10 %)
Interacted	Clicked on the link provided in the post comments (P38) I clicked on the notification, which sent me straight to the banking app (P39)	2 (10 %)

These findings suggest that younger adults may prefer to quickly dismiss or block online threats rather than investigate them further. This could reflect a desire to avoid hassle, limited confidence in

knowing what to do next, or a belief that threats are common and not worth reporting unless serious harm occurs.

6.3.2.8 Actions Participants Took to Investigate Potential Threats and Attempt to Resolve Them

Participants were asked an open-ended question: *"*What did you do to try to figure out whether it was a threat/scam and what to do to resolve the issue?" This question was designed to understand how participants checked the message and resolution actions (e.g. blocking, deleting, reporting) they took. Responses were analysed using content analysis and were coded into two categories:

- Actions to figure out whether it was a threat
- Actions taken to resolve the threat

In 31 (26 %) of cases, participants provided information. 37 instances of actions were coded, as some participants reported taking more than one action for a particular threat. These actions were grouped into two categories: those taken to investigate whether the potential threat was an actual threat (Investigate) and those taken to address the issue (Resolve).

In total, 2 different actions that investigate a potential were identified (see Table 6.11), with 13 mentions of these actions. The most common approach was to search online, taken in 11 (85 %) of cases, typically by Googling the phone number, sender, or the nature of the message. In only two cases (by different participants, P10 and P34, 15 %), participants interacted with the attackers to understand what the threat might be.

The remaining 24 actions involved responses to resolve the threat (see Table 6.12). The most frequent actions in this category were deleting the message (33 %), followed by reporting the threat to external authorities or platforms (e.g. Facebook, TikTok), or blocking the sender, each mentioned 29 %. In a few cases, participants took further actions by updating their account details.

Table 6.11: Actions taken to investigate whether a potential threat was an actual threat (N = 13).

Action	Example	N (%)
Research (online)	Googled the phone number. This indicated life insurance phone spam (P4)	11 (85 %)
Interacted with the attacker	I asked further probing questions to understand how it works and if they were going to demand for certain funds from me to which they said £100 or £50 monthly, depending on the package (P10)	2 (15 %)

Table 6.12: Actions taken to resolve the threat (N = 24).

Action	Example	N (%)
Deleted the email/message	Delete contact (P31)	8 (33 %)
Reported the threat	I blocked and reported to TikTok moderation (P34)	7 (29 %)
Blocked the attacker	Block the number (P5)	7 (29 %)
Changed my personal details	I googled the account and how to change my details account to try to secure them (P21)	2 (8 %)

6.3.2.9 Purpose of Threats

Participants were asked what they thought the purpose of the threat or scam was. Their open-ended responses were analysed using content analysis. Two of the categories, data theft and financial fraud, had been previously developed during the analysis of the KSA diary study and were retained here, as similar themes were present in the UK responses. These categories were defined in Section 5.2.5. In this study, two additional categories were added: spreading malware and phishing for credentials. The definitions of the categories and examples of each are provided in Table 6.13.

Table 6.13: Purpose of threat definitions and examples.

Purpose of Threat Category	Definition	Example
Spreading malware	Attempt to infect devices with malicious software, such as viruses, spyware, or trojans.	Click on the link and it will install malware (P4)
Phishing for credentials	Attempts to obtain login credentials to gain unauthorised access to accounts	To get my Instagram log in (P9)

In all, 110 (91 %) participants provided explanations of what they thought the purposes of threats were. Table 6.14 presents what participants thought the purpose of the threat was. Data theft was the most commonly mentioned purpose of threats, occurring in 68 (62 %) instances. Financial fraud was mentioned in 21 (19 %) instances, while phishing to obtain credentials and spreading malware was mentioned less frequently.

Table 6.14: Participants' explanations of purposes of threats (N = 110).

Purpose of Threat	Example	N (%)
Data theft	The purpose was probably to get me to click the link which would then try to gain some personal information from me (P1)	68 (62 %)
Financial fraud	To extract money from me, likely after I make the payment, they'd continue blackmailing me for more crypto (P13)	21 (19 %)
Spreading malware	Phishing attempt for personal information; it's also possible it contained a link to a fraudulent site with malware, leading to a cyberattack or ransomware download (P19)	10 (9 %)
Phishing for credentials	Installing keylogger or stealing login information (P16)	11 (10 %)

Finally, participants rated whether they thought a potential was actually a threat (from "definitely not" scored as 1 to "definitely" scored as 5).

The median rating was 5.0 (SIQR: 0.5), significantly above the midpoint of the scale ($Z = 9.09$, $p < .001$), so participants were usually certain or reasonably certain it was a threat. There was only one case in which the participant decided it was definitely not a threat. This participant described the incident in a previous question as a "typical phishing email", but then rated it as "definitely not a threat". This shows a possible misunderstanding of the question, as he/she may have thought it was about the consequences of the threat instead of whether the message was a threat.

6.3.3 Participants' Individual Characteristics Related to Online Security

The following result examines participants' individual characteristics using scales. Two of the scales (SeBIS and DOSPERT) were completed by all 66 participants as part of the initial questionnaire. The other two measures (CFC and UO) were included in the final questionnaire, which was completed by 45 participants.

6.3.3.1 Participants' Risk-Taking Behaviour: DOSPERT

Table 6.15 shows the mean scores for each DOSPERT subscale in the current UK sample with a statistical comparison to the normative data reported by Blais and Weber (2006). Additionally, each subscale was tested against the neutral midpoint of the 7-point scale (midpoint = 4) to determine whether participants were risk-taking in each domain.

Across all five subscales, the current sample reported significantly lower risk-taking scores than those in the normative sample. Ethical and Recreational risk-taking were notably low in the current sample, significantly below both the normative mean and the midpoint, indicating strong ethical risk aversion and low engagement in physically risky activities. In the Financial domain, participants also reported significantly lower risk-taking compared to the normative mean and significantly below the midpoint. Health/Safety risks were significantly lower than the normative mean and significantly

below the midpoint. This suggests that the current sample was less inclined to take financial and health/safety risks compared to the normative sample.

Finally, Social risk-taking was significantly lower than the normative mean. However, this subscale was significantly above the midpoint, suggesting that participants are still generally comfortable taking risks in social settings, albeit to a lesser extent than the normative sample.

Table 6.15: Mean scores for DOSPERT subscales in the current sample, with statistical comparison with scores from Blais and Weber (2006) and with midpoints of each subscale.

DOSPERT Subscale	Blais and Weber Mean[5]	Current sample Mean (SD)	Comparison with Blais and Weber	Comparison with midpoint
Ethical	2.82[2]	1.93 (0.73)	Z = -6.80, p < 0.00	Z = -7.07, p < 0.00
Financial	3.27	2.48 (1.22)	Z = -4.32, p < 0.00	Z = -6.30, p < 0.00
Health/Safety	3.44	3.05 (1.21)	Z = -1.98, p = 0.04	Z = -4.97, p < 0.00
Recreational	3.74	2.49 (1.26)	Z = -5.66, p < 0.00	Z = -6.17, p < 0.00
Social	5.43	4.63 (1.26)	Z = -4.27, p < 0.00	Z = 3.95, p < 0.00

1. Mean scores were calculated from Blais and Weber (2006) to allow comparison, as the number of items in each subscale was different in the version of the scale used here.
2. Standard deviations could not be calculated as I did not have access to the raw data from Blais and Weber (2006).

6.3.3.2 Participants' Online Security Behaviours: SeBIS

Table 6.16 shows the means of SeBIS scores for this sample. Since the original SeBIS scale uses a 5-point Likert format, and a 7-point scale was used in this study, the means for the current sample were adjusted to allow for comparison with the normative values reported by Egelman and Peer (2015). The table displays both the unadjusted and adjusted means, along with comparisons to the normative scores and midpoint of each subscale.

UK participants scored significantly higher than the normative scores reported by Egelman and Peer (2015) across most SeBIS subscales. The largest difference was found in Device Securement, where the UK sample reported much stronger behaviours compared to the normative mean. This subscale also showed a significant positive difference from the midpoint of the scale, suggesting a high level of security behaviour when it comes to locking devices and controlling physical access.

Participants also scored significantly higher on Proactive Awareness than the normative value, again showing that the UK sample has better security practices in terms of evaluating links before clicking, checking for insecure websites, and suspicious links. This sample score was also significantly above the midpoint implies stronger security awareness.

For Password Generation and Updating subscales, while the score was significantly higher than the normative mean, it did not differ significantly from the scale midpoint, indicating average behaviour in these domains.

These results suggest that participants demonstrated particularly strong behaviours in securing devices and greater awareness and precautionary behaviour but were more moderate in generating strong passwords and updating software.

Table 6.16: Means SeBIS Subscales in current sample, with statistical comparison with scores from Egelman and Peer (2015) and with midpoints of each subscale.

Subscale	Egelman and Peer Mean[1]	Current sample Mean (SD)	Adjusted mean[2]	Comparison with Egelman and Peer	Comparison with midpoint
Device Securement	3.21	5.87 (1.01)	4.19	Z = 7.06, p <0.00	Z = 6.83, p < 0.00
Password Generation	3.25	4.09 (1.36)	2.92	Z = 4.61, p < 0.00	Z = 0.56, n.s.
Proactive Awareness	3.73	4.89 (1.19)	3.49	Z = 5.99, p < 0.00	Z = 5.16, p <0.00
Updating	3.47	4.04 (1.49)	2.88	Z = 3.12, p = 0.002	Z = 0.38, n.s.

[1.] Egelman and Peer (2015) only provide mean scores for individual items in SeBIS, not the subscales. So I calculated the mean score for each subscale, but this means I cannot calculate the SD for each subscale in their sample

[2.] I used a 1–7 scale; the original SeBIS used a 1–5 scale, therefore, these are the subscale scores adjusted to a 1–5 scale to allow comparison with the original SeBIS results by multiplying by 0.714.

6.3.3.3 Participants' Concern about the Future: Consideration of Future Consequences Scale (CFC)

Table 6.17 presents participants' scores on the two subscales of the CFC-14 and the normative scores reported by Joireman et al. (2012), along with a statistical comparison between these scores and a comparison of the current sample scores with the midpoints of the subscales.

For the CFC-I subscale, the mean score of the current sample was not significantly different from Joireman et al.'s normative mean. While in the (CFC-F) subscale, the mean score in the current sample was significantly lower than Joireman's normative mean. Additionally, it was significantly above the midpoint**,** indicating that although future concern is present, it is lower than that observed in previous research**.**

Table 6.17: Mean CFC subscales in the current sample, with statistical comparison with scores from Joireman et al. (2012) and with the midpoints of each subscale.

CFC Subscales	Joireman et al. Mean (SD)	Current Sample Mean (SD)	Comparison with Joireman et al.	Comparison with midpoint
CFC-I	3.74 (1.07)	3.78 (0.84)	Z = 0.79, n.s.	Z = -2.05, p = 0.04
CFC-F	5.12 (0.90)	4.49 (0.79)	Z = - 4.74, p < 0.00	Z = 4.37, p < 0.00

6.3.3.4 Unrealistic Optimism

Table 6.18 shows the median scores and interquartile ranges for participants' responses to six questions about unrealistic optimism. These questions assess how participants perceive their likelihood of receiving, detecting, and dealing with online threats compared to friends and a typical person of their age, using a 5-point Likert scale (1 = much less likely / less able, to 5 = much more

likely / more able)**.** The table also provides Spearman correlation, which measures how consistent participants' perceptions are when comparing themselves to friends versus a typical person.

When asked about their likelihood of receiving threats, the median was 3.0, suggesting participants view themselves as receiving fewer threats than others. However, for detecting and dealing with threats, the median was 4.0, indicating that participants generally perceived themselves as more capable than their peers to detect and deal with online threats.

To assess the consistency between participants' self-comparisons with friends versus a typical person of their age, Spearman correlations were conducted. There were significant correlations between each pair, so those who viewed themselves as more capable than friends also believed they were more capable than a typical person of their age. Therefore, friends' ratings will be used in the subsequent analysis.

Table 6.18: Unrealistic optimism median scores for each question, with Spearman correlations between the pairs of questions about "your friends" and "a typical person".

Compared to …	**Median (SIQR)**	**Spearman Correlation (r_s) Friends – Typical person**
your friends, do you think you are more or less likely to receive online threats and attacks?	3.0 (0.5)	r = 0.79, p < 0.00
a typical person of your age, do you think you are more or less likely to receive online threats and attacks	3.0 (0.5)	
your friends, do you think you are more or less able to detect whether a call, message, link, or website is an online threat?	4.0 (0.5)	r = 0.58, p < 0.00
a typical person of your age, do you think you are more or less able to detect whether a call, message, link, or website is an online threat?	4.0 (0.5)	
to your friends, do you think you know how to deal with online attacks?	4.0 (0.5)	r = 0.75, p < 0.00
a typical person of your age, do you think you know how to deal with online attacks?	4.0 (1.0)	

To assess whether participants showed unrealistic optimism, one-sample Wilcoxon signed-rank tests were conducted to compare their ratings against the midpoint of the scale. The result was not statistically significant for receiving fewer threats than friends (Z = -0.37, n.s.). This suggests that there was no significant tendency for participants to perceive themselves as either more or less at risk than a friend.

On the other hand, the result of detecting and dealing with online threats compared to friends was statistically significant, indicating that participants perceived themselves as significantly more able than their friends to detect (Z = 5.34, p < 0.00) and deal (Z = 4.59, p <0.00) with online threats.

These findings show that the participants had unrealistic optimism**,** particularly about their ability to detect and deal with threats.

6.3.3.5 Relationship Between Participants' Online Threat Experiences and Their Individual Characteristics

To investigate the relationship between participants' online threat experiences and their individual characteristics, I conducted a series of linear regressions on a number of key threat experience measures and the measures of participants' individual characteristics. The key threat variables were:

- The percentage of threat reports when participants stated they were aware of the threat type
- The percentage of threat reports when participants stated that they interacted with the threat
- The percentage of threat reports when participants stated that they took action to figure out whether it was really a threat or not
- The average number of cues participants detected per threat
- The number of different cue types participants used in total

The individual characteristic variables were: age, gender, self-ratings of expertise with the internet and online security, scores on SeBIS, DOSPERT, and CFC subscales, and unrealistic optimism ratings in relation to friends (of the tendency to receive threats, ability to detect threats when received and ability to deal with threats).

A variety of specific hypotheses could be made about these relationships, for example:

- Participants who are aware of a higher percentage of threat types will score higher on SeBIS Proactive Awareness subscale, as they are more aware of all security issues
- Participants who interact with a higher percentage of threats will score higher on DOSPERT subscales, as they measure risk-taking in other areas which may transfer to threat behaviour
- Participants who took action to figure out a higher percentage of threats will score higher on SeBIS Device Securement subscale, as they are more careful in their online security behaviours
- Participants who reported a higher number of cues detected per threat and a higher number of threat cues in total will score higher on SeBIS Proactive Awareness subscale, as they are more proactive about all security issues
- Participants who are more unrealistically optimistic will score lower on all the threat variables, as they will be less concerned about dealing with threats.

As the number of participants was relatively small for a linear regression with this many predictor variables, I also considered effects for which the probability was between 0.05 and 0.10, often referred to as a "trend to significance" (which is controversial, see Nead et al., 2018).

Table 6.19 summarises the results of the linear regression for each key threat variable.

Table 6.19: Results of the linear regression to predict five threat experience variables from participants' individual characteristics.

Predicting ….	**Overall significance of regression**	**Significance of individual predictors**
Awareness of threat	F = 2.36 p = 0.034	Unrealistic Optimism in ability to detect threats p = 0.008, negative correlation SeBIS Proactive Awareness subscale p = 0.077, positive correlation
Interacted with threat	F = 1.45 n.s.	Unrealistic Optimism in ability to deal with threats p = 0.009, negative correlation SeBIS Proactive Awareness subscale p = 0.073, positive correlation
Acted to figure out the threat	F = 1.56 n.s.	Unrealistic Optimism in Tendency to receive threats p = 0.040, positive correlation Unrealistic Optimism in ability to deal with threats p = 0.064, positive correlation SeBIS Proactive Awareness subscale p = 0.073, negative correlation
Cues/threat	F = 0.83 n.s.	No individually significant predictors
Total cues	F = 1.11 n.s.	SeBIS Device Securement subscale p = 0.078, negative correlation

The linear regression analyses revealed a number of interesting relationships, either significant or trending to significance.

Awareness of the types of threats was significantly predicted by a lower unrealistic optimism by participants in their ability to detect threats. In other words, participants who were more realistic about their ability to detect threats were more aware of the types of threats. There was also a trend towards a positive prediction of awareness of the types of threats by the Proactive Awareness SeBIS subscale. Thus, participants who scored higher on the general online security awareness measure also scored higher on the specific awareness of the types of threats.

The same individual characteristics variables predicted whether participants tended to interact with threats. Thus, interacting with a higher percentage of threats was predicted by more realistic estimations of one's ability to detect threats and higher general online security awareness.

The same individual characteristics variables predicted whether participants tended to take actions to figure out whether incidents were indeed threats, along with one of the other unrealistic optimism variables. But in this case, the pattern of relationships was different. A tendency to take actions was predicted by higher unrealistic optimism about the number of threats received and the

ability to detect threats and predicted by lower Proactive Awareness scores. This suggests that the tendency to take action to figure out whether incidents are indeed threats is associated with a sense of confidence about online security in general and online threats in particular, which may be misplaced.

In terms of the use of cues, none of the individual characteristics predicted using more or less cues per threat and the number of different cue types used was only predicted (and only with a trend) by the Device Securement SeBIS subscale. This was the only prediction which was not meaningful, as the use of more cue types was predicted by lower Device Securement scores. This may be a spurious relationship.

Thus overall, the SeBIS Proactive Awareness subscale and two of the unrealistic optimism measures, about the number of threats received and the ability to detect threats in comparison to one's friends were the predictors of aspects of participants' threat experiences.

6.3.4 Participants' Attitudes and Experiences after Participating in the Study

Participants rated whether the study period had been typical in terms of the number of threats encountered during the study period. The median rating was 3.0 (SIQR: 0.5), so overall the period was judged "fairly typical".

Eight participants provided comments on how typical the period was, with two confirming it was typical and six thinking they received fewer threats than they usually did, for a range of reasons.

For example, one participant reflected (P28:"*I think it was probably on the lower side than what I have experienced over the past few years, and that might be because I have recently been ignoring scam calls and messages, and maybe the scammers are a little tired of trying the same schemes on me. They might come back with different ones*"). Another wrote (P40: "*I find I get a call from fraudsters reporting to be HMRC more weeks than not, but perhaps they took the week off*!").

Then, for the question about any threat or reports that appeared as particularly interesting or problematic. Seven participants also provided comments, two related to threats which appeared to be received from a real person not an AI (P34: "*The second scam did because it did seem to be a real person and not script or bot messaging me as it was able to respond to my questions, but also had imperfections indicating it's likely not an AI model*"). Two related to how many threats were received from Facebook, one related to a spear phishing attack in which the attackers appeared to have particular personal information about the participant, and one to a threat type the participant had not seen before.

Participants rated whether their attitude to online threats changed as a result of participating in the study. The median rating was 2.0 (SIQR = 1.5), which was significantly above "not at all" ($Z = 4.43$, $p < .001$), although clearly not a great deal above that rating, although the ratings cover the full range, with two participants answering "a great deal".

In the optional follow-up question to explain further, five participants said they were now more aware of threats, one said they understood them better, one said they would take more security measures in future, and one said they would be more likely to report threats to relevant authorities.

A further question specifically asked participants to rate whether they would be more vigilant about monitoring for threats in the future. The median rating was 1.0 (SIQR: 1.0), significantly above "about the same" ($Z = 4.36$, $p < .001$). Participants also rated whether they would be better at detecting and dealing with threats in the future (detecting threats: Median rating: 0.0, SIQR: 0.5; dealing with threats: Median rating: 0.0, SIQR: 0.5), somewhat lower than their ratings of future vigilance but still significantly above the "about the same" rating (in spite of the median ratings of 0.0, due to the nature of the distributions of ratings; detecting threats: $Z = 3.70$, $p < .001$; dealing with threats: 3.67, $p < .001$).

Nine participants answered a follow-up open-ended question as to whether their behaviour in relation to threats might be different in the future. Three answered that their behaviour would not change (as they felt they were careful and vigilant already), the other six mentioned interesting changes such as getting a VPN or setting up a sandbox to open suspicious messages in, as well as reporting threats more often and monitoring more carefully for threats.

6.3.5 Comparison of the Results from the Survey and Diary Studies with Younger British Adults

This section compares results from the UK survey study (Chapter 3) and the UK diary study (Chapter 6) to examine how retrospective self-reports align with, and differ from, daily self-reports of encounters with online threats.

In both the survey and the diary study, phishing was the most common type of online threat reported by younger adults in the UK. More than three-quarters of UK survey participants said they had experienced phishing, followed by malware, while data or identity theft was mentioned less often. The diary study confirmed this pattern, showing that most threats reported during the diary period were phishing-related, while other types, such as malware and spoofed websites, were less encountered in participants' everyday experiences. Together, these findings indicate strong consistency between the two methods in identifying phishing as the dominant threat encountered by this population.

Both studies also explored the sources from which threats originated. In the survey, websites were the most frequently reported source overall, particularly in relation to malware. For phishing-related scenarios, participants most frequently reported receiving threats via social media messages and email, while phone calls were mentioned less often. In contrast, the diary study showed that email was the most frequent delivery method, followed by social media. Direct phone calls were rarely reported. This difference may reflect the nature of the diary method, which captures immediate, routine encounters, such as email-based threats, more accurately than retrospective reports, which may give greater weight to less frequent but more memorable experiences.

The studies also provide insights into how threats were detected. The survey responses indicated that participants relied on cues related to content and design, such as suspicious links and requests for personal or financial information, especially in phishing scenarios. However, the survey provided limited insight into how these cues were applied in everyday experiences. In contrast, the diary study showed that participants most frequently selected cues related to sender credibility and suspicious links. Notably, screenshot analysis revealed that some cues, such as urgency and unprofessional design, were present but were not reported by participants. This suggests that while

participants consciously recognised some cues, they did not always notice other cues that were present in the threat. This gap between the cues embedded in the threat and those participants explicitly reported was only apparent through the diary entries, showing how diary data can reveal aspects of threat detection that are not captured through survey responses.

In terms of their responses to threats, the survey findings showed a wide range of actions taken by participants. Technical actions such as deleting or uninstalling software were frequently reported in response to malware, while account-related actions like changing passwords or cancelling cards were more often mentioned in relation to data or identity theft. Some participants reported recognising a threat and choosing not to engage. However, protective behaviours such as reporting threats or seeking advice were rarely described, and overall, only about half of the reported actions were assessed as adequate.

The diary study offered a more structured account of how participants responded to threats as they encountered them. Most participants reported avoiding engagement, such as by deleting messages or blocking senders, and some took steps to verify the threat by searching online. Reporting incidents or taking follow-up security actions, such as changing account details, was infrequently reported. These findings suggest that responses were generally limited to immediate threat avoidance rather than more proactive or preventative behaviours.

Security behavioural intention was also measured in both studies using the SeBIS scale. In both studies, participants showed consistent strengths in basic security behaviours, particularly those related to device securement. However, there was weaker engagement with behaviours requiring more effort or technical knowledge, such as creating strong passwords or regularly updating software. The consistency of this pattern suggests that even among digitally literate and confident younger adults, some key areas of online security remain underdeveloped.

Taken together, the survey and diary findings provide complementary perspectives on how younger adults in the UK experience and respond to online threats. Survey data captures broad patterns of exposure, while diary data reveals the practical decisions, routines, and blind spots that shape users' real-world security behaviour. These findings highlight the value of using both retrospective and day-to-day reporting methods to build a more complete understanding of user behaviour in the context of online security.

6.4 Comparison of Online Threat Experiences among the Younger KSA and UK Adults

This section compares key results across the four studies—survey and diary results from the UK and KSA, focusing on threat types, detection cues, responses, and individual characteristics. The aim is to highlight where findings aligned across contexts and where differences emerged between the samples' perceptions and behaviours.

Threat Types and Frequency

Across both the KSA and UK samples, phishing-related threats and malware were the most frequently reported online threats in both the survey and diary studies. This pattern indicates that younger adults in both contexts are exposed to a broadly similar set of online threats, likely reflecting shared use of common digital platforms and services.

Detection Strategies and Cues

Participants in both countries relied primarily on content-based cues, such as requests for personal information, as well as sender-related indicators, including suspicious sender details and links, to detect threats. In the survey phases, reports of detection cues were often general, reflecting retrospective recognition of suspicious requests or known scam formats. In the diary studies, participants provided more specific descriptions of cues used in real-world encounters, including sender information, message content, and links. Notably, in both diary studies, some cues, such as urgency, unprofessional design, "too good to be true" offers, and hidden or shortened URLs, were identified through screenshot analysis but were not always explicitly reported by participants. This suggests that while participants relied on familiar cues, some indicators of malicious activity were overlooked or not consciously recognised during threat encounters.

Responses to Threats

Across both countries, participants reported taking protective actions in response to online threats; however, these actions were often limited to avoidance strategies. In the survey studies, relatively few fully appropriate responses were described, and reporting threats to service providers or authorities was rare. The diary studies provided greater insight into response behaviour. In the UK diary, responses were typically reactive, most often involving deletion or blocking. In the KSA diary, early suspicion frequently led to non-interaction with the threat, which was coded as an appropriate response in phishing contexts. These findings suggest that avoidance was the dominant response strategy across both samples, with less emphasis on proactive protective actions.

Individual Characteristics

Across both diary studies, participants reported stronger intentions for basic security behaviours, such as device securement, than for behaviours requiring ongoing effort, including software updating and password management. Unrealistic optimism was evident in both samples, though expressed in slightly different ways: UK participants showed optimism regarding their ability to detect and handle threats, while KSA participants expressed optimism related to threat exposure and detection. In both cases, this confidence was not consistently reflected in response behaviour. Results from the CFC scale indicated future-oriented thinking in both samples, though this was not directly associated with more proactive security actions. Findings from the DOSPERT scale showed generally low risk-taking tendencies across both groups, with social risk-taking remaining comparatively higher in the UK diary sample and overall low risk-taking across domains in the KSA diary sample.

Table 6.20 presents a summary of the comparisons of the main results from the UK and KSA survey and diary studies. It highlights similarities and differences in threat exposure, detection cues, response behaviour, and individual characteristics.

Table 6.20: Summary table of the key results across the four studies.

	UK Survey	UK Diary	KSA Survey	KSA Diary
Most reported threats	Phishing, malware	Phishing (email, social media)	Phishing, malware	Phishing (email, WhatsApp)
Rarely reported threats	Ransomware, spoofed websites	Ransomware	Ransomware	Spoofed websites
Most frequently reported detection cues	Suspicious design, requests for personal information	Sender details, suspicious links	Requests for personal information, unusual transactions	Requests for personal information
Main sources of threats	Websites, social media	Email	Websites, social media	Email
Most frequent unreported cues (identified from screenshots)	N/A	Urgency, unprofessional design	N/A	"Too good to be true" offers, hidden/shortened URLs
Common responses to threats	Deleting or uninstalling software, blocking the sender	Deletion, blocking, limited reporting	Avoiding interaction, blocking the sender	Verifying the request
Appropriateness of responses	52 % appropriate	N/A	78 %* appropriate	77 % appropriate
Security behaviour intentions (SeBIS)	Stronger intentions for device securement	Stronger intentions for device securement and proactive awareness	Stronger intentions for device securement	Stronger intentions for device securement
Unrealistic optimism	N/A	Present in threat detection and handling	N/A	Present in threat exposure and detection
Consideration of Future Consequences (CFC)	N/A	More future-oriented than midpoint, but lower than norms	N/A	Future-oriented thinking
Risk-taking behaviour (DOSPERT)	N/A	Social risk-taking remained comparatively higher	N/A	Generally low risk-taking across domains

*A small number of adequate solutions resulted in a relatively high adequacy percentage

These cross-study comparisons offer a foundational view of shared and context-specific patterns in threat experience and user response. Chapter 7 builds on these findings by exploring their theoretical and practical implications, with a focus on how cultural, cognitive, and behavioural factors shape the security practices of younger adults.

6.5 Discussion

This study investigated how younger adults in the UK experience online threats by using a diary-based method. It refined the previous diary study presented in Chapter 5 that examined online threat encounters among Saudi younger adults. In the earlier study, participant recruitment resulted in only 16 participants over a 30-day period, despite extensive recruitment efforts. To improve this, the current study implemented a more efficient design by shortening the diary period to 14 days in Round 1 and then 7 days in Round 2. Round 1 successfully generated 60 threat reports from 15 participants, comparable to the number collected over a full month in the previous study. To avoid participant fatigue, a second 7-day round was conducted with a larger sample size of 30 participants, yielding an additional 61 threat reports. No differences were found between the two rounds in terms of participants' responses, allowing for the datasets to be combined.

While maintaining the main goal from the previous study, new questions were introduced to gather details on device type, threat channel, and perceived purpose. Additionally, the diary questionnaire was refined by replacing some open-ended questions with closed-ended formats. This change was intended to ease the response process for participants and to ease data analysis for researcher. Participants were also given an expanded list of threat detection cues. These refinements enhanced the overall data collection process and improved data quality.

In terms of the research questions investigated:

RQ1: How frequently do younger British adults encounter different types of online threats?
The first research question examined the frequency of encountering different types of threats by younger adults in the UK. Participants reported a mean of 0.29 threats per day, which is equivalent to approximately 8.5 threats per month. Most diary entries included a single threat, despite participants being able to report up to three per day. This could imply that threats are typically limited to one notable incident per day when they occur. However, it may also reflect other factors, such as participant fatigue, time constraints, or the perception that only one threat was worth reporting.

Notably, participants reported encountering 0.34 threats per day (SD = 0.29), or around 10.05 per month, but threats submitted through diary entries averaged slightly lower, at 0.29 per day (SD = 0.22), or 8.57 per month. This discrepancy highlights the gap between encountered and reported threats, suggesting that some incidents may have gone unreported.

Importantly, in the final questionnaire, most participants indicated that the study period was fairly typical in terms of the number of threats they encountered. This strengthens confidence that the reported frequency reflects their usual experiences, rather than being unusually high or low due to temporary factors.

More than half of the reported threats were phishing. This result agrees with the findings from the survey I conducted with a similar sample of younger UK participants. It is also an expected outcome, as prior literature highlights the persistent nature of phishing and other forms of digital deception in everyday online interactions (Montasari, 2023; Department for Science, Innovation and Technology & Home Office, 2024).

In this study, about 66% of the incidents reported that they were already aware of the type of threat they encountered. The most frequently mentioned source of awareness was past personal experience, followed by hearing about threats from family or friends.

While this suggests a relatively high level of threat awareness among participants, prior research has shown that awareness alone does not guarantee effective security behaviour. Jeske & van Schaik (2017) emphasise the distinction between awareness and deeper familiarity, arguing that the latter, developed through direct experience or meaningful learning, is more predictive of proactive behaviours.

RQ2: What cues do younger British adults use to detect online threats?
The second research question examined the cues that were used by this sample of participants to detect threats. Suspicious and unknown emails/numbers/usernames were the most frequent cues used, while spelling and grammar errors were the least frequently selected cues. The latter is a particularly interesting result as many previous studies have found spelling mistakes to be a commonly used cue for detecting phishing attempts (Parsons et al., 2015; Steves et al., 2020). The infrequent mention of that type of cue in this study suggests that participants may have developed alternative detection strategies, focusing more on technical or source-related indicators rather than linguistic inconsistencies.

Interestingly, analysis of the uploaded screenshots revealed that certain cues, particularly a sense of urgency and unprofessional layout or design**,** were sometimes present in the threats, yet participants did not identify or report them. This may suggest that while these cues are salient to an expert, they are either overlooked or not consciously recognised by users when assessing online threats.

RQ3: How do younger British adults respond to online threats?
The third research question explored how younger adults in the UK respond to online threats. the findings indicate that most participants were cautious. In 80% of cases**,** participants reported very limited interaction with the threat, for example, opening a suspicious email or message, but not engaging further by clicking links or replying. Only 10% of cases involved *active interaction* with the threat, such as responding to a phishing message, typically in an attempt to investigate or confirm its legitimacy. These findings suggest that while threats were often opened out of curiosity or habit, participants generally avoided actions that could compromise their security.

This cautious approach may reflect a general risk-averse mindset, but it can also be interpreted in light of the findings by Greene et al. (2018), who found that individuals who click on suspicious links and those who do not, clickers and non-clickers, differ not only in their behaviour in relation to possible online threats but also in how they interpret possible cues to detect threats and the consequences of threats. Their study showed that individuals who clicked on phishing link were often motivated by concerns about missing important information or failing to respond to a request that seemed contextually relevant. Conversely, individuals who did not click on phishing links, non-clickers, were focused on the potential risks of engaging**,** such as downloading malware or exposing personal information. In the current study, the lack of alignment between participants' context and the threat content may have contributed to the limited interaction reported.

In terms of resolving the issues of threat, participants demonstrated a range of protective responses once a potential threat was identified. The most common action was searching online for more information about the source of the threat, such as googling the sender's phone number, email address, or message content. Other reported behaviours included deleting the message, reporting it, and blocking the sender. These actions reflect generally appropriate responses to suspicious messages by removing the threat or avoiding further engagement. However, only a small proportion of participants took more complex steps, such as changing their login credentials. This may indicate that although participants were generally aware of some countermeasures, they did not always actively secure their digital presence after a suspicious incident.

RQ4: What is the relationship between younger British adults' individual characteristics (risk taking, unrealistic optimism, consideration of future consequences, online security behaviours) and their experiences of online threats?

The fourth research question explored how young adults' individual characteristics related to their experience of online threats. Beginning with risk-taking behaviour, as measured by the Domain-Specific Risk-Taking (DOSPERT) scale, participants in this UK sample reported significantly lower scores on all five subscales (Ethical, Financial, Health/Safety, Recreational, and Social risk-taking) compared to the normative sample reported by Blais and Weber (2006). In particular, scores for the Ethical and Recreational subscales were the lowest among the subscales, suggesting that participants were especially reluctant to engage in behaviours that either violate social or moral norms or involve physical challenges and adventurous activities that may be perceived as risky or impulsive.

This lower risk profile may partly explain the relatively cautious approach participants showed when encountering online threats, such as high rates of limited interaction (e.g. opening but not clicking) and avoidance actions like deleting or blocking. Although the relationship between domain-specific risk-taking and cybersecurity behaviour has emerged recently, these findings support previous work suggesting that individuals who risk taking aversion may also be less likely to take risks online (Egelman & Peer, 2015; Gratian et al., 2018)

The results on the SEBIS scale indicate that participants in this study exhibited particularly strong security behaviours regarding device security, such as locking their devices and controlling physical access to them. This was reflected in significantly higher scores on the Device Securement subscale compared to both the normative data and the midpoint of the scale. Participants also demonstrated relatively high levels of proactive awareness about online security, suggesting that they would have good abilities to recognise and respond to online threats. However, more moderate intentions were noted in areas such as password generation and software updates. On these subscales, participants did not significantly differ from the midpoint scores. This pattern suggests that while participants are generally vigilant, especially in visible or habitual practices like locking their devices, they may be less consistent in behaviours that require more effort or technical knowledge, such as creating strong passwords or keeping software up to date. The SeBIS normative sample, developed by Egelman and Peer in 2015, consisted primarily of U.S. adults with a broad age range (19–70, median age approximately 35). In contrast, the current study focused on younger adults in the UK. In addition to the age and national differences, the comparison is also limited by the time gap, as user behaviours and security practices may have evolved since the original scale was developed.

In addition, unrealistic optimism (UO) was explored by comparing participants' self-perceptions of how they rated their exposure to, detection of and ability to deal with online threats compared to their peers. While participants saw themselves as equally likely to receive threats, they believed they were more able to detect and deal with them compared to both their friends and the average person their age. This pattern reflects common findings of optimism bias, particularly among young, educated individuals who consider themselves technologically competent. These results agree with the findings of Hewitt & White (2022), who found that prior computer use or formal security education did not significantly reduce unrealistic optimism. That study also concluded that time spent online or receiving training did not necessarily lead to more accurate threat assessments.

Regarding Consideration of Future Consequences (CFC), Participants scored significantly lower than the normative sample (Joireman et al., 2012) on the CFC-Future subscale, suggesting reduced concern for long-term consequences compared to the normative sample. Despite this, their scores were still significantly above the midpoint of the scale, indicating a moderate to high concern with future outcomes. This finding, moderate concern for future outcomes and low concern for immediate consequences may suggest that participants do value future impacts of their behaviour, but possibly not to the same extent as broader populations. The comparatively lower CFC-Future score may help explain why some long-term security behaviours (like regularly updating passwords or software) were not as robust in this sample, despite general awareness of threats.

The regression analyses highlighted the importance of realistic threat perception and proactive awareness in how participants respond to online threats. Lower levels of unrealistic optimism about detecting threats and higher scores on the SeBIS Proactive Awareness subscale were linked to better recognition of threat types.

6.5.1 Limitations of the Study

The study had a number of limitations which need to be considered. The data relied heavily on participants' self-reports, although compared to the survey, participants were now only reporting on events which had happened the same day, and they were asked to make a few notes about any potential online threats when they occurred and take a screenshot if possible. This should have decreased the problems of poor and distorted memory of events, which is typical of traditional questionnaires. However, there may still have been a misunderstanding of the questions, and in particular social desirability bias. For example, some participants might underreport their risky interactions with threats or overstate their security awareness.

Although the diary periods (7 and 14 days) were designed to reduce participant fatigue, the relatively short duration may not reflect long-term online behaviour or rare threat encounters. It also limits the ability to observe patterns over time. However, the decision was made due to the challenge faced in the previous diary study with the Saudi participants, when I had great difficulty recruiting participants and retaining them in the study, so I went for a shorter period and a larger sample. The sample mainly consisted of Prolific participants, who were relatively technology literature (Althobaiti et al., 2021). This may limit the generalisability of the findings to wider young adults with more varied range of digital literacy levels.

Chapter 7 Final Discussion and Conclusion

This chapter presents the key findings across the programme of research about the experience, recognition, and response to online security threats by younger adults in two different cultural contexts: the United Kingdom and Saudi Arabia. The overall aim of this research programme was to investigate the types and frequencies of online threats encountered by younger adults in both countries. How they perceive these threats and deal with them, and understand the role of individual characteristics, such as risk taking, thinking about the future, online security intentions, and demographic factors, in shaping younger adults' responses to real-world online threats.

7.1 Summary of Key Findings Across Studies

In this section, I present a summary of the key findings across all four studies in relation to the thesis objectives, integrating insights related to Objective 4 by highlighting differences between UK and Saudi participants across threat types, detection strategies, and responses.

Obj 1. Identify the types and frequency of online security threats encountered by younger adults in the UK and KSA.

The first two studies were online surveys which provided valuable insights into the types of online threats experienced by participants from the UK and KSA. Phishing and spear phishing were the most frequently encountered threats in both countries, around three-quarters of participants experienced it. In particular, messages that appeared to come from trusted sources were the most frequent type of phishing. Malware, specifically that delivered through malicious links, was frequently reported in both countries. In contrast, threats such as ransomware and spoofed websites were among the least frequently reported.

These findings were further supported by the diary studies, which captured participants' self-reported encounters with threats on a daily basis. In the KSA diary study, the majority of threats were phishing-related, with general phishing via email being the most frequently reported. Spear phishing, which often involves impersonation of banks or employers, was also common, while smishing (phishing via SMS) and WhatsApp-based phishing appeared less frequently. Similarly, in the UK diary study, phishing was also the most commonly encountered threat.

This finding aligns with expectations, as phishing remains a widespread and frequently reported issue in both academic literature (Alhashim & Hafizur Rahman, 2021; Alkhalil et al., 2021; Kettani & Wainwright, 2019) and international cybersecurity reports (Action Fraud News, 2025; APWG, 2024).

Phishing threats across various contexts highlight the ongoing effectiveness of deception-based attacks. According to global cybersecurity monitoring bodies such as the Anti-Phishing Working Group (APWG, 2024), phishing remains one of the most reported cybercrimes worldwide, with millions of incidents affecting individuals across regions. The persistent nature of these threats across different countries indicates that phishing is a global concern, particularly for younger adult users in their everyday digital interactions. This underscores the need for improved user detection strategies and support mechanisms.

Obj 2. Examine how younger adults in both countries detect and respond to online threats and the cues that support their threat recognition.

Participants identified threats by using cues related to message content and design, device behaviour, or suspicious requests. The most commonly used detection cues included suspicious design elements and requests for personal information, followed by unusual device behaviour, especially in malware cases, and prior knowledge in phishing contexts. Prior knowledge about the type of threat was one of the detection cues that emerged from responses to phishing scenarios in the survey studies. This cue has been found in previous research that users rely on what they hear from families and friends, as well as their own exposure to threats, to learn about online threats (Jeske & van Schaik, 2017).

For both countries, an interesting pattern in the timeline of detection also emerged: malware threats were often recognised only after noticeable issues with device performance, such as slowdowns or unexpected pop-ups. This suggests that the detection of these threats tends to be reactive, occurring after the harm may have already begun. In contrast, threats such as phishing were more likely to be identified through initial use of cues, indicating a more proactive recognition process.

Although the UK and KSA diary studies used different methods for capturing detection cues, open-ended responses in the KSA study and multiple-choice responses in the UK study, there were similarities in the types of cues reported by participants. In the KSA sample, the most frequently cited cues were related to language and content, such as requests for sensitive information or incorrect information. These were followed by technical indicators, including suspicious sender names or hidden URLs. Some participants also mentioned relying on prior knowledge to recognise common scam tactics. Similarly, UK participants frequently reported using technical indicators such as suspicious or unknown sender names or numbers to detect threats. However, in the UK sample, the frequency of specific types of cues was not the same as those in the KSA sample; this might be due to the differences in reporting formats.

Supporting these findings, an experimental study by Alsharnouby et al. (2015) examined Canadian university students' ability to detect phishing websites using eye-tracking technology. The study found that users tended to focus more on the website's content rather than on the browser's security indicators. This suggests that visual cues designed to help users detect phishing sites are often overlooked. Interestingly, Alsharnouby et al.'s study also found that participants who spent more time looking at browser elements, such as the address bar, performed better in detecting threats.

However, in the current UK and KSA diary studies, certain cues such as messages that created urgency or impersonated a friend or boss, were not mentioned by participants, even though they were visible in the uploaded screenshots. These cues fall under the "Common Tactics" category of the Phish Scale. Their absence from participants' reports may be because users have not noticed them at the time of interaction, or participants may have perceived some cues as less important to report. Spelling and grammar errors, frequently highlighted in previous research (Parsons et al., 2015; Steves et al., 2020), were also rarely reported by both samples. This suggests that detection is not only influenced by cue presence but also by users' perceptions of the relevance and salience of

the cues, so there is a need for improved detection literacy to support users in identifying both obvious and subtle cues of phishing and other threats.

When responding to threats, UK participants reported employing a range of solutions. Technical actions, such as scanning the device or restarting it, were most frequently used in cases of malware, while managing account settings and seeking support were more common in response to phishing or data theft. Among Saudi participants, reports of responses were generally limited in both number and diversity. In phishing scenarios, the most common action reported was simply avoiding interaction with the threat, and a few participants reported blocking the sender. In particular, reporting the threat to authorities or platforms was rarely mentioned across both samples. It was only mentioned four times by Saudi participants and five times by the UK participants, primarily about phishing or data theft. This suggests that although some protective behaviours were present, more proactive or formal responses, such as reporting, remain uncommon.

The adequacy of the solutions proposed to threats by both UK and KSA participants was assessed by comparing the solutions participants followed when they encountered threats similar to those presented in the scenarios to a set of solutions recommended by experts. In several cases, participants chose only partial or insufficient solutions. For example, in a scenario where experts recommended multiple actions (e.g. contact providers, recovering the account, and changing passwords), many participants performed only one action, suggesting limited understanding of comprehensive threat mitigation. Interestingly, phishing and spear phishing scenarios showed high rates of adequate responses than malware. One possible explanation is that these types of threats are more commonly encountered by users, which may increase their familiarity and awareness (Jeske & van Schaik, 2017). Greater exposure over time may lead to a better understanding of typical warning signs, making it easier for users to recognise and respond to such threats appropriately.

Another possible explanation for the high rate of adequate solutions for phishing attacks is that inaction, such as ignoring or not interacting with phishing emails, was coded as an adequate response. This contrasts with the coding approach used by Jaeger and Eckhardt (2021), who considered inaction to be insecure behaviour, arguing that it reflected a lack of motivation to resist phishing attempts. They defined secure actions as actively protective steps (e.g. deleting the phishing email or reporting it). In the present research, however, the assessment of response adequacy was based on widely accepted security guidelines and recommendations found in cybersecurity reports and expert advice. These sources generally stated that ignoring or not engaging with phishing messages is an appropriate solution, particularly for general users.

Analysis of the KSA diary study (Chapter 5) found a set of six behavioural patterns that emerged, reflecting how participants responded to online threats. These patterns can be understood as progressing through three general phases: (1) possible initial suspicion, (2) interaction or non-interaction, and (3) outcome. The most frequent pattern was when participants initially found something was suspicious, which might be based on cues such as unexpected messages or requests for personal information. This led to a decision point: either to interact with the content (e.g. clicking a link, opening a message) or to avoid interaction. Then the outcome is either a threat or not. Another common pattern observed was when participants did not suspect the threat and chose to interact or took some form of action (such as clicking a link or opening a message), and later discovered it was actually a threat.

These behavioural patterns illustrate how users navigate uncertainty about possible online threats in real-time and provide insights into threat recognition and decision-making processes. By mapping participant responses into these three phases, the analysis revealed that user behaviour is not set (the same participant may show different patterns across different threat encounters) but is shaped by evolving perceptions and situational cues. It also underscores the importance of reinforcing security guidance at each stage, not only teaching users how to detect suspicious elements, but also what to do next and how to evaluate the outcome of their actions.

Obj 3. Investigate how individual characteristics, such as risk-taking, security behaviour intentions, consideration of future consequences, and unrealistic optimism, affect their experiences of online threats.

The results from the SeBIS subscales on general online security behavioural intentions revealed several similarities and differences in the self-reported security behaviours of young adults in the UK and KSA. In both samples, participants scored significantly higher than the original normative sample (Egelman & Peer, 2015) and the midpoint on the Device Securement subscale. This suggests that screen locking and securing devices are well-established habits among younger adults in both countries. This may reflect increased reliance on mobile technologies and growing public awareness of device privacy across different cultural contexts. The SeBIS normative sample consisted of American older adults aged between 18 and 69 years.

In contrast, both samples reported significantly lower scores on the Updating subscale compared to the normative data and the scale midpoint. This indicates a shared reluctance or delay in applying security updates, despite such actions being widely recommended in cybersecurity guidance. These findings are consistent with broader literature showing that users across cultures tend to postpone or ignore software updates due to inconvenience, perceived low risk, or lack of awareness (Rajivan et al., 2020). The consistency of this practice across two distinct national contexts suggests that updating behaviour remains a global challenge, not just a regional one.

When it comes to Password Generation, both samples demonstrated room for improvement, though the issue appeared more pronounced in the Saudi sample. While UK participants did not significantly differ from the normative mean, Saudi participants scored significantly lower, indicating weaker practices in creating strong and unique passwords. This agrees with previous studies in the Saudi context reporting poor password practices and frequent reuse of passwords (Alkhaiwani & Almalki, 2021; Alqahtani, 2022). Cultural factors may also play a role; for instance, sharing passwords with close family members, especially spouses, has been documented among Saudi users despite it contradicting formal security regulations in the KSA (Flechais et al., 2013).

For risk taking as measured by DOSPERT, Saudi younger adults were found to be less risk-taking compared to the original normative sample by Blais and Weber (2006), which included university students from the United States and Canada. The Saudi sample scored significantly lower on several subscales, particularly Ethical, Health/Safety, and Social, suggesting more risk-averse tendencies in these areas. Similarly, UK participants showed lower risk-taking scores across all subscales than the normative sample, with particularly low scores in the Ethical and Recreational subscales.

However, this comparison of risk taking should be interpreted in light of both temporal and cultural differences. The Blais and Weber normative data were collected nearly two decades ago in a different social and technological context. Over time, risk attitudes may shift due to broader societal, cultural, and economic changes (Varnum & Grossmann, 2017). For example, recent studies have found that younger generations in the UK have become more cautious and risk-aware in several domains and have a heightened awareness of mental health and personal safety (Pennay et al., 2025). These shifts may help explain the more risk aversive scores among UK participants, especially in areas involving ethical and recreational risks.

While this risk-aversive orientation may appear protective, it does not automatically translate into safer online practices. Other results from the UK and KSA diary studies (e.g. SeBIS scores and reported experiences with threats) suggest that participants still struggle with security behaviours. This indicates that attitudes toward digital risks may not always agree with a broader risk aversion as captured by DOSPERT. Moreover, previous research has reported mixed findings regarding the relationship between specific risk domains and risk in relation to security behaviours. For example, Egelman and Peer (2015) found that social risk-taking was significantly associated with password generation behaviours, whereas Gratian et al. (2018) found no such relationship. These inconsistencies highlight the need to examine risk perception in more context-specific ways when assessing online security practices.

The Consideration of Future Consequences (CFC) results in the diary studies showed that participants from both samples were generally more focused on future outcomes than immediate outcomes, showing a tendency to consider the long-term impact of their actions. In previous research, this trait has been linked to better security practices (Egelman & Peer, 2015). However, this association was not supported by the findings in either sample.

Although participants in both samples rated themselves above the midpoint for computer and security knowledge, this did not consistently translate into stronger self-reported security behaviours. This highlights a potential gap between knowledge and action, a well-documented issue in security research (Parsons et al., 2013) as individuals may be aware of recommended practices but fail to apply them. This self-assessed confidence, even if not matched by consistently secure behaviour, may explain the pattern of considerable unrealistic optimism observed in both samples.

KSA participants reported unrealistic optimism in relation to online threats, rating themselves as more capable than their peers at detecting and dealing with threats. This cognitive bias could reduce perceived vulnerability and potentially increase risky behaviour, despite good intentions. However, unrealistic optimism did not significantly predict whether participants interacted with online threats. This suggests that believing oneself to be less vulnerable than others did not lead to measurable differences in behaviour, though this may be due to the small sample size of the KSA study.

Similarly, unrealistic optimism was reported in the UK participants' self-assessment, while they considered themselves as likely as their friends and a typical person of their age to face threats, they believed they were better equipped to detect and deal with threats. This agrees with prior findings on optimism bias among younger, educated users and may contribute to overconfidence in their security decision-making (Hewitt & White, 2022).

Obj 4. Compare cultural similarities and differences between younger adults in the UK and KSA regarding their threat experiences, perceptions, and online security behaviours.

While culture has often been emphasised as a key factor influencing online security behaviours, the findings of this programme of research suggest that cultural background alone may not fully explain how users detect and respond to online threats. Despite being drawn from two distinct cultural contexts, KSA and the UK, participants showed broadly similar patterns in the types of threats encountered (especially phishing), the cues they relied on for detection, and the range of responses reported. For example, reporting behaviours to appropriate authorities remained rare, and protective actions such as blocking or searching online for more information were more common than actively changing passwords or securing accounts. Both samples showed relatively high confidence in their ability to detect and deal with attacks (reflecting elements of unrealistic optimism), and moderate to high SeBIS scores, particularly on Device Securement, alongside low scores on Password Generation and Proactive Awareness. These similarities suggest that despite cultural and regional differences, there are shared behaviours and challenges in how younger adults experience online threats.

These similar results highlight the importance of shifting focus toward the individual level, considering personal characteristics (e.g. digital literacy, risk perception, prior exposure), situational constraints, and the systems and tools available at the point of action. In this light, security support should move beyond generalised cultural assumptions and instead offer flexible, context-aware guidance that adapts to the needs of diverse users within a shared digital ecosystem.

This agrees with prior research showing that while culture can influence privacy attitudes, it is not a strong predictor of actual cybersecurity behaviour (Halevi et al., 2016). Rather, individual-level variables, such as personality, prior and technical experience, may play a greater role across cultural contexts. A comparative study of password behaviours in China, Turkey, and the UK found that while Hofstede's dimensions offered partial explanations, actual behaviours often diverged from predictions, highlighting the complexity of cultural influence on password security (Petrie & Merdenyan, 2016).

There has also been a growing call in security research to focus not only on user knowledge, but also on the broader networks of influence, including social norms, technical affordances, and prior experience, that shape behaviour at the moment of threat. For example, users may fail to report phishing not due to cultural reluctance, but because the option to report is not visible, intuitive, or socially reinforced.

This shift in perspective aligns well with Actor-Network Theory (Latour, 1999), which I only came across late in my research and which offers a useful lens to understand how security behaviour emerges through dynamic interactions between users, technologies, and the surrounding environment.

7.2 Interpreting User Behaviour Through Actor-Network Theory

The results across all four studies suggest that participants' responses to online threats are not solely shaped by their individual knowledge or attitudes, but by a combination of factors present at the

time of the incident. While some participants demonstrated awareness of threats or rated their security knowledge highly, their actions did not always align with secure behaviour.

The data collected from the four studies indicate that participants' responses to online threats followed phases that outline the progression users made when encountering the incident. This process typically begins with detection, followed by an immediate decision or action at the time of the encounter, and, in some cases, extends to further protective measures based on the perceived severity or nature of the threat.

During detection, participants often recognised phishing threats. However, the number of cues reported did not reflect all the cues presented in the screenshots or answers; some cues, such as urgency or impersonation, were present in the screenshots but not explicitly identified by participants in their responses. This suggests that these cues were not always consciously processed. During the immediate response and once a threat was detected, the most common responses were minimal, such as deleting the message or ignoring it. In some instances, participants blocked the sender or searched online to verify the threat. These reactions were often considered routine actions taken upon noticing the threat. Finally, further protective measures were only followed by a few participants in who reported taking additional steps, such as changing passwords or updating account settings. These more proactive responses were appropriate only in specific cases, such as when account details were entered in the phishing link.

Actor-Network Theory (ANT) provides a useful lens to interpret this gap between awareness and behaviour. ANT is a sociotechnical framework that views actions and outcomes as the result of interactions between human and non-human actors within a network (Latour, 2005). Rather than treating behaviour as driven solely by individual intention or knowledge, ANT emphasises how technologies, interfaces, rules, tools, and social practices collectively shape what actions become possible or likely in a given situation. ANT suggests that security behaviour is not produced by the individual alone but emerges from a network of interacting elements, human and non-human, including the user, the threat design (e.g. cues, context), the available support options (e.g. block or report buttons), past experiences, and social norms (Jeske & van Schaik, 2017). For instance, if a participant notices a suspicious message but the interface lacks clear reporting tools or warnings, the network does not support protective action, even if the user has the intent. Similarly, cultural norms (e.g. viewing phishing as normal or not worth reporting) may influence whether the user feels a response is necessary.

By viewing security responses as the outcome of these interconnected networks, it becomes possible to better understand why some users fail to act, or act inconsistently, even when they are aware of potential risks. This approach supports the argument that improving online security behaviours requires not only raising awareness but also addressing the broader systems and contexts in which users operate.

Building on this actor-network perspective not only shifts the focus from individual responsibility to the relational conditions of action but also highlights a significant limitation in many current security guidelines. They often assume that users are technically skilled and highly motivated individuals. In contrast, findings from this thesis demonstrate that younger adults in both the UK and KSA encounter online threats within dynamic socio-technical environments. Their decisions are

influenced by device interfaces, peer norms, prior experiences, and the clarity of the available advice. Unfortunately, existing user guidance is often scattered across platforms, inconsistently organised, and difficult to access during real-time decision-making. One practical implication emerging from this analysis is the need for a centralised, user-centred support resource. This would serve as a single digital point of access where users who face or fall victim to an online threat can receive prioritised, actionable guidance. Instead of overwhelming users with general hygiene practices (e.g. password strength and regular backups), such a resource could distinguish between ongoing preventative habits and urgent, situation-specific actions, such as scanning for malware, deleting infected files and changing account details. This approach would not only reduce cognitive load during high-stress moments but also improve the likelihood that users engage in effective protective behaviours.

7.3 A Diary-Based Self-Diagnostic Tool for Online Threat Awareness

Building on the success of the diary study in encouraging participants to capture and reflect on their personal encounters with online threats, a potential practical outcome of this research is the concept of a diary-based self-diagnostic tool for online threat awareness. Rather than serving as a data collection instrument for researchers, such a tool would be designed for end users and would support reflection on recent online threat experiences in a structured yet lightweight manner.

The core idea would be to prompt users, over a short period, to document recent encounters with suspicious messages, links, or online incidents, focusing on how the threat was noticed, what cues were relied upon, and what actions were taken. This process would encourage them to reflect on their behaviour and mirrors the diary method used in this research, but would be adapted for everyday use, with a focus on helping users recognise patterns in their own behaviour rather than providing exhaustive reporting. By encouraging users to articulate their experiences shortly after encountering a threat, the tool could support awareness of commonly overlooked cues and habitual response strategies.

Importantly, the value of such a tool would lie not only in reflection but in how that reflection connects users to appropriate guidance. Based on the type of threat encountered and the actions reported, users could be directed towards clear, situation-specific advice relevant to their context. Existing official resources already demonstrate how such guidance can be structured. For example, in the UK, services such as Get Safe Online (Get Safe Online, 2026) and guidance from the National Cyber Security Centre (NSCS, n.d) provide practical steps for responding to phishing, malware, and account compromise. In the KSA, organisations such as Saudi CERT publish alerts and user-focused guidance on common online threats. These resources illustrate how actionable support can be organised around concrete threat scenarios rather than abstract security principles.

This approach aligns with the actor-network perspective discussed earlier in the chapter by recognising that secure behaviour emerges from interactions between users, threat characteristics, interfaces, and available support mechanisms. Rather than assuming high levels of technical expertise or motivation, the diary-based self-diagnostic tool would support users at the point where decisions are made, linking their own experiences to relevant guidance that is timely and accessible. In this way, reflection becomes an entry point to awareness raising and support, grounded in situations users have encountered.

Any further design, implementation, or evaluation of such a tool falls beyond the scope of this thesis and is therefore proposed as a direction for future research. Future work could explore how diary-based self-reflection might be adapted across cultural contexts, how much structure is needed to balance usability and insight, and how such a tool could be evaluated as an engagement and learning mechanism rather than a traditional security intervention.

7.4 Research Limitations and Future Work

While this programme of research has provided important insights into the experiences, perceptions, and behaviours of young adults in the UK and KSA regarding online threats, several limitations in the research should be acknowledged.

First, the research relied primarily on self-reported data through surveys and diary entries. Although these methods captured rich subjective accounts, they may not fully reflect actual behaviours due to recall bias or social desirability. Future research should complement these approaches with experimental or observational methods that can capture real-time user responses to simulated threats. For example, a planned phishing simulation study could observe participants' in-situ behaviours when encountering suspicious emails in more naturalistic settings, allowing for a closer examination of their detection cues, reaction, and decision-making strategies. However, such research is extremely time-consuming for researchers and participants. For example, Distler (2023) observed 14 participants in their regular work environments to understand their responses to a spear-phishing attack. The participants were instructed to work as they normally would for one hour without being informed that the study focused on phishing. After 50 minutes, a simulated phishing email was sent to the participants. After this period, the researcher conducted interviews to gather qualitative data about the participants' thoughts, emotions, and decisions. The study employed a combination of observational data through live streaming, where a camera was set up to monitor participants' interactions with their environment, along with interviews and a UX curve (a reflective exercise) to gain insights into the participants' emotions, thought processes, and actions.

Second, the sample sizes, particularly for the diary studies, were relatively small. This limits the generalisability of the findings and the ability to conduct robust statistical analyses, particularly comparisons between groups. Future studies should involve larger samples from both countries to improve validity and explore cross-cultural differences with greater confidence.

Third, while validated psychological measures such as SeBIS, DOSPERT, and CFC were used, it is important to note that these scales were originally developed and validated in other countries, often years ago. This study could not test the predictive validity of these scales against observed behaviour. Further work is needed to assess whether and how these individual difference measures correspond to actual security practices, especially in high-risk or time-sensitive threat contexts. A future large-scale study will aim to explore these relationships in depth and consider whether these instruments require adaptation for different cultures.

Taken together, these next steps aim to move beyond intention and perception to more accurately understand and support user behaviour in the face of evolving online threats. The above limitations highlight the need for future research that captures real-world user behaviour more directly and translates findings into practical support tools. One promising direction is the development of a

diary-based self-diagnostic tool that enables users to reflect on recent threat encounters and access tailored guidance. This would help shift from understanding user behaviour to actively supporting safer online practices in everyday contexts.

This thesis provides a cross-cultural perspective on how younger adults in the UK and KSA encounter, detect, and respond to online threats. By combining survey data with an innovative diary method, used for the first time in both countries, this research offers valuable insights into users' experiences of online threats. Key findings reveal that phishing is consistently prevalent in both countries, with shared challenges in detection, such as limited recognition of cues, and varied but often ineffective response strategies. These results not only enhance our understanding of end-user security practices but also establish a foundation for more user-centred support approaches.

References

Action Fraud News. (2025, May 7). New alert issued as action fraud reveals staggering rise of extortion phishing email reports in March. Action Fraud. https://www.actionfraud.police.uk/news/extortion-alert

Ainin, S., Jaafar, N. I., & Dezdar, S. (2015). Consideration of future consequences among managers in Iran and Malaysia. *Futures*, *71*, 29–35. . https://doi.org/https://doi.org/10.1016/j.futures.2015.06.003

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet*, *12*(10), 168. https://doi.org/10.3390/fi12100168

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*. . hhttps://doi.org/10.1016/j.chb.2022.107376

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, *8*(1). https://doi.org/10.1186/s13673-018-0128-7

Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1). https://doi.org/10.1186/s42400-020-00047-5

Aldossary, A. A., & Zeki, A. M. (2016). Web users' knowledge and their behavior towards security threats and vulnerabilities. *Proceedings - 2015 4th International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2015*, 256–260. https://doi.org/10.1109/ACSAT.2015.51

Alelyani, S., & GR, H. K. (2018). Overview of cyberattack on Saudi organizations. *Journal of Information Security and Cybercrimes Research*, *1*(1), 32-39.

Aleroud, A., Abu-Shanab, E., Al-Aiad, A., & Alshboul, Y. (2020). An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities. *Journal of Information Security and Applications*, *55*. https://doi.org/10.1016/j.jisa.2020.102614

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, *26*(6), 661–687. https://doi.org/10.1057/s41303-017-0057-y

Alhashim, S. S., & Hafizur Rahman, M. M. (2021). Cybersecurity threats in line with awareness in Saudi Arabia. *2021 International Conference on Information Technology, ICIT 2021 - Proceedings*, 314–319. https://doi.org/10.1109/ICIT52682.2021.9491711

Aljeaid, D., Alzhrani, A., Alrougi, M., & Almalki, O. (2020). *Assessment of end-user susceptibility to cybersecurity threats in Saudi Arabia by simulating phishing attacks*. https://doi.org/10.3390/info11120547

Alkhaiwani, A. H., & Almalki, G. A. (2021, March 27). Saudi human awareness needs. A survey in how human causes errors and mistakes leads to leak confidential data with proposed solutions in Saudi Arabia. *Proceedings - 2021 IEEE 4th National Computing Colleges Conference, NCCC 2021*. https://doi.org/10.1109/NCCC49330.2021.9428790

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. In *Frontiers in Computer Science* (Vol. 3). Frontiers Media S.A. https://doi.org/10.3389/fcomp.2021.563060

Alohali, M., Clarke, N., Furnell, S., & Albakri, S. (2017). *information Security Behavior: Recognizing the Influencers* (IEEE).

Alotibi, G. (2024). A cybersecurity awareness model for the protection of Saudi students from social media attacks. *Engineering, Technology & Applied Science Research, 14*(2), 13787–13795. https://doi.org/10.48084/etasr.7123

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). *A survey of cyber-security awareness in Saudi Arabia*.

Alowais, S., Armeen, I., Sharma, P., & Johnston, A. (2023). Cyber hygiene practices across cultures: A cross cultural study of the US and Saudi Arabia based information systems users. In (pp. 744-750): *Procedia Computer Science*.

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences (Switzerland)*, *12*(5). https://doi.org/10.3390/app12052589

Alqarni, A. M., Timko, D., & Rahman, M. L. (2023). Saudi Arabian perspective of security, privacy, and attitude of using facial recognition technology. *2023 20th Annual International Conference on Privacy, Security and Trust, PST 2023*. https://doi.org/10.1109/PST58708.2023.10320185

Alseadoon, I., Chan, T., Foo, E., & Gonzalez Nieto, J. (2012). *Who is more susceptible to phishing emails?: A Saudi Arabian study*. https://aisel.aisnet.org/acis2012/21

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human Computer Studies*, *82*, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Althobaiti, K., Meng, N., & Vaniea, K. (2021, May 6). I don't need an expert! making url phishing features human comprehensible. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3411764.3445574

Alyahya, A., & Weir, G. R. S. (2021, March 27). Understanding responses to phishing in Saudi Arabia via the theory of planned behaviour. *Proceedings - 2021 IEEE 4th National Computing Colleges Conference, NCCC 2021*. https://doi.org/10.1109/NCCC49330.2021.9428823

Alzahrani, L. (2021). Statistical analysis of cybersecurity awareness issues in higher education institutes. *International Journal of Advanced Computer Science and Applications*, *12*(11). www.ijacsa.thesai.org

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1). https://doi.org/10.1016/j.heliyon.2021.e06016

APWG. (2024). *Phishing activity trends reports*. https://apwg.org/trendsreports/

Ayyagari, R., & Crowell, A. (2020). Risk and demographics' influence on security behavior intentions. *Journal of the Southern Association for Information Systems*, *7*(1). https://doi.org/10.17705/3JSIS.00013

BBC News. (2016). "Smart" home devices used as weapons in website attack. https://www.bbc.com/news/technology-37738823

BBC News. (2017). Ukraine power cut "was a cyber-attack". https://www.bbc.com/news/technology-38573074

BBC News. (2019, April 4). *Data on 540 million Facebook users exposed*. https://www.bbc.com/news/technology-47812470

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51–61. https://doi.org/10.1016/j.chb.2015.01.039

Bera, D., Ogbanufe, O., & Kim, D. J. (2023). Towards a thematic dimensional framework of online fraud: An exploration of fraudulent email attack tactics and intentions. *Decision Support Systems*, *171*. https://doi.org/10.1016/j.dss.2023.113977

Bitton, R., Boymgold, K., Puzis, R., & Shabtai, A. (2020). *Evaluating the information security awareness of smartphone isers*. 258. https://doi.org/10.1145/3313831.3376385

Blais, A.-R., & Weber, E. U. (2006). A Domain-Specific Risk-Taking (DOSPERT) scale for adult populations. *Judgment and Decision Making*, *1* (1). http://ssrn.com/abstract=1301089Electroniccopyavailableat:http://ssrn.com/abstract=1301089

Butler, S. (2025, April 29). M&S cyber-attack linked to hacking group Scattered Spider. *The Guardian*. https://www.theguardian.com/business/2025/apr/29/m-and-s-cyber-attack-linked-to-hacking-group-scattered-spider

Buxton, O. (2025, February 28). *Malware: What it is, how it works, and how to get rid of it*. https://uk.norton.com/blog/emerging-threats/malware

Caldwell, T. (2013). Spear-phishing: how to spot and mitigate the menace. *Computer Fraud & Security*, *2013*(1), 11–16. https://doi.org/10.1016/s1361-3723(13)70007-1

Centre for Strategic and International Studies CSIS. (2025). Significant cyber incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Chalhoub, G., & Kraemer, M. J. (2021, May 6). It did not give me an option to decline: A longitudinal analysis of the user experience of security and privacy in smart home products. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3411764.3445691

Chetty, M., Kim, H., Sundaresan, S., Burnett, S., Feamster, N., & Edwards, W. K. (2015). UCap: An internet data management tool for the home. *Conference on Human Factors in Computing Systems - Proceedings*, *2015-April*, 3093–3102. https://doi.org/10.1145/2702123.2702218

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. In *Expert Systems with Applications* (Vol. 106, pp. 1–20). Elsevier Ltd. https://doi.org/10.1016/j.eswa.2018.03.050

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *SA Journal of Information Management*, *23*(1), 1–11. https://doi.org/10.4102/sajim.v23i1.1277

Cifas. (2025, April 3). *Fraudscape 2025: Reported fraud hits record levels*. Cifas.org.uk; Cifas. https://www.cifas.org.uk/newsroom/fraudscape-2025-record-fraud-levels

Coles-Kemp, L., Jensen, R. B., & Heath, C. P. R. (2020, April 21). Too much information: Questioning security in a post-digital society. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3313831.3376214

Communications, Space & Technology Commission (CSTC). (2025, May 12). *Saudi Internet report 2024.* Communications, Space & Technology Commission, Kingdom of Saudi Arabia. https://www.cst.gov.sa/en/media-center/news/N2025051200

Computing and Communication Services, T. (2025). *Sophisticated phishing attacks*. Toronto Metropolitan University (TMU). https://www.torontomu.ca/ccs/services/ITSecurity/protecting-your-identity/phishing/sophisticated-phishing-attacks/#

Corera, G (2020). Coronavirus: Hackers targeted Covid vaccine supply "cold chain". https://www.bbc.com/news/technology-55165552

Cramer, F. (2015). What is "post-digital"? *Postdigital aesthetics: Art, computation and design* (pp. 12–26). London: Palgrave Macmillan UK.

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: A comparative study of nations and regions. *Personal and Ubiquitous Computing, 25*(5), 941–955. https://doi.org/10.1007/s00779-021-01520-7

Cybersecurity and Infrastructure Security Agency (CISA). (2023, October 18). *Phishing guidance: Stopping the attack cycle at Phase One*. https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

CybSafe. (2020). *Human error to blame for 9 in 10 UK cyber data breaches in 2019*. https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/ .

Debb, S. M., Schaffer, D. R., & Colson, D. G. (2020). A reverse digital divide: Comparing information security behaviors of Generation Y and Generation Z adults. *The International Journal of Cybersecurity Intelligence and Cybercrime*, *3*(1), 42–55. https://doi.org/10.52306/03010420gxuv5876

Department for Science, Innovation and Technology. (2023, April 11). *UK wireless infrastructure strategy.* GOV.UK. https://www.gov.uk/government/publications/uk-wireless-infrastructure-strategy/uk-wireless-infrastructure-strategy

Deutrom, J., Katos, V., & Ali, R. (2022). Loneliness, life satisfaction, problematic internet use and security behaviours: Re-examining the relationships when working from home during COVID-19. *Behaviour and Information Technology*, *41*(14), 3161–3175. https://doi.org/10.1080/0144929X.2021.1973107

Distler, V. (2023). *The influence of context on response to spear-phishing attacks: an in-situ deception study*. https://doi.org/10.1145/3544548.3581170

Dodge, C. E., Fisk, N., Burruss, G. W., Moule, R. K., Jr., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy, 22*(4), 849–868. https://doi.org/10.1111/1745-9133.12641

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). *Decision strategies and susceptibility to phishing*. https://doi.org/https://doi.org/10.1145/1143120.1143131

Dumas, J. F., & Redish, J. C. (1993). *A practical guide to usability testing*. Greenwood Publishing Group Inc.

Edwards, T. (2024, September 28). *Transport for London (TfL) cyber attack: What you need to know*. https://www.bbc.com/news/articles/ceqn7xng7lpo

Egelman, S., & Peer, E. (2015a). *Predicting privacy and security attitudes*. https://doi.org/https://doi.org/10.1145/2738210.2738215

Egelman, S., & Peer, E. (2015b). Scaling the security wall: Developing a Security Behavior Intentions Scale (SeBIS). *Conference on Human Factors in Computing Systems - Proceedings*, *2015-April*, 2873–2882. https://doi.org/10.1145/2702123.2702249

Egelman, S., Harbach, M., & Peer, E. (2016). Behavior ever follows intention? A validation of the Security Behavior Intentions Scale (SeBIS). *Conference on Human Factors in Computing Systems - Proceedings*, 5257–5261. https://doi.org/10.1145/2858036.2858265

European Union Agency for Cybersecurity (ENISA). (2024). *ENISA threat landscape 2024*. https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

European Union. (2023). *ENISA threat landscape 2023: July 2022 to June 2023.* Publications Office of the EU. https://op.europa.eu/en/publication-detail/-/publication/3bd053c2-9e1e-11ee-b164-01aa75ed71a1/language-en/format-PDF/source-317574128 .

Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers and Security*, *80*, 74–89. https://doi.org/10.1016/j.cose.2018.09.002

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian universities. *Journal of Physics: Conference Series*, *1339*(1). https://doi.org/10.1088/1742-6596/1339/1/012098

Flechais, I., Jirotka, M., & Alghhamdi, D. (2013). *In the balance in Saudi Arabia: Security, privacy and trust*. ACM.

Furnell, S. (2007). Phishing: can we spot the signs? *Computer Fraud & Security*, *2007*(3), 10–15. https://doi.org/10.1016/S1361-3723(07)70035-0

Furnell, S. (2021). Categorising Cybercrime cybercrime and Cybercriminalscybercriminals. *Source: Journal of Information Warfare*, *20*(4), 68–76. https://doi.org/10.2307/27125014

Furnell, S., & Moore, L. (2014). Security literacy: the The missing link in today's online society? *Computer Fraud & Security*, *2014*(5), 12–18. https://doi.org/https://doi.org/10.1016/S1361-3723(14)70491-9

Get Safe Online. (2026). *Get Safe Online*. https://www.getsafeonline.org/

Gies, S. V., Piquero, N. L., Piquero, A. R., Green, B., & Bobnis, A. (2020). Wild, wild theft: Identity crimes in the digital frontier. *Criminal Justice Policy Review, 32*(6), 592–617. https://doi.org/10.1177/0887403420949650

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1), 22–44. https://doi.org/10.17705/1jais.00447

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers and Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Greitzer, F. L., Li, W., Laskey, K. B., Lee, J., & Purl, J. (2021). Experimental Investigation investigation of Technical technical and Human human Factors factors Related related to Phishing phishing Susceptibilitysusceptibility. *ACM Transactions on Social Computing*, *4*(2), 1–48. https://doi.org/10.1145/3461672

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*, 346. https://doi.org/10.1016/j.heliyon.2017

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F., & Chen, J. (2016). Cultural and psychological factors in cyber-security. *ACM International Conference Proceeding Series*, 318–324. https://doi.org/10.1145/3011141.3011165

Harbach, M., De Luca, A., Malkin, N., & Egelman, S. (2016). Keep on lockin' in the free world: A multi-national comparison of smartphone locking. *Conference on Human Factors in Computing Systems - Proceedings*, 4823–4827. https://doi.org/10.1145/2858036.2858273

He, J., Van de Vijver, F. J. R., Fetvadjiev, V. H., de Carmen Dominguez Espinosa, A., Adams, B., Alonso-Arbiol, I., Aydinli-Karakulak, A., Buzea, C., Dimitrova, R., Fortin, A., Hapunda, G., Ma, S., Sargautyte, R., Sim, S., Schachner, M. K., Suryani, A., Zeinoun, P., & Zhang, R. (2017). On Enhancing enhancing the Crosscross-Cultural cultural Comparability comparability of Likert-Scale scale Personality personality and Value value Measuresmeasures: A Comparison comparison of Common common Proceduresprocedures. *European Journal of Personality*, *31*(6), 642–657. https://doi.org/10.1002/per.2132

Hewitt, B., & White, G. (2021). Factors influencing security incidents on personal computing devices. *Journal of Organizational and End User Computing*, *33*(4), 1–27. https://doi.org/10.4018/JOEUC.20210701.oa9

Hewitt, B., & White, G. L. (2022). Optimistic bias and exposure affect security incidents on home computer. *Journal of Computer Information Systems*, *62*(1), 50–60. https://doi.org/10.1080/08874417.2019.1697860

Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, *57*. https://doi.org/10.1016/j.jisa.2020.102710

Honolulu, H. I., & Chi, U. (2020). *Examining the adoption and abandonment of security, privacy, and identity theft protection practices*. *20*. https://doi.org/10.1145/3313831.3376570

Huang, H.-Y., Seray Tuncay, G., Gunter, C. A., Bashir, M., Demetriou, S., & Hassan, M. (2023). *Evaluating user behavior in smartphone security: A psychometric perspective*. https://www.usenix.org/conference/soups2023/presentation/huang

Humayun, M., Niazi, M., Jhanjhi, · N. zZ., Alshayeb, · Mohammad., & Mahmood, · Sajjad. (2020). Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering*, *45*(3), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

ICO. (2024, May 10). *Phishing*. Ico.org.uk. https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/learning-from-the-mistakes-of-others-a-retrospective-review/phishing/

ICO. (2025, April). *Statement on British Library's 2023 ransomware attack*. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/04/statement-on-british-library-s-2023-ransomware-attack/

Ismail, E., & Farah, A. (2017). *A study on cybercrime awareness test in Saudi Arabia - – Alnamas region*. https://doi.org/10.1109/anti-cybercrime.2017.7905290

Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, *31*(3), 429–472. https://doi.org/10.1111/isj.12317

Jayatilaka, A., Asanka, N., Arachchilage, G., & Ali Babar, M. (2021). *Falling for phishing: An empirical investigation into people's email response behaviors.* Completed Research Paper.

Jeske, D., & van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers and Security*, *66*, 129–141. https://doi.org/10.1016/j.cose.2017.01.010

Joireman, J., Shaffer, M. J., Balliet, D., & Strathman, A. (2012a). Promotion orientation explains why future-oriented people exercise and eat healthy: Evidence from the Two-Factor Consideration of Future Consequences-14 Scale. *Personality and Social Psychology Bulletin*, *38*(10), 1272–1287. https://doi.org/10.1177/0146167212449362

Joireman, J., Shaffer, M. J., Balliet, D., & Strathman, A. (2012b). Promotion orientation explains why future-oriented people exercise and eat healthy: Evidence from the Two-Factor Consideration of Future Consequences-14 Scale. *Personality and Social Psychology Bulletin*, *38*(10), 1272–1287. https://doi.org/10.1177/0146167212449362

Kang, M., Shonman, M., Subramanya, A., Zhang, H., Li, X., & Dahbura, A. (2021). *Understanding security behavior of real users: Analysis of a phishing study*. http://behavior.isi.jhu.edu/ .

Kaspersky (n.d.-c). *What is smishing and how to defend against it?* https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it .

Kaspersky (n.d.-d). *What is spoofing?* https://usa.kaspersky.com/resource-center/definitions/spoofing .

Kaspersky (n.d.-e) *What is adware*? https://www.kaspersky.com/resource-center/threats/adware .

Kaspersky (n.d.-f) *Malware protection: All you need to know*. https://www.kaspersky.com/resource-center/threats/malware-protection .

Kaspersky Lab. (2024). *What is spoofing – Definition and explanation*. https://usa.kaspersky.com/resource-center/definitions/spoofing .

Kaspersky. (2022, October 9). *Financial cyberthreats targeting businesses in Saudi Arabia drop by 24% in Q2 of 2022*. /. https://me-en.kaspersky.com/about/press-releases/financial-cyberthreats-targeting-businesses-in-saudi-arabia-drop-by-24-in-q2-of-2022

Kaspersky. (n.d.-a). *What is a Trojan? Trojan virus explained*. https://www.kaspersky.com/resource-center/threats/trojans .

Kaspersky. (n.d.-b). *What is spear phishing?* https://usa.kaspersky.com/resource-center/definitions/spear-phishing .

Kävrestad, J., Fernow, R., Lööf, D., & Birath, M. (2024). *Multi-factor authentication adoption: A comparison between digital natives and digital immigrants in Sweden*.

Kettani, H., & Wainwright, P. (2019). *On the top threats to cyber systems*. IEEE.

Kidd, C. (2022) Cyber kill chains explained: Phases, pros/cons & security tactics. Splunk. https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html .

Latour, B. (1999). On recalling ANT. *The sociological review*, *47*(1_suppl), 15-–25.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.

Lazar, J., Feng, J. H., & Hochheiser, H. (2017). *Research methods in human-computer interaction*. Saint Louis Elsevier Science. https://www.elsevier.com/books/research-methods-in-human-computer-interaction/lazar/978-0-12-805390-4

Lemonnier, J., & Regan, J. (2022). *How to get rid of a virus & other malware on your computer*. https://www.avg.com/en/signal/how-to-get-rid-of-a-virus-or-malware-on-your-computer#topic-3

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020). *Experimental investigation of demographic factors related to phishing susceptibility*. Proceedings of the 53rd Hawaii International Conference on System Sciences.

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to spear-phishing emails. *ACM Transactions on Computer-Human Interaction*, *26*(5), 1–28. https://doi.org/10.1145/3336141

Lyon, G. (2023). Informational inequality: The role of resources and attributes in information security awareness. *Information and Computer Security*. https://doi.org/10.1108/ICS-04-2023-0063

Malware News. (2017). The state of Shamoon: Same actor, different lines. *Malware News*. Retrieved from: https://malware.news/t/the-state-of-shamoon-same-actor-different-lines/11146/1 [accessed 11 September 2025].

McAfee. (2022, August). *The McAfee safety series phishing protection guide*. https://media.mcafeeassets.com/content/dam/npcld/ecommerce/en-us/docs/guides/gd-phishing-security-guide.pdf .

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2016). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

Ministry of Communications and Information Technology (MCIT) (2025, April 27). *Saudi Arabia's digital economy: A new era of tech growth, innovation, and global impact empowered by HRH*. Ministry of Communications and Information Technology, Kingdom of Saudi Arabia. https://www.mcit.gov.sa/en/news/saudi-arabia%E2%80%99s-digital-economy-new-era-tech-growth-innovation-and-global-impact-empowered-hrh

Montasari, R. (2023). Cyber threats and the security risks they pose to national security: An assessment of cybersecurity policy in the United Kingdom. In *Advances in Information Security* (Vol. 101, pp. 7–25). Springer. https://doi.org/10.1007/978-3-031-21920-7_2

Mori, K., Watanabe, T., Zhou, Y., Hasegawa, A. A., Akiyama, M., & Mori, T. (2020). *Comparative analysis of three language spheres: Are linguistic and cultural differences reflected in password selection habits? IEICE Transactions on Information and Systems, 103*(7), 1541–1555. https://doi.org/10.1587/transinf.2019EDP7272

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. In *Frontiers in Psychology* (Vol. 12). Frontiers Media S.A. https://doi.org/10.3389/fpsyg.2021.561011

Naik, N., Jenkins, P., Grace, P., & Song, J. (2022). Comparing attack models for IT systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model. *ISSE 2022 - 2022 8th IEEE International Symposium on Systems Engineering, Conference Proceedings*. https://doi.org/10.1109/ISSE54508.2022.10005490

National Cyber Security Center (2021) Phishing scams: If you've shared sensitive information. (n.d.). wWww.ncsc.gov.uk. https://www.ncsc.gov.uk/collection/phishing-scams/what-to-do

National Cyber Security Center (NSCS). (n.d.). *Cyber aware: Advice on how to stay secure from the UK's National Cyber Security Center (NCSC)*. https://www.ncsc.gov.uk/cyberaware/home.

National Cyber Security Centre (NCSC). (2023). *Warns of enduring and significant threat to UK's critical infrastructure*. https://www.ncsc.gov.uk/news/ncsc-warns-enduring-significant-threat-to-uks-critical-infrastructure

National Cyber Security Centre (NCSC). (n.d.). *Glossary*. https://www.ncsc.gov.uk/section/advice-guidance/glossary .

National Cyber Security Centre (NCSC). (n.d.). *How to spot and report scams*. https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams .

National Institute of Standards and Technology (NIST). (n.d.-a). *Malware*. U.S. Department of Commerce. https://csrc.nist.gov/glossary/term/malware .

National Institute of Standards and Technology (NIST). (n.d.-b). *Trojan horse*. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/trojan_horse.

National Institute of Standards and Technology (NIST). (n.d.-c). *Virus*. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/virus .

National Institute of Standards and Technology (NIST). (n.d.-e). *Phishing*. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/phishing .
National Institute of Standards and Technology (NIST). (n.d.-f). *Spear phishing*. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/spear_phishing .
National Institute of Standards and Technology. NIST (2025). *Cybersecurity framework (CSF)*. Computer Security Resource Center (CSRC). U.S. Department of Commerce. https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters
National Portal (2025). *Digital government strategy*. https://my.gov.sa/en/content/digital-strategy#section-3
Nead, K. T., Wehner, M. R., and & Mitra, N. (2018). The use of "trend" statements to describe statistically nonsignificant results in the oncology literature. *JAMA Oncology*, *4*(12), 1778–1779. https://doi.org.10.1001/jamaoncol.2018.4524
Netemeyer, R. G., Bearden, W. O., & Sharma, S. (2003). *Scaling procedures: Issues and applications*. Sage.
Nthala, N., & Wash, R. (2021). *How non-experts try to detect phishing scam emails*. https://msucas-paid.sona-systems.com
O'Connor, P. (2022, September 25). *The biggest cyber attacks of 2022*. BCS. https://www.bcs.org/articles-opinion-and-research/the-biggest-cyber-attacks-of-2022/
Ofcom. (2023). *Online fraud and scams: Research summary report.* https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/online-fraud-and-scams/online-scams-and-fraud-research-summary-report?v=329362
Office for National Statistics. (2021, April 6). *Internet users, UK: 2020*. https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2020
Office of Communication (Ofcom). (2023). *Adults' media use and attitudes report 2023*.
Office of Communications, Ofcom (2025, March 1). *Connected Nations update: Spring 2025.* Ofcom. https://www.ofcom.org.uk/phones-and-broadband/coverage-and-speeds/connected-nations-update-spring-2025
Onyewuchi Ofoegbu, K. D., Osundare, O. S., Somadina Ike, C., Fakeyede, O. G., & Bolatito Ige, A. (2024). Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols. *Computer Science & IT Research Journal*, *5*(8), 2083–2106. https://doi.org/10.51594/csitrj.v5i8.1493
Parsons, K., Butavicius, M., Pattinson, M., Mccormac, A., Calic, D., & Jerram, C. (2015). *Do users focus on the correct cues to differentiate between phishing and genuine emails?*
Parsons, K., Mccormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2013). *The development of the human aspects of information security questionnaire (HAIS-Q)*. https://aisel.aisnet.org/acis2013/31
Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003
Pascual, A., Marchini, K., & Miller, S. (2018). *2018 identity fraud: Fraud enters a new era of complexity*. Javelin Strategy & Research. https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity
Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: A comparison of two studies. *Information and Computer Security*, *24*(2), 228–240. https://doi.org/10.1108/ICS-01-2016-0009
Pattnaik, N., Li, S., & Nurse, J. R. C. (2023). *A survey of user perspectives on security and privacy in a home networking environment*. *ACM Computing Surveys, 55*(9), Article 180. https://doi.org/10.1145/3558095

Peng, P., Xu, C., Quinn, L., Hu, H., Viswanath, B., & Wang, G. (2019). What happens after you leak your password: Understanding credential sharing on phishing sites. *AsiaCCS 2019 - Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 181–192. https://doi.org/10.1145/3321705.3329818

Petrie, H., & Merdenyan, B. (2016). Cultural and gender differences in password behaviors: Evidence from China, Turkey and the UK. *ACM International Conference Proceeding Series*, *23-27-October-2016*. https://doi.org/10.1145/2971485.2971563

Petrosyan, A. (2025, August 29). *Annual cost of cybercrime worldwide 2018-2029*. Statista. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide?srsltid=AfmBOoo36muRt3hJ-oFx3hUK30MRer0RggvaBLRQeKipLXv2v-1PYHAJ

Pfleeger, C., Pfleeger, S., & Margulies, J. (2015). *Security in computing* (5th ed.). Pearson.

Prensky, M. (2001). Digital Nativesnatives, Digital digital Immigrants immigrants Part 1. *On the Horizon*, *9*(5), 1–6. https://doi.org/10.1108/10748120110424816

Rabitti, G., Khorrami Chokami, A., Coyle, P., & Cohen, R. D. (2024). A taxonomy of cyber risk taxonomies. *Risk Analysis*. https://doi.org/10.1111/risa.16629

Rader, E., Wash, R., & Brooks, B. (2012). *Stories as informal lessons about security*. http://www.engineeringchallenges.org/cms/8996/9042.aspx

Rahman-Jones, I. (2025, September 24). *Man arrested in connection with cyber-attack on airports*. https://www.bbc.com/news/articles/c62ldxyj431o

Rajivan, P., Aharonov-Majar, E., & Gonzalez, C. (2020). Update now or later? Effects of experience, cost, and risk preference on update decisions. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/CYBSEC/TYAA002

Rashed Albediwi, M., & Sadaf, K. (2023). A framework for cybersecurity awareness in Saudi Arabia. *Journal of Engineering and Applied Sciences*, *10* (1).

Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing cyber security governance and policy for SMEs in industry 5.0: A comparative study between Saudi Arabia and the United Kingdom. *Digital*, *3*(3), 200–231. https://doi.org/10.3390/digital3030014

Rhee, H. S., Ryu, Y. U., & Kim, C. T. (2012). Unrealistic optimism on information security management. *Computers and Security*, *31*(2), 221–232. https://doi.org/10.1016/j.cose.2011.12.001

Rhee, H.-S., Ryu, Y., & Tag Kim, C. (2005). *I am fine but you are not: Optimistic bias and illusion of control on information security*. http://aisel.aisnet.org/icis2005

Rocha Flores, W., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security*, *22*(4), 393–406. https://doi.org/10.1108/imcs-11-2013-0083

Rogers, J. (2017). Nothing to lose: Charitable donations as incentives in risk preference measurement. *Journal of Experimental Political Science*, *4*(1), 34–56. https://doi.org/10.1017/XPS.2017.4

Russon, B. M. (2021, May 10). *US fuel pipeline hackers "didn't mean to create problems."* https://www.bbc.com/news/business-57050690

Sakikawa, T. (2024). The connections between national and organizational cultures: Evidence from the UK, the US, Saudi Arabia, and Japan. *Journal of Global Management 3* (3), 67–86.

Samarasinghe, N., & Mannan, M. (2021). On cloaking behaviors of malicious websites. *Computers and Security*, *101*. https://doi.org/10.1016/j.cose.2020.102114

Santos, P. R. da P. F., Resende, P. A. A., Gondim, J. J. C., & Drummond, A. C. (2025). Towards robust cyber attack taxonomies: A survey with requirements, structures, and assessment. *ACM Computing Surveys*, *57*(8), 1–36. https://doi.org/10.1145/3717606

Sarno, D. M., Harris, M. W., & Black, J. (2023). Which phish is captured in the net? Understanding phishing susceptibility and individual differences. *Applied Cognitive Psychology*, *37*(4), 789–803. https://doi.org/10.1002/acp.4075

Saudi General Authority for Statistics. (2023). *GASTAT: 83.83% of individuals (12 to 65 years) use internet, and 92% use cell phone*. (2023). https://www.stats.gov.sa/en/w/gastat-83.83-of-individuals-12-to-65-years-use-internet-and-92-use-cell-phonePetr

Sawaya, Y., Sharif, M., Christin, N., Kubota, A., Nakarai, A., & Yamada, A. (2017). Self-confidence trumps knowledge: A cross-cultural study of security behavior. *Conference on Human Factors in Computing Systems - Proceedings*, *2017-May*, 2202–2214. https://doi.org/10.1145/3025453.3025926

Shah, M. U., Iqbal, F., Rehman, U., & Hung, P. C. K. (2023). A comparative assessment of human factors in cybersecurity: Implications for cyber governance. *IEEE Access*, *11*, 87970–87984. https://doi.org/10.1109/ACCESS.2023.3296580

She, L., Ma, L., & Khoshnavay Fomani, F. (2021). The Consideration of Future Consequences Scale among Malaysian young adults: A psychometric evaluation. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/fpsyg.2021.770609

Shirey, R. (2007). *Internet Security Glossary, Version 2.* The IETF Trust. https://www.rfc-editor.org/rfc/rfc4949.html#section-1 .

Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N., & Diakopoulos, N. (2016). Grand challenges for HCI researchers. *Interactions*, *23*(5), 24-25.

Siegel, S., & N John Castellan. (2000). *Nonparametric statistics for the behavioral sciences*. McGraw-Hill.

Spero, E., & Biddle, R. (2020). Out of sight, out of mind: UI design and the inhibition of mental models of security. *ACM International Conference Proceeding Series*, 127–143. https://doi.org/10.1145/3442167.3442174

Steinberg, J. (2019). *Cybersecurity for dummies*. Wiley.

Steves, M., Greene, K., & Theofanos, M. (2020). Categorizing human phishing difficulty: A Phish Scale. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/CYBSEC/TYAA009

Stouffer, C. (2022). *Website spoofing: A definition + how spoofing works | Norton*. Usus.norton.com. https://us.norton.com/blog/malware/website-spoofing

Strathman, A., Gleicher, F., Boninger, D. S., & Edwards, C. S. (1994). The Consideration of Future Consequences: Weighing immediate and distant outcomes of behavior. *Journal of Personality and Social Psychology*, *66*(742).

The Guardian. (2017) Uber concealed massive hack that exposed data of 57m users and drivers. https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

The New York Times. (2018). A cyberattack in Saudi Arabia had a deadly goal. Experts fear another try. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

Turner, S., Nurse, J. R. C., & Li, S. (2022, April 27). "It was hard to find the words": Using an autoethnographic diary study to understand the difficulties of smart home cyber security practices. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3491101.3503577

van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283–297. https://doi.org/10.1016/j.chb.2017.10.007

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559. https://doi.org/10.1016/j.chb.2017.05.038

Varnum, M. E. W., & Grossmann, I. (2017). Cultural change: The how and the why. *Perspectives on Psychological Science*, *12*(6), 956–972. https://doi.org/10.1177/1745691617699971

Vashistha, A., Anderson, R., & Mare, S. (2018, June 20). Examining security and privacy research in developing regions. *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies, COMPASS 2018*. https://doi.org/10.1145/3209811.3209818

Verdict Encrypt (n.d.) *The biggest cybersecurity attacks of 2018: An interactive map*. https://verdict--encrypt.nridigital.com/verdict_encrypt_winter18/the_biggest_cybersecurity_attacks_of_2018_interactive_map

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, *45*(8), 1146–1166. https://doi.org/10.1177/0093650215627483

Wani, M. M., & Wani, J. I. (2020). Is digital or internet addiction a reality: Study from King Khalid University Saudi Arabia. *International Journal of Community Medicine and Public Health*, *7*(5), 1645. https://doi.org/10.18203/2394-6040.ijcmph20201961

Wash, R. (2020). How experts detect phishing scam emails. *Proceedings of the ACM on Human-Computer Interaction*, *4*(CSCW2). https://doi.org/10.1145/3415231

Weber, E. U., Blais, A. R., & Betz, N. E. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making*, *15*(4), 263–290. https://doi.org/10.1002/bdm.414

White, G., Ekin, T., & Visinescu, L. (2017). *Analysis of protective behavior and security incidents for home computers*. https://doi.org/10.1080/08874417.2016.1232991

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3–7. https://doi.org/10.1089/cyber.2014.0179

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412–421. https://doi.org/10.1016/j.chb.2017.03.002

Wisniewski, P., Xu, H., Rosson, M. B., Perkins, D. F., & Carroll, J. M. (2016). Dear diary: Teens reflect on their weekly online risk experiences. *Conference on Human Factors in Computing Systems - Proceedings*, 3919–3930. https://doi.org/10.1145/2858036.2858317

Wu, M. J., Zhao, K., & Fils-Aime, F. (2022). Response rates of online surveys in published research: A meta-analysis. *Computers in Human Behavior Reports*, *7*, 100206. https://doi.org/10.1016/j.chbr.2022.100206

Wu, T., Zhang, R., Ma, W., Wen, S., Paris CecileParis, C., Data, csiroau, Xiang, Y., Xia, X., Paris, C., & Nepal, S. (2020). *What risk? I don't understand. An empirical study on users' understanding of the terms used in security texts*. 15. https://doi.org/10.1145/3320269.3384761

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). *Phishing, sMiShing & vishing: An assessment of threats against mobile devices*. *5*(4). http://www.cisjournal.org

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Appendix A: Attention Check Questions (AC) and Analysis

Attention check (AC) questions were derived from the ISA and SeBIS scales. Each set includes two sentences that convey the same meaning but are phrased differently, one in a positive context and the other in a negative context. If the participants gave a positive rating to one statement, they should have assigned the corresponding negative rating to the other statement of the same set. For instance, if the rating for the first statement in (AC1) is 1, the rating for the other statement should be 7.

Attention Check Pair 1(AC1)

SeBIS1_4 and SeBIS2_10
Attention Check Pair 2 (AC2)
SeBIS1_10 and SeBIS2_3
Attention Check Pair 3 (AC3)
SeBIS4_1 and SeBIS3_10
Attention Check Pair 4 (AC4)
SeBIS3_7 and SeBIS4_10
Analysis of ACs questions
Perfect swapping (Pairing Assessments)
For the four sets of attention check questions, if a participant gave a rating on one statement he/she gave the appropriate opposite rating for the other statement in the same set. For example, if the rating on the first statement was 1, then the rating for the other statement should be 7. The only exception is that if the rating is 4 on one statement, it should be 4 on the other statement. The check that I followed in the AC question assessment is illustrated in table 3.5.

Table 3.5: Perfect swap process

1	2	3	4	5	6	7
1	2	3	4	5	6	7
1	2	3	4	5	6	7
1	2	3	4	5	6	7

Then by scoring each pair and adding the scores up. Table 3.6 shows the results. Just under half of the participants get two or less attention checks wrong, while over half get more than half the attention checks wrong.

Table 3.6: Results of perfect swapping

Status	Number of participants	% of participants	Cumulative %
All 4 swapped perfectly	3	1.4	1.4
1 wrong	39	18.7	20.1
2 wrong	62	29.7	49.8
3 wrong	73	34.9	84.7
4 wrong	32	15.3	100.0

There were also big differences in the pairs, see Table 3.7.

Table 3.7: Failure rate for the different attention check pairs (perfect swapping)

Attention check pair	% of participants who failed the perfect swap
AC1	78.0
AC2	65.1
AC3	50.2
AC4	50.7

Perhaps the previous assessment approach was strict on the participants. It's easy to say never or always, but if you are somewhere in the middle, you might not do a perfect swap. So, I re-scored using a more flexible scoring which were allowed swap and perfect swap. Apart from the endpoints, participants could rate on either side of the rating. For example, if participants selected 4 on one statement they could select 3 or 5 (+/-1) for the other statement. For the endpoints, if participants chose a rating of 1 for one statement, they could select a rating of 6 or 7 for the other statement. The new assessment using allowed and perfect swaps is shown in Table 3.8.

Table 3.8: More flexible swap process (Perfect +/- 1) (first statement rating in yellow, allowed swaps in green, and with an asterisk, two asterisks for the perfect swap)

1	2	3	4	5	6*	7**
1	2	3	4	5*	6**	7*
1	2	3	4*	5**	6*	7
1	2	3*	4**	5*	6	7
1	2*	3**	4*	5	6	7
1*	2**	3*	4	5	6	7
1**	2*	3	4	5	6	7

And now the scores are shown in Table 3.9.

Table 3.9: Results of Perfect +/- 1 swapping

Status	Number of participants	% of participants	Cumulative %
All 4 swapped OK	45	21.5	21.5
1 wrong	89	42.6	64.1
2 wrong	58	27.8	91.9
3 wrong	14	6.7	98.6
4 wrong	3	1.4	100.0

Table 3.10: Failure rate for the different attention check pairs (Perfect +/- 1 swapping)

Attention check pair	% of participants who failed the +/- 1 swap
AC1	49.8
AC2	30.1
AC3	18.2
AC4	25.8

The first pair (AC1) has a very high fail rate. That may be because SeBIS2_10 has two negatives in it, so it is quite hard to understand. So, this set of AC was removed. So, from the remaining three AC (2,3,4) sets, those who answered two sets correctly were included in the study. After removing those who failed, 81 responses were valid for analysis.

Appendix B: Original and modified SeBIS Scale

	Original text	**Proposed text – to standardized the style of statement and correct grammatical mistakes, bring questions up to date**	**Number of words**
1	I set my computer screen to automatically lock if I don't use it for a prolonged period of time. (SeBIS) (Not just computers, all devices)	I set my device screen to automatically lock if I do not use it for a prolonged period of time	19
2	I use a password/passcode to unlock my laptop or tablet. (SeBIS) (not just laptop or tablet, all devices)	I use passwords/passcodes to lock my devices	8
3	manually lock my computer screen when I step away from it. (SeBIS) (not just computers, all devices)	I manually lock my device screen when I step away from it	12
4	I do not change my passwords, unless I have to. (SeBIS) (incorrect grammar)	I do not change my passwords unless I have to	10
5	I use different passwords for different accounts that I have (SeBIS) (poor wording)	I use different passwords for my different online accounts	9
6	When I create a new online account, I try to use a password that goes beyond the site's minimum requirements. (SeBIS) [need to change because we are not only referring to accounts on websites any more. Also you create new passwords not only for new accounts, but when you are asked to renew your password, so this seems very dated]	When I create a new password, I try to create one that goes beyond the minimum requirements stated	18
7	I do not include special	I do not include special characters in	14

	characters in my password if it's not required. (SeBIS) Poor to use contractions in formal written language	my password if it is not required	
8	When someone sends me a link, I open it without first verifying where it goes (SeBIS)	When someone sends me a link, I open it without first verifying where it goes	15
9	I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar. (SeBIS) ["URL bar" is very old fashioned]	I know what website I am visiting based on its look and feel, rather than by looking at the address bar	21
10	I submit information to websites without first verifying that it will be sent securely (e.g. SSL, "https://", a lock icon)	I submit information to websites without first verifying that it will be sent securely (e.g. by the indication of SSL, https://, or a lock icon)	25
11	When browsing websites, I mouseover links to see where they go, before clicking them. (SeBIS)	When browsing websites, I mouseover links to see where they go before clicking them	14
12	If I discover a security problem, I continue what I was doing because I assume someone else will fix it. (SeBIS)	If I discover a security problem, I continue what I was doing because I assume someone else will fix it.	20
13	When I'm prompted about a software update, I install it right away (SeBIS) "right away" very American	When I am prompted about a software update, I install it straight away	13
14	I try to make sure that the programs I use are up-to-date [bringing it uptodate with apps]	I try to make sure that the programs and apps I use are uptodate	14
15	I verify that my anti-virus software has been regularly updating itself (SeBIS) (poor wording)	I verify that my anti-virus software is regularly updated	9

Appendix C: Full The full wording of the Scenarios Questionnaire, Study 1, and 2

Scenarios Intro: In the following questions, you will be asked about some common online security incidents that you may have encountered. These will be presented as short scenarios, there are 12 in all. For each one, if you have encountered something like it (it does not have to be exactly the same), you will be asked a short series of questions.

When the scenarios and questions refer to “device” it means your computer (desktop, laptop, tablet) or phone (mobile or smartphone), i.e. any device that you use to access the internet.

The main questions in each scenario use a seven-point scale for you to rate how frequently something like this has happened. You will find that the two ends of the scale are identified by a label such as "never" and "many times" - so the points between these two ends can be considered as gradual steps between "never" and "many times" for you to choose.

S1a: I click on a link (e.g. on a website, in social media, in a SMS) and then notice my device acting strangely (e.g. the device freezes, runs slowly or crashes repeatedly). I realise this may have been caused by clicking on the link.
Has something like this ever happened to you?

- Never (1)
- (2)
- (3)
- (4)
- (5)
- (6)
- Many times (7)

S1b
For this scenario:I click on a link (e.g. on a website, in social media, in a SMS) and then notice my device acting strangely (e.g. the device froze, ran slowly or crashed repeatedly), and realise this may have been caused by clicking on the link.
Think of a recent or memorable time when something like this happened …

What were the consequences for your device? (select all that apply)

- The screen froze (1)
- The device ran very slowly (2)
- The device crashed repeatedly (3)
- Other, you can explain in a later question (4)
- I can't remember/I'm not sure (5)

S1c Which kind of device did this happen on?

- Desktop (1)
- Laptop (2)
- Tablet (3)
- Phone (4)
- I can't remember/I'm not sure (5)

S1d Where was the link you clicked on?

- On a website (1)
- In an app (2)
- On a social media site (e.g. What's up, Twitter...etc.) (3)
- In a SMS (4)
- Other, please explain in the next question (5)
- I can't remember/I'm not sure (6)

S1e Please briefly explain the memorable/recent incident in your own words, e.g. what did you click on, where did the link come from, how did you realize something was wrong, what happened to your device, how did you try to solve the problem?

_____

S2a : I download an attachment (e.g. from an email or website) and then notice my device acting strangely (e.g. device freezes, runs slowly or crashes repeatedly). I realise this may have been caused by downloading the attachment.
Has something like this ever happened to you?

Never (1)
(2)
(3)
(4)
(5)
(6)
Many times (7)

S2b
For this scenario:I download an attachment (e.g. from an email or website) and then notice my device acting strangely (e.g. device freezes, runs slowly or crashes repeatedly). I realise this may have been caused by downloading the attachment.

Think of a recent or memorable time when something like this happened …
What were the consequences for your device? (select all that apply)

The screen frozen (1)
The device ran very slowly (2)
The device crashed repeatedly (3)
Other, you can explain in a later question (4)
I can't remember/I'm not sure (5)

S2c Which kind of device did this happen on?

Desktop (1)
Laptop (2)
Tablet (3)
Phone (4)
I can't remember/I'm not sure (5)

S2d Where was the attachment?

On a website (1)
in an app (2)
On a social media site (e.g. What's up, Twitter...etc.) (3)
In a SMS (4)
Other, please explain in the next question (5)
I can't remember/I'm not sure (6)

S2e Please briefly explain the recent/memorable incident in your own words, e.g. where did the attachment come from, how did you realize something was wrong, what happened to your device, how did you try to solve the problem?

_____

S3a : I download a free app or game from an unknown or possibly untrustworthy source. Then I notice that my device is running slowly or crashing more frequently than normal.

Has something like this ever happened to you?

Never (1)
(2)
(3)
(4)
(5)
(6)
Many times (7)

S3b
For this scenario: I download a free app or game from an unknown or possibly untrustworthy source. Then I notice that my device is running slowly or crashing more frequently than normal.

Think of a recent or memorable time when something like this happened ...
What were the consequences for your device? (Select all that apply)
The screen froze (1)
The device ran very slowly (2)
The device crashed repeatedly (3)
Other, you can explain in a later question (4)
I can't remember/I'm not sure (5)

S3c Which kind of device did this happen on?
Desktop (1)
Laptop (2)
Tablet (3)
Phone (4)
I can't remember/I'm not sure (5)

S3d Where was the downloaded app or game from?
On a website (1)
In an app (2)
On a social media site (e.g. What's up, Twitter...etc.) (3)
In a SMS (4)
Other, please explain in the next question (5)
I can't remember/I'm not sure (6)

S3e Please briefly explain the recent/memorable incident in your own words, e.g. where did the app/game come from, how did you realize something was wrong, what happened to your device, how did you try to solve the problem?

_____

S4a : I install some software or a file on my device from a link or attachment I received in an email, then notice the device acting strangely. I can't access some or all of my files and then I am asked to pay a ransom to be able to retrieve these files. I realise this may have been caused by installing that software/file.
Has something like this ever happened to you?

Never (1)
(2)
(3)
(4)
(5)
(6)
Many times (7)

S4b
For this scenario: I install some software or a file on my device from a link or attachment I received in an email, then notice the device acting strangely. I can't access some or all of my files and then I am asked to pay a ransom to be able to retrieve these files, this may have been caused by installing that software/file.

Think of a recent or memorable time when something like this happened …
What were the consequences ? (Select all that apply)

I could not access any of my files (1)
I could not access some of my files (2)
I paid the requested ransom (5)
Other, you can explain in a later question (3)
I can't remember/I'm not sure (4)

S4c Which kind of device did this happen on?

Desktop (1)
Laptop (2)
Tablet (3)
Phone (4)
I can't remember/I'm not sure (5)

S4d Where was the software/file from?

On a website (1)
In an app (2)
On social media site (e.g. What's up, Twitter...etc.) (3)
In a SMS (4)
Other, please explain in the next question (5)
I can't remember/I'm not sure (6)

S4e Please briefly explain the recent/memorable incident in your own words, e.g. what was the software or file you installed, where did it come from, how did you realize something was wrong, what happened to your device, how did you try to solve the problem?

_____

S5a: I realise that someone has made a purchase using my credit card or bank account details. I remember that I have recently entered these details online and they may have been stolen.

Has something like this ever happened to you?
- Never (1)
- (2)
- (3)
- (4)
- (5)
- (6)
- Many times (7)

S5b For this scenario: I realise that someone has made a purchase using my credit card or bank account details. I remember that I have recently entered these details online and they may have been stolen.

Think of a recent or memorable time when something like this happened …
What were the consequences? (Select all that apply)
- I lost money (1)
- My credit card could not be used (2)
- My bank account became overdrawn (3)
- Other, you can explain in a later question (4)
- I can't remember/I'm not sure (5)

S5c Which kind of device did this happen on?
- Desktop (1)
- Laptop (2)
- Tablet (3)
- Phone (4)
- I can't remember/I'm not sure (5)

S5d Where did you enter your credit card or bank account details?
- On a website (1)
- In an app (2)
- On a social media site (e.g. What's up, Twitter...etc.) (3)
- In a SMS (4)
- Other, please explain in the next question (5)
- I can't remember/I'm not sure (6)

S5e Please briefly explain the recent/memorable incident in your own words, e.g. where did you enter your credit card/bank account details, why were you doing that, how did you realise something was wrong, what were the consequences, how did you try to solve the problem?

_____

S6a: I realise that someone has used my personal information or something I have stored online (e.g. personal name, a photo). I remember that I have that stored online and it may have been stolen. Has something like this ever happened to you?

Never (1)
(2)
(3)
(4)
(5)
(6)
Many times (7)

S6b

For this scenario: I realise that someone has used my personal information or something I have stored online (e.g. your name, a photo). I remember that I have that stored online and it may have been stolen.

Think of a recent or memorable time when something like this happened …

What were the consequences? (Select all that apply)

Someone blackmailed me (1)
Someone stole my identity (2)
I received annoying SMS or calls (3)
Other, you can explain in a later question (4)
I can't remember/I'm not sure (5)

S6c Which kind of device did this happen on?

Desktop (1)
Laptop (2)
Tablet (3)
Phone (4)
I can't remember/I'm not sure (5)

S6d Where did you store this personal information or data?

On a website (1)
In an app (2)
On a social media site (e.g. What's up, Twitter...etc.) (3)
Other, please explain in the next question (4)
I can't remember/I'm not sure (5)

S6e Please briefly explain the recent/memorable incident in your own words, e.g. what kind of information or data was it (you do not have to be very specific, just the type), where did you store it, how did you realise something was wrong, what were the consequences, how did you try to solve the problem?

_____

_____

S7a
I download some anti-virus/malware software to try to protect my device. But the software does not seem to be effective and it keeps showing me advertisements on the device.
Has something like this ever happened to you?

Never (1)
(2)
(3)
(4)
(5)
(6)
Many times (7)

S7b For this scenario: I download some anti-virus/malware software to try to protect my device. But it does not seem to be effective and it keeps showing me advertisements on the device.

Think of a recent or memorable time when something like this happened …
What were the consequences? (Select all that apply)Strange popups appeared (1)
The device ran very slowly (2)
The device/programs crashed repeatedly (3)
The browser homepage changed (4)
Other, you can explain in a later question (5)
I can't remember/I'm not sure (6)

S7c Which kind of device did this happen on?
Desktop (1)
Laptop (2)
Tablet (3)
Phone (4)
I can't remember/I'm not sure (5)

S7d Where did you find out about this anti-virus/malware software?
On a website (1)
In an app (2)
On a social media site (e.g. What's up, Twitter...etc.) (3)
Other, please explain in the next question (4)
I can't remember/I'm not sure (5)

S7e Please briefly explain the recent/memorable incident in your own words, e.g. why you decided to install anti-virus/malware software, where you downloaded it from, how did you realise something was wrong, what were the consequences, how did you try to solve the problem?

_____

S8a
I click on a link (e.g. on a website, in social media, in a SMS) and then notice strange things happening on my device (e.g. pop-ups appearing frequently, unrecognised apps being installed). I realise this may have been caused by clicking on the link.

Has something like this ever happened to you?

Never (1)
(2)
(3)
(4)
(5)
(6)
Many times (7)

S8b
For this scenario: I click on a link (e.g. on a website, in social media, in a SMS) and then notice strange things happening on my device (e.g. pop-ups appearing frequently, unrecognized apps being installed). I realise this may have been caused by clicking on the link.

Think of a recent or memorable time when something like this happened …
What were the consequences? (Select all that apply)
Strange popups appeared (1)
Unknown software/apps installed (2)
Mass emails were sent from my email address (5)
Other, you can explain in a later question (3)
I can't remember/I'm not sure (4)

S8c Which kind of device did this happen on?
Desktop (1)
Laptop (2)
Tablet (3)
Phone (4)
I can't remember/I'm not sure (5)

S8d Where was the link you clicked on it?
On a website (1)
In an app (2)
On a social media site (e.g. What's up, Twitter...etc.) (3)
In a SMS (4)
Other, please explain in the next question (5)
I can't remember/I'm not sure (6)

S8e Please briefly explain the recent/memorable incident in your own words, e.g. what did you click on, where did the link come from, how did you realise something was wrong, what happened to your device, how did you try to solve the problem?

_____

_____

S9a
My friends report receiving strange messages from me (e.g. requesting money because I am in trouble, including suspicious links). I realise someone must have illegally used one of my accounts.

Has something like this ever happened to you?

Never (1)
(2)
(3)
(4)
(5)
(6)
Many times (7)

S9b
For this scenario: My friends report receiving strange messages from me (e.g. requesting money because I am in trouble, including suspicious links). I realize someone must have illegally used one of my accounts.

Think of a recent or memorable time when something like this happened …
What were the consequences? (Select all that apply)

My friends were upset with me (1)
Many of my contacts received the same message (2)
Someone responded before verifying whether it was me (3)
Other, you can explain in a later question (4)
I can't remember / I'm not sure (5)

S9c: Which kind of account were these messages sent from?
Email account (1)
Social media message system (e.g. What's up, Twitter...etc.) (2)
Online account on a site (3)
Online account for an app (6)
Other, you can explain in a later question (4)
I can't remember/I'm not sure (5)

S9d Please briefly explain the recent/memorable incident in your own words, e.g. which account do you think was used illegally, how was that done, how did you realize something was wrong, what happened, how did you try to solve the problem?

_____

_____

S10a I receive a message or call from what seems to be a trustworthy source (e.g. via email, social media, SMS or phone call) asking me for personal information (e.g. account details, password) for a legitimate reason (e.g. updating data). At some point I realise this is a fake message or call.

Has something like this ever happened to you?

Never (1)
(2)
(4)
(5)
(6)
(7)
Many times (8)

S10b
For this scenario: I receive a message or call from what seems to be a trustworthy source (e.g. via email, social media, SMS or phone call) asking me for personal information (e.g. account details, password) for a legitimate reason (e.g. updating data). At some point I realise this is a fake message or call.

Think of a recent or memorable time when something like this happened …
Where did this message come from?

Email (1)
Phone call (3)
SMS (7)
Social media message system (e.g. What's up, Twitter...etc.) (2)
Other, you can explain in a later question (6)
I can't remember/I'm not sure (5)

S10c

What were the consequences? (Select all that apply)

I responded and entered my personal data (1)
I could not access some of my online accounts (2)
My personal information was used illegally (3)
Malicious software was downloaded to my device (4)
Other, you can explain in the next question (5)
I can't remember/I'm not sure (6)

S10d Please briefly explain the recent/memorable incident in your own words, e.g. what communication did you receive, where did it come from, how did you realize something was wrong, what happened to your device, how did you try to solve the problem?

_____

S11a
I receive a message which seems to be from someone I know (e.g. via email, social media, SMS) asking me to give them urgent assistance (e.g. transfer money). At some point I realise this is a fake message.
Has something like this ever happened to you?

- Never (1)
- (2)
- (3)
- (4)
- (5)
- (6)
- Many times (7)

S11b For this scenario: I receive a message which seems to be from someone I know (e.g. via email, social media, SMS) asking me to give them urgent assistance (e.g. transfer money). At some point I realise this is a fake message.

Think of a recent or memorable time when this happened ...
Which account did this message come from?

- Email (1)
- SMS (2)
- Social media message system (e.g. What's up, Twitter etc.) (3)
- I can't remember/I'm not sure (5)
- Other, please explain in a later question (6)

S11c
What were the consequences? (Select all that apply)

- I sent money to the fraudulent person (1)
- I responded to the request but did not give the assistance asked for (2)
- Other, you can explain in the next question (3)
- I can't remember/I'm not sure (4)

S11d Please briefly explain the recent/memorable incident in your own words, e.g. what did you receive, where did the message come from, how did you realize something was wrong, what happened to your device, how did you try to solve the problem?

_____

_____

S12a I need to undertake an urgent task on the government website (e.g. renewing my passport or driving license). I search quickly for the website in Google. The website asks for personal information (e.g. my name, date of birth and credit card details). After entering my personal information and making a payment, I realise it was not the actual government website, but a fraudulent one with a very similar address and information

Has something like this ever happened to you?

Never (1)
(2)
(3)
(4)
(5)
(6)
Many times (7)

S12b
For this scenario: I need to undertake an urgent task on the government website (e.g. renewing my passport or driving license). I search quickly for the website in Google. The website asks for personal information (e.g. my name, date of birth and credit card details). After entering my personal information and making a payment, I realise it was not the actual government website, but a fraudulent one with a very similar address and information

Think of a recent or memorable time when something like this happened ...
What were the consequences? (Select all that apply)

I lost money (1)
I handed over my personal data to the fraudulent website (2)
I handed over my credit card number to the fraudulent website (3)
My device was infected with malicious software (4)
Other, you can explain in a later question (6)

S12c Which kind of device did this happen on?

Desktop (1)
Laptop (2)
Tablet (3)
Phone (4)
I can't remember / I'm not sure (5)

S12d Please briefly explain the recent/memorable incident in your own words, e.g. how did you find the fraudulent website, how did you realize something was wrong, what happened to your device, how did you try to solve the problem?

G3 How worried or not are you that your device could be targeted with one of the following security threats
Each sentence contains a seven-point scale for determining how worried you are that something like this will happen. You will find the two endpoints of the scale are defined by a label - "not worried at ll" and "very worried" - so the points between these two ends are gradations between not worried at all and very worried

	Not worried at all (1)	(2)	(3)	(4)	(5)	(6)	Very worried (7)
Someone will steal my device which has my personal data (e.g. images) (1)							
My device will be accessed by an attacker and my data will be destroyed (2)							
I will receive an email with a link leading to a fake website (3)							
I will receive an email with an attachment that may include malicious code (4)							
Someone will lock me out of my device(s) and demand money to restore access (5)							
Someone will access my device(s) or account(s), look at my information and use it to blackmail me (6)							
Someone will steal my online identity and misuse it (7)							
Someone will access my device(s) or account(s), steal my data and use it for malicious purposes or to their advantage (e.g. make illegal purchases) (8)							
I will receive a phone call from someone asking about my confidential data (e.g. password, bank account details) (9)							
I will click on a link in a SMS message or email from a source that I can not verify its origin, whether it is trustworthy (10)							

ISA&SeBIS1 How often do you take the following actions in relation to your devices?

If any of the actions are not applicable or you do not understand what is being referred to in any of the statements, please select Never.

	Never (1)	(2)	(3)	(4)	(5)	(6)	Always (7)
When someone sends me a link, I open it without first verifying where it goes (2) SeBis3-1	•	•	•	•	•	•	•
I set my device screen to automatically lock if I do not use it for a prolonged period of time (4) SeBIS1-1	•	•	•	•	•	•	•
I manually lock my device screen when I step away from it (6) SeBIS1-3	•	•	•	•	•	•	•
I verify that my anti-virus software is regularly updated (8) SeBIS4-3	•	•	•	•	•	•	•
I use embedded security systems (e.g. firewalls, encryption) (9)	•	•	•	•	•	•	•
I do not delete apps not in use on my device (10) AC1	•	•	•	•	•	•	•

ISA&SeBIS2 How often do you take the following actions in relation to your devices?

If any of the actions are not applicable or you do not understand what is being referred to in any of the statements, please select Never.

	Never (1)	(2)	(3)	(4)	(5)	(6)	Always (7)
I use passwords/passcodes to lock my devices (2)SeBIS1-2	•	•	•	•	•	•	•
I do not include special characters in my password if it is not required (4) SeBIS2-4	•	•	•	•	•	•	•
I do not set my device screen to automatically lock if I do not use it for a prolonged period of time (10) AC2	•	•	•	•	•	•	•
When I am prompted about a software update, I install it straight away (7) SeBIS4-1	•	•	•	•	•	•	•

Start of Block: ISA&SeBIS3

ISA&SeBIS3 How often do you take the following actions in relation to your devices?
If any of the actions are not applicable or you do not understand what is being referred to in any of the statements, please select Never

	Never (1)	(2)	(3)	(4)	(5)	(6)	Always (7)
I create passwords made up of different characters and numbers (1)	•	•	•	•	•	•	•
I try to make sure that the programs and apps I use are up to date (4)	•	•	•	•	•	•	•
I do not change my passwords unless I have to (6) SeBIS2-1	•	•	•	•	•	•	•
I know what website I am visiting based on its look and feel, rather than by looking at the address bar (8) SeBIS3-2	•	•	•	•	•	•	•
If I discover a security problem, I continue what I was doing because I assume someone else will fix it (9) SeBIS3-5	•	•	•	•	•	•	•
I use same password for my different online accounts (10) AC3	•	•	•	•	•	•	•

ISA&SeBIS4 How often do you take the following actions in relation to your devices?

	Never (1)	(2)	(3)	(4)	(5)	(6)	Always (7)
I use different passwords for	•	•	•	•	•	•	•

my different online accounts (1) SeBIS2-2							
When I create a new password, I try to create one that goes beyond the minimum requirements stated (4) SeBIS2-3	•	•	•	•	•	•	•
When browsing websites, I mouseover links to see where they go before clicking them (6) SeBIS3-4	•	•	•	•	•	•	•
I submit information to websites without first verifying that it will be sent securely (e.g. by the indication of SSL, https://, or a lock icon) (8) SeBIS3-3	•	•	•	•	•	•	•
I do not download files sent in emails if they are from unknown senders (10) AC4	•	•	•	•	•	•	•

Demographic Information

Q78 Finally, just for statistical purposes, please answer these questions about yourself

Q1 How old are you?

▼ 18 (1) ... 30 (13)

Q4 What is your highest educational level?

- Primary school (1)
- High school (2)
- Bachelors degree (3)
- Postgraduate (MA, MSc, PhD etc) (4)
- Professional qualification (5)
- Other, please specify (6) _____

Q5 How would you rate your general computer knowledge?

- Not at all knowledgeable (1)
- (2)
- (3)
- (4)
- (5)
- (6)
- Very knowledgeable (7)

Q6 How would you rate your online security knowledge?

- Not at all knowledgeable (1)
- (2)
- (3)
- (4)
- (5)
- (6)
- Very knowledgeable (7)

Q7 How confident are you in your ability to identify an attack from a cybercriminal (e.g. a malicious or illegitimate email, link or website)?

- Not at all confident (1)
- (2)
- (3)
- (4)
- (5)
- (6)
- Very confident (7)

Appendix D: List of Recommended Solutions Provided by Security Expert

Scenario No.	Suggested solutions by reputable security	Prioritized solutions	Comment

	companies		
Scenario 1 (Phishing through links on website, social media, or SMS)	According to Kaspersky and AV, these are some common steps to remove malware: **1-** Download Antivirus software and Scan the device **2-** Delete any infected files **3-** Restart the device **4-** Update applications and system (Hygiene) **5-** Backup important files **6-** Change the passwords (Hygiene)	**1-** Download Antivirus software and Scan the device **2-** Delete any infected files	Only one participant did the first right solution to remove malware, three restarted their devices which is one of the recommended solutions but not the first step in removing malware.
Scenario 2 (phishing through files attached in email, website)	According to NCSC in the UK: **1-** Scan your device using trusted antivirus **2-** Follow the advice of AV software (e.g. quarantine/delete the infected files) **3-** If you cannot have AV software (web browser is infected) get help from experts 4- Restore your backup (escalation)	**1-** Scan the device using a trusted antivirus **2-** Follow the advice of AV software (e.g. quarantine/delete the infected files)	some participants stated that they only removed/cleared the installed files – without mentioning scan or use of antivirus software only 1 participant (UK80) delete the files and use antivirus to scan the device.
Scenario 3 *Malicious Code* (in free app or game) *Denial of Service, Trojan Horse*	When the device had infected files with the trojan horse (come from free app/game) it can be used by attackers to commit cybercrimes (DOS attack) **1-** Use antivirus and scan the device **2-** Update all software **3-** Reset the system to factory	**1-** Use antivirus and scan the device **2-** Update all software	Most of the participants chose to uninstall the game or app as a solution, which is not the only recommended action in a similar case according to the experts' advice. one participant did not know what to do to solve the

	settings(escalation) **4-** Use a firewall (it is come as defual in most OS so no need to mention this as step here) **5-** Update passwords Hygiene		problem
Scenario 4 *Phishing* (attachment in email, website) *Ransomware*	According to Norton & Kaspersky: **1-** Do not pay the ransom **2-** Disconnect from the Internet **3-** Use Internet security software to scan your device **4-** Delete or quarantine infected files **5-** Find a ransomware decryption tool (difficult for general users) 6- Restore backup	**1-** Do not pay the ransom **2-** Disconnect from the Internet **3-** Use Internet security software to scan your device 4- Delete or quarantine infected files	In all reported cases, participants had not mentioned that they had been asked to pay a ransom. The only problem was they could not access some of the files on their devices. Even though the reported solutions were not similar to the ones provided by experts
Scenario 5 Info. Entered online (or in data leak) Exploitation: *Data Theft*, *Identity Theft*	According to Bitdefender: **1-** Contact the bank and cancel the cards **2-** Change passwords 3- Report the crime to the authority	**1-** Contact the bank and cancel the cards	10 participants reported that they did the right first step in this scenario. As they contacted the banks or service providers to report the illegal payment and block their cards. 2 participants did not write how they solved this problem.
Scenario 6 Info. Stored online Delivery: unknown Exploitation:	The most popular solution is to contact the platform/service provider to freeze the fraudulent account	The most popular solution is to contact the platform/service provider to freeze the fraudulent account	Most of the participants who answered this question did not write about how they solved this problem.

Data Theft, *Identity Theft*			
Scenario 7 Solution Delivery: *Malicious Code* (free app) Exploitation: *Adware*	Recognizing and Avoiding Spyware | CISA **1-** Run a full scan **2-** Use official software that is specifically designed to remove adware/spyware	• Run a full scan • Use official software that is specifically designed to remove adware/spyware	The recommendation given from the security experts about spyware/adware was to scan the device and installing anti-spyware/adware. None of the participants solved the problem according to experts' recommendations
Scenario 8 Solutions Delivery: *Phishing* (link on website, social media, SMS) Exploitation: *Malware*	According to Kaspersky and AV, these are some common steps to remove malware: **1-** Download Antivirus software and Scan the device **2-** Delete any infected files **3-** Restart the device **4-** Change the passwords **5-** Update applications and system 6- Backup important files	Download Antivirus software and Scan the device Delete any infected files	
Scenario 9 Solutions Delivery: *Spear Phishing* Exploitation: *Identity Theft*	one of the recommended actions to take is to 1- notify all your friends that someone impersonating you online and warn them not to respond to requests sent from your accounts. Google advises to follow these steps in case of account has been hacked: 3- Try to recover your account 4- Change your passwords	notify all your friends that someone impersonating you Try to recover your account	Most of the participants were almost aware of some corrective actions to take in case of identity theft, but I found that only 3 of them do more than one step to solve the problem (UK24, 17,60). Other participants stated that they only changed their

	5- Turn on 2FA 6- Remove any malicious software 7- Install a more secure web browser		password or closed the hacked account. According to what has been recommended by experts there is more than one step needs to be taken to mitigate this threat.
Scenario 10 Solutions Delivery: *Spear Phishing* (email, social media, SMS or phone call) Exploitation: *Data Theft, Identity Theft*	Norton recommendation: 1- Contact the real source (e.g. the bank) before responding to the request	Contact the real source (e.g. the bank) before responding to the request Block/closed/change number, email, profile , account Report phishing	Most of the participants were aware of this type of attack and reported that they ignore/block such calls and messages of this nature. Some participants responded and after entering/giving their data they recognised these requests could be fraudulent so they changed their passwords.
Scenario 11 Solutions Delivery: *Identity Theft* (of another person), *Spear Phishing* Exploitation: Theft	Contact the real person and verify the request	Contact the real person and verify the request Block, delete, Report	1 & 25 & 26,41 notify & block Scenarios 10 and 11 are the most frequent threats participants experienced. In scenario 11, there are no severe consequences for the participants. This can be because it is about impersonating someone participants know
Scenario 12 Solutions Delivery: *Spoofed Website* Exploitation:	Report the spoofed website Change the passwords Scan your device Contact service provider/bank	Report the spoofed website Change the passwords in case of user entered his/her personal data) Scan your device (in case	Only 2 participants reported that they encountered similar threats. And both close the website once they

Data Theft, Identity Theft		of you download any file from the spoofed website) Contact service provider/bank	recognised it was a fake one. The important notice in this type of attack (i.e. phishing scams) is that the most prominent solution by experts is to report the incident to the authority or service provider, but in all scenarios which asked about phishing scams there are only a few respondents who stated that they report the hacked account

Appendix E: SeBIS Principal Component Analysis

A principal component analysis (PCA) was used to determine if the data collected from the UK young adults sample supports the four-factor structure of SeBIS. Data from 207 participants (81 from the full questionnaire and 126 from the second round of data collection on Prolific) were used.
Using all 15 items and taking items with loadings over 0.5, 53.1% of the variance was explained. The four components are:
Component 1: Proactive awareness, similar to the original SeBIS but missing one item (SeBIS3_4: When browsing websites, I mouse over links to see where they go, before clicking them) which did not load onto any of the components.) (26.4% of the variance)

Item	Loading	Item wording
SeBIS3_2	.809	I know what website I am visiting based on its look and feel, rather than by looking at the address bar
SeBIS3_3	.702	I submit information to websites without first verifying that it will be sent securely (e.g. by the indication of SSL, https://, or a lock icon)
SeBIS3_5	.714	If I discover a security problem, I continue what I was doing because I assume someone else will fix it.
SeBIS3_1	.478	When someone sends me a link, I open it without first verifying where it goes

Component 2: Device securement (but missing one item from the original SeBIS, and one item from Updating (SeBIS4_1) strongly loaded onto this component (.807), but it should be dropped as it's not about this component and did not load onto the updating component) (10.0%)

Item	Loading	Item wording
SeBIS1_1	.668	I set my device screen to automatically lock if I do not use it for a prolonged period of time
SeBIS1_2	.638	I use passwords/passcodes to lock my devices
SeBIS1_3	.717	I manually lock my device screen when I step away from it

Component 3: Password generation (all the original SeBIS items included) (9.2%)

Item	Loading	Item wording
SeBIS2_1	-.541	I do not change my passwords unless I have to
SeBIS2_2	-.853	I use different passwords for my different online accounts
SeBIS2_3	-.695	When I create a new password, I try to create one that goes beyond the minimum requirements stated
SeBIS2_4	-.616	I do not include special characters in my password if it is not required

Component 4: Updating (only 2 of the three items from the original SeBIS) (8.1%)

Item	Loading	Item wording
SeBIS4_2	-.670	I try to make sure that the programs and apps I use are up-to-date
SeBIS4_3	-.774	I verify that my anti-virus software is regularly updated

Appendix F: Original and Modified DOSPERT scale

Note. E = Ethical, F = Financial, H/S = Health/Safety, R = Recreational, and S = Social.

Original Statement	Modified version	Comment
1. Admitting that your tastes are different from those of a friend. (S)	1. Admitting that your opinions are different from those of a friend. (S)	
2. Going camping in the wilderness. (R)	2. Going camping in the wilderness. (R)	
3. Betting a day's income at the horse races. (F)	~~3. Betting a day's income at the horse races. (F)~~	Deleted from UK & KSA participants
4. Investing 10% of your annual income in a moderate growth mutual fund. (F)	4. Investing 10% of your annual income / saving in moderate growth tech company	
5. Drinking heavily at a social function. (H/S)	5. Drinking heavily at a social function. (H/S) (UK) 5. Taking medicine that might affect your behaviour before a social event (KSA)	
6. Taking some questionable deductions on your income tax return. (E)	6. Making questionable claims on expenses to your employer or for a university project" (E)	Is it referring to asking for money more than what the actual expenses are? Yes, it is. "questionable" means they might not be valid or correct If yes, same statement can be used for KSA
7. Disagreeing with an authority figure on a major issue. (S)	7. Disagreeing with an authority figure on a major issue. (S)	
8. Betting a day's income at a high-stake poker game. (F)	~~8. Betting a day's income at a high-stake poker game. (F)~~	Deleted for both UK & KSA
9. Having an affair with a married man/woman. (E)	~~9. Having an affair with a married man/woman. (E)~~	Deleted for both UK and KSA
10. Passing off somebody else's work as your own. (E)	10. Passing off somebody else's work as your own. (E)	
11. Going down a ski run that is beyond your ability. (R)	11. Going down a ski run that is beyond your ability. (R) (UK) 11. Doing an activity like sandboarding that is beyond your ability. (KSA)	
12. Investing 5% of your	12. Investing 5% of your annual	As the original is "very

annual income in a very speculative stock. (F)	income / saving in a risky start-up tech company (F)	speculative", I think "risky" is more appropriate than "fairly risky" (even though it's probably what I suggested before!)
13. Going whitewater rafting at high water in the spring. (R)	13. Going jet ski-ing in very rough waves. (R) (UK) 13. Going jet skiing in surging sea waves. (KSA)	I've made the UK one closely to the KSA one and I think it's better (I was struggling for the correct words on this one before)
14. Betting a day's income on the outcome of a sporting event (F)	~~14. Betting a day's income on the outcome of a sporting event (F)~~	Deleted for both UK & KSA
15. Engaging in unprotected sex. (H/S)	15. Engaging in unprotected sex. (H/S) (UK) 15. Smoking in closed spaces/buildings (KSA)	
16. Revealing a friend's secret to someone else. (E)	16. Revealing a friend's secret to someone else. (E)	
17. Driving a car without wearing a seat belt. (H/S)	17. Driving a car without wearing a seat belt. (H/S)	
18. Investing 10% of your annual income in a new business venture. (F)	18. Investing 10% of your annual income in a new business venture. (F)	This statement seems very similar to 4 and 12, although it is clear but not sure if I need to ask young people about investing three times.
19. Taking a skydiving class. (R)	19. Taking a skydiving class. (R)	
20. Riding a motorcycle without a helmet. (H/S)	20. Riding a motorcycle without a helmet. (H/S)	
21. Choosing a career that you truly enjoy over a more secure one. (S)	21. Choosing a career that you truly enjoy over a more secure one. (S)	
22. Speaking your mind about an unpopular issue in a meeting at work. (S)	22. Speaking your mind about an unpopular issue in a meeting at work. (S)	
23. Sunbathing without sunscreen. (H/S)	23. Sunbathing without sunscreen. (H/S) (UK) 23. Going outside in a very hot and sunny day without sunscreen. (KSA)	
24. Bungee jumping off a tall bridge. (R)	24. Bungee jumping off a tall bridge. (R)	
25. Piloting a small plane. (R)	25. Piloting a small plane. (R)	
26. Walking home alone at night in an unsafe area of town. (H/S)	26. Walking home alone at night in an unsafe area of town. (H/S)	
27. Moving to a city far	27. Moving to a city far away	

away from your extended family. (S)	from your extended family. (S)	
28. Starting a new career in your mid-thirties. (S)	28. Starting a new career in your mid-thirties. (S)	
29. Leaving your young children alone at home while running an errand. (E)	29. Leaving young children alone at home while running an errand. (E)	As many people in my target age group (at least in the UK) will not have their own children yet, I will remove "your" – so they could be looking after younger siblings, relatives or someone else's children.
30. Not returning a wallet you found that contains $200. (E)	30. Not returning a wallet you found that contains £200. (E) 30. Not returning a wallet you found that contains SR 1000	I think it would be better if I change the currency (and maybe the amount) for both UK & KSA

The modified version will be a set of 26 statements while the original one contains 30 statements.

Appendix G: The Information Sheet Shared with Saudi Participants before the Diary Study

التهديدات و الهجمات الإلكترونية

من دراسة سابقة ، وجدنا أن المستخدمين الشباب في المملكة المتحدة والمملكة العربية السعودية أبلغوا أن هجمات التصيد الاحتيالي وسرقة البيانات الشخصية كانت أكثر تهديدات الأمان الإلكترونية التي واجهوها

هنا أحاول تقديم لمحة عامة عن هذه التهديدات الأمنية الشائعة عبر الإنترنت والتي تستهدف غالباً المستخدمين الأفراد أكثر من الشركات أو المنظمات. قد يلفت هذا الملف انتباهك إلى بعض هذه التهديدات التي قد تستهدفك أثناء وبعد فترة مشاركتك

تتمثل خطة هذا الملف في البدء بالتهديدات الأمنية العامة (وتم تقسيمها إلى قسمين أ و ب) ثم تتدرج إلى الأنواع الأكثر تحديدًا ضمن كل فئة. سيتم تقديم أمثلة وصور من الحياة الواقعية للمساعدة في تحديد وتمييز التهديدات الأمنية المختلفة عبر الإنترنت التي قد يواجهها الأفراد في حياتهم اليومية

أ. هجمات الهندسة الاجتماعية

تُعرَّف هجمات الهندسة الاجتماعية على أنها: "علم استخدام التفاعل الاجتماعي كوسيلة لإقناع فرد أو مؤسسة بالامتثال لطلب محدد من المهاجم حيث يتضمن التفاعل الاجتماعي و الإقناع"

هناك أنواع مختلفة من هجمات الهندسة الاجتماعية بناءً على الخصائص وطرق التشغيل مثلا:

1- **التصيد الاحتيالي**: يرسل المهاجمون رسائل بريد إلكتروني أو رسائل نصية تبدو وكأنها من شركة أو مؤسسة حقيقية. غالبًا ما يُطلب من الأشخاص الذين يتلقون رسائل البريد الإلكتروني أو الرسائل النصية هذه النقر فوق رابط أو تقديم معلومات شخصية. يمكن للمجرمين سرقة اسم المستلم أو المعلومات المالية إذا نقر المستلم على الرابط أو قدم معلومات شخصية

غالباً تتضمن الطلبات في التصيد الاحتيالي ما يلي

تنزيل ملف مرفق

تمكين وحدات الماكرو في مستند وورد

تغيير كلمة المرور

الرد على طلب صداقة أو طلب اتصال على وسائل التواصل الاجتماعي

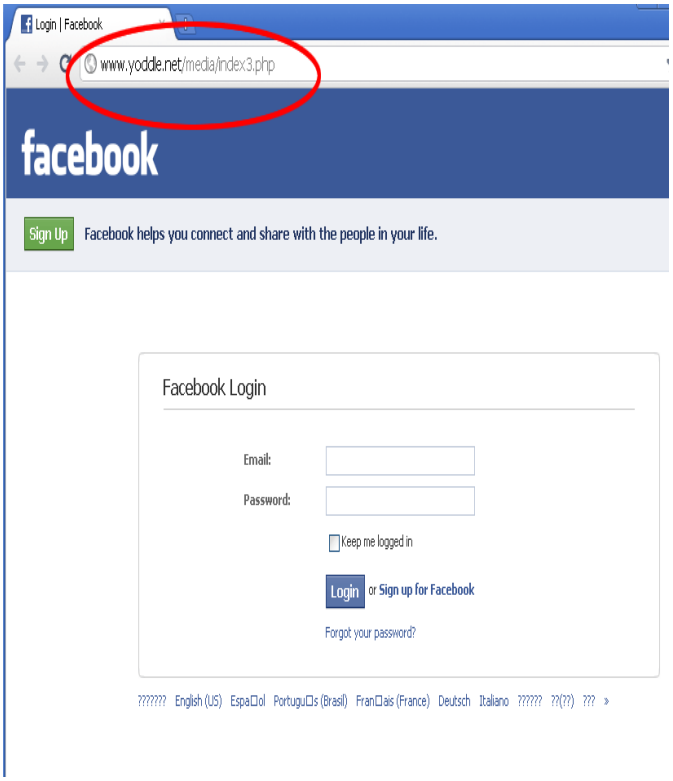
الاتصال بشبكة لا سلكية جديدة

أمثلة عن الهجمات وكيف تتم بطرق توزيع مختلفة

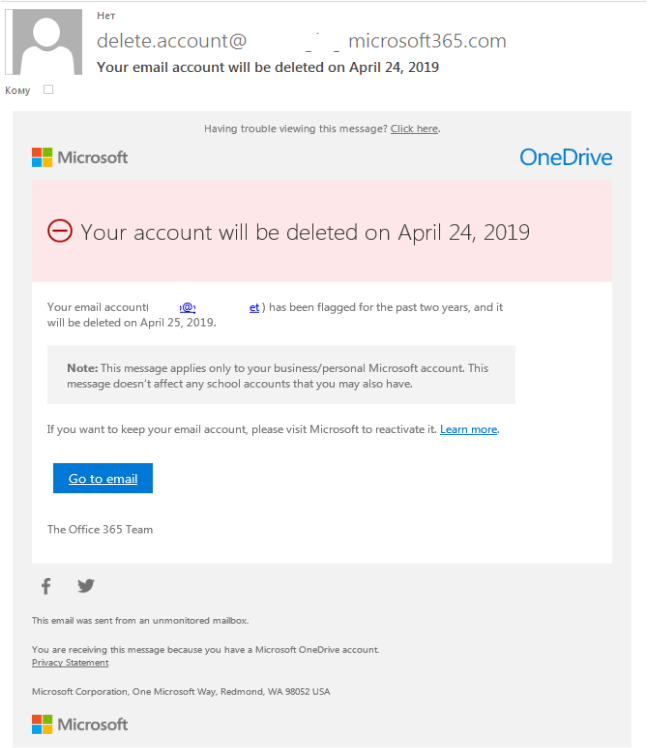
التصيد الاحتيالي بالبريد الإلكتروني: يتلقى المستخدم ما يبدو أنه بريد إلكتروني من شركة معروفة مثل الفيس بوك يطلب منه التحقق من معلومات حسابه من خلال الضغط عالرابط . يبدو أن البريد الإلكتروني حقيقي وله شعار فيس بوك وبالنقر على الرابط يؤخذ المستخدم إلى موقع ويب مزيف حيث تتم سرقة معلومات تسجيل الدخول الخاصة به

الصورة (1) توضح الموقع المزيف والذي يتم من خلاله خداع المستخدم للحصول على بياناته الخاصة بتسجيل الدخول

الصورة (2) توضح هجمة تصيد احتيالي باستخدام البريد الالكتروني تبدو أنها بريد مُرسل من مايكروسوفت يطلب الضغط على رابط للإبقاء عالحساب



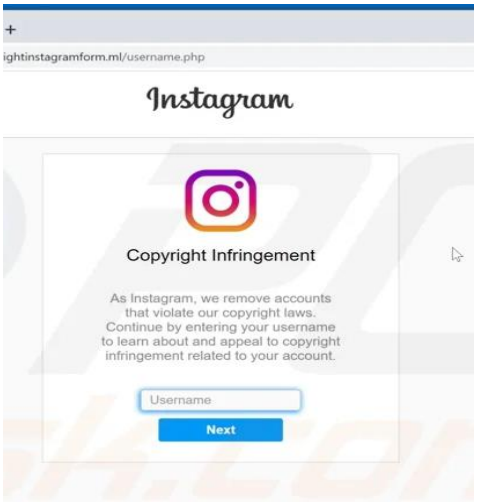
الصورة 1



الصورة 2

1.2 مواقع التصيد الاحتيالي: عبارة عن مواقع ويب احتيالية تحاكي مواقع حقيقة (كالبنوك و مواقع التواصل الاجتماعي) بقصد خداع المستخدمين للكشف عن معلومات حساسة ، مثل بيانات تسجيل الدخول أو البيانات الشخصية أو التفاصيل المالية. غالبًا ما تستغل هذه الهجمات ثقة الإنسان ومعرفته بالمواقع المعروفة لخداع الضحايا

مثال: الإعلان في عدد من المواقع الإلكترونية الاحتيالية عن عملية تسمى "انتهاك حقوق الطبع والنشر في انستقرام". حيث يتم الاعلان على أنه تم اكتشاف أن حسابات المستخدمين تحتوي على محتوى ينتهك لوائح حقوق النشر في انستقرام. و في الحقيقة هي محاولة للحصول على معلومات تسجيل الدخول بما في ذلك اسم المستخدم وكلمة المرور (الصورة3)

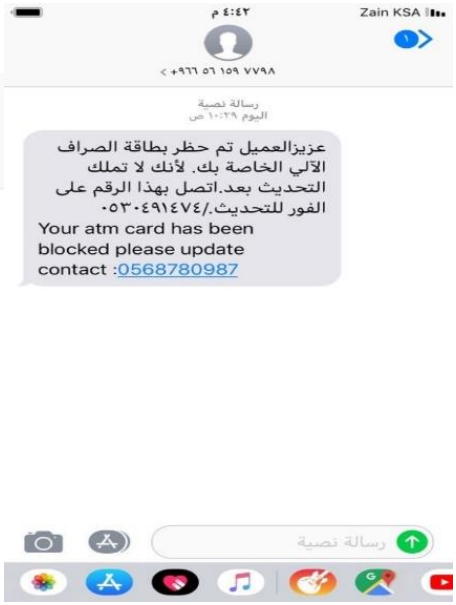


الصورة 3

مثال أخر حيث يتم انشاء موقع مشابه لموقع (نور) التابع لوزارة التعليم السعودية و يتم نشره على انه الموقع الحقيقي وبالتالي يتم سرقة بيانات المستخدمين. (صورة 4)

صورة 4

1.3 التصيد الاحتيالي عبر الرسائل النصية القصيرة: يشبه التصيد الاحتيالي ، ولكن يتم إجراؤه من خلال الرسائل النصية القصيرة لخداع المستخدمين لتقديم معلومات شخصية أو النقر على روابط ضارة (صورة5 و 6)



الصورة 5 **الصورة 6**

1.4 التصيد الاحتيالي الموجه: هجمات التصيد الموجهه تكون عالية الاستهداف حيث يتم جمع معلومات حول أفراد أو مؤسسات معينة لجعل الهجوم أكثر إقناعًا وتخصيصًا. غالبًا ما تستخدم هذه الرسائل الخاصة بالتصيد الاحتيالي لغة عاجلة ومعروفة لإقناع ضحاياها باتخاذ إجراءات فورية (انظر صورة 7 و 8)

صورة 7 **صورة 8**

1.5 التصيد الصوتي: يتم استخدام الاتصالات الصوتية ، مثل المكالمات الهاتفية ، لخداع الأفراد للكشف عن معلومات حساسة أو القيام بإجراءات معينة

على سبيل المثال: يدعي المتصل أنه من بنك أو شركة أو مكتب حكومي أو قسم شرطة أو شركة تكنولوجيا معلومات ولديه احتياجات عاجلة مثل مذكرة توقيف أو ديون متأخرة أو معاملات احتيالية أو فرص محدودة المدة. قد يتظاهر المتصلون بأنهم يحاولون مساعدة الضحية وحل بعض المشكلات ، وللقيام بذلك يحتاجون إلى مزيد من المعلومات مثل بيانات تسجيل الدخول وأرقام البطاقات البنكية أو أرقام الهوية الوطنية. قد يكون المتصلون من أي مكان. قد يكون معرف المتصل خاصًا أو غير مدرج.

احيانا تظهر الأرقام المخادعة في معرف المتصل مشابه لمن يدعي أنه يمثله. يستخدم المتصلون أسلوب الاستعجال لإغراء الضحايا لاتخاذ قرارات عاطفية بسرعة

تعد هجمات التصيد بأنواعها المختلفة من أكثر الطرق شيوعاً ضد الأفراد. تستخدم هذه الهجمات في بعض الأحيان كبداية لهجمات أخرى. قد يتم مثلا من خلال تصيد صوتي سرقة بيانات شخصية وبنكية يتم استخدامها لاحقا في تحويلات مالية أو الشروع في أعمال اجرامية باسم الضحية .

ب. البرمجيات الخبيثة

هي فئة من البرامج التي تتضمن الفيروسات وبرامج التجسس وبرامج الإعلانات المتسللة وبرامج الفدية. يمكن أن تصيب جهازك بطريقتين شائعتين: من خلال تقنيات الهندسة الاجتماعية (وهي شائعة جدًا للمستخدمين الأفراد) كما هو موضح أدناه ، أو من خلال الثغرات الأمنية

من المهم معرفة أن المهاجمين يشنون هجومهم على مراحل متعددة: يمكنك اكتشاف التهديد في أي مرحلة وبمجرد أن تتمكن من اكتشافه سيكون من السهل منعه أو التقليل من الخسارة. يحاول المهاجمون أولاً إرسال التهديدات ثم بمجرد تلقيها سيتمكنون من استغلالها

تستخدم الهجمات الإلكترونية الهندسة الاجتماعية لخداع الأشخاص للقيام بأعمال أو تقديم معلومات مهمة. تتضمن حيل الهندسة الاجتماعية استخدام الخوف أو الفضول أو اللطف لخداع الضحية والاستجابة لطلباتهم

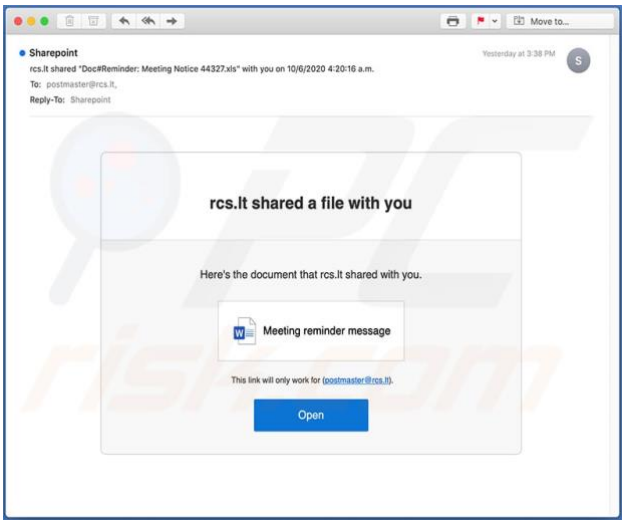
على سبيل المثال: كيف ينقل المهاجمون الفيروسات من خلال رسائل البريد الإلكتروني المخادعة

الخطوة 1 نشر وارسال البرامج الضارة: يرسل المهاجمون رسائل بريد إلكتروني أو رسائل نصية قصيرة تبدو وكأنها من مصدر معروف ، مثل بنك أو منصة وسائط اجتماعية ، ويطلبون معلومات حساسة من خلال النقر على رابط يؤدي إلى موقع ويب ضار أو تحميل ملف مرفق

الخطوة الثانية: مرحلة الهجوم أو الاستغلال

يؤدي النقر فوق الارتباط أو تنزيل الملف إلى السماح للمهاجم بالوصول إلى جهاز الضحية من خلال البرامج الضارة التي تم تنزيلها بعد الاصابة قد يلاحظ الضحية مجموعة متنوعة من مؤشرات الإصابة بالبرنامج الخبيث، مثل: أداء الجهاز ضعيف فيعمل جهاز الكمبيوتر بشكل أبطأ من المعتاد أو يتعطل كثيرًا

يمكن أيضاً ملاحظة تشغيل بعض برامج بشكل تلقائي أو تنفيذ عمليات أخرى غير مبررة على الجهاز. من الأمور الملاحظة ايضاً زيادة في تكرار النوافذ المنبثقة في المتصفح والبريد الإلكتروني العشوائي. صورة 9 توضح مثال لارسال البرمجيات الخبيثة كملف مرفق.



صورة 9

Appendix H: UK Diary Study Questionnaire

Online threats and scams Diary Study

Day 1

Welcome to the diary study. As this is first day, if you encountered any threats/scams, it might take a bit longer to complete the questionnaire, but once you are familiar with the questions, you will find it becomes much quicker and you will know the things we are interested in.

We will just ask you to report how many threats/scams you might have encountered today. Then if you did encounter any, for up to three threats/scams, we will ask for more information.

In case you want to consult it and didn't download it, the notes on some of the different types of threats/scams can be found here: **Error! Hyperlink reference not valid.**

If you have any questions, just message Helen through the Prolific Messaging system

Q18 What is your Prolific ID? Please note this response should auto-fill with the correct ID

_____

Q2 Did you encounter any possible online threats or scams today?

- ○ No (1)
- ○ Yes (2)

Q3 In total how many possible threats/scams did you encounter?

- ○ 1 (1)
- ○ 2 (2)
- ○ 3 (3)
- ○ 4 (4)
- ○ 5 (5)
- ○ more than 5, please specify how many (6)

_____

Scam1_1 Reporting on a first threat/scam

Which device did this possible threat/scam occur on?

- ○ Desktop (1)
- ○ Laptop (2)
- ○ Tablet (3)
- ○ Smart/mobile phone (4)
- ○ Other, please explain (5) _____
- ○ Can't remember (6)

Scam1_2 Which channel did it come through?

- ○ email (1)
- ○ text message (2)
- ○ voice message (3)
- ○ social media site, please specify (4)
- ○ website (5)
- ○ app (6)
- ○ other, please explain (7) _____
- ○ Can't remember (8)

Scam1_3 If you can, please upload a screenshot of the threat/scam

---

Scam1_4 Was the threat/scam a ...

- ○ Phish (a non-specific attempt to obtain information/money from you) (1)
- ○ Spear phish (a somewhat personalised attempt to obtain information/money from you) (2)
- ○ Malware/virus (3)
- ○ Ransomware (an attempt to blackmail you/extort money from you) (4)
- ○ Spoofed website/app (a website or app which was not what it should have been) (5) _____
- ○ Other, please explain (6) _____
- ○ Not sure (7)

Scam1_5 What made you think it might be a threat/scam? (select all that apply)

- [ ] Request for sensitive information (e.g. bank details) (1)
- [ ] Incorrect information (e.g. parcel delivery, but you are not expecting a parcel) (2)
- [ ] Suspicious email/number/user name (3)
- [ ] Unknown email/number/user name (4)
- [ ] Lack of sender/business information (5)
- [ ] Making an offer too good to be true (6)
- [ ] Suspicious link (7)
- [ ] Trying to look like a well-known company (e.g. using logo) (8)
- [ ] Spelling/grammatical mistaks (9)
- [ ] Unprofessional layout/presentation (10)
- [ ] Other, please explain (11) _____

Scam1_6 Could you explain a bit on what made you think it might be a threat/scam?

_____

Scam1_7 Were you already aware of this kind of threat/scam?

- ○ Yes (1)
- ○ I think so (2)
- ○ No (3)

Scam1_8 How were you aware of this kind of threat/scam? (select all that apply)

- [ ] Television/newspaper information, specify if possible (1)

_____

☐ Social media, specify if possible (2)
_____

☐ Family or friends (3)

☐ I've encountered it before (4)

☐ I don't remember (5)

Scam1_9 Did you interact with the possible threat/scam at all? Meaning, did you open a message/email, click on a link etc?

○ No (1)

○ Yes (2)

Scam1_10 How did you interact with the threat/scam?

_____

_____

Scam1_11 Did you do anything to try to figure out whether it was a threat/scam or to resolve the issue (e.g. delete the contact, report it to www.actionfraud.police.uk)?

○ No (1)

○ Yes (2)

Scam1_12 What did you do to try to figure out whether it was a threat/scam or resolve the issue?

_____

Scam1_16 Did you understand what the purpose of threat/scam was?

○ I have no idea (1)

○ (2)

○ I have some idea (3)

○ (4)

○ I am sure about the purpose of the threat/scam (5)

Scam1_17 If you think you have some idea about the purpose of the threat/scam, could you briefly explain

_____

Scam1_13 In the end, did you think it was a threat/scam?

- Definitely not a threat/scam (1)
- (2)
- Still not sure (3)
- (4)
- Definitely a threat/scam (5)

Scam1_14 Is there anything else you would like to say about this possible threat/scam?

Scam1_15 Do you have another threat/scam to report today?

- No (1)
- Yes (2)

Appendix I: Pre-study Questionnaire for the Diary Studies

DOSPRET Please rate how likely it is that you would act in the manner described in each of the following statements if you were in that particular situation.

	Extremely Unlikely (1)	(2)	(3)	(4)	(5)	(6)	Extremely likely (7)
Admitting that your opinions are different from those of a friend. (1)	○	○	○	○	○	○	○
Going camping in the wilderness. (2)	○	○	○	○	○	○	○
Investing 10% of your annual income / saving in moderate growth tech company (3)	○	○	○	○	○	○	○
Take certain medications that may affect your behavior before a social event (4)	○	○	○	○	○	○	○
Making questionable claims on expenses to your employer or for a university project (5)	○	○	○	○	○	○	○
Disagreeing with an authority figure on a major issue (6)	○	○	○	○	○	○	○
Passing off somebody	○	○	○	○	○	○	○

else's work as your own (7)							
Go on a path that you know is beyond your ability (8)	○	○	○	○	○	○	○
Investing 5% of your annual income / saving in a risky start-up tech company (9)	○	○	○	○	○	○	○
Crossing valleys on a rainy day (10)	○	○	○	○	○	○	○
Skipping recommended health screenings or medical check-ups (11)	○	○	○	○	○	○	○
Revealing a friend's secret to someone else (12)	○	○	○	○	○	○	○
Driving a car without wearing a seat belt (13)	○	○	○	○	○	○	○
Taking out a large loan, even if I was not sure I could afford to repay it. (14)	○	○	○	○	○	○	○
Taking a skydiving class (15)	○	○	○	○	○	○	○
Riding a motorcycle without a helmet (16)	○	○	○	○	○	○	○
Choosing a career that	○	○	○	○	○	○	○

you truly enjoy over a more secure one (17)							
Speaking your mind about an unpopular issue in a meeting at work (18)	○	○	○	○	○	○	○
Going for a walk outside on a very hot sunny day without sunscreen (19)	○	○	○	○	○	○	○
Rock climbing without proper safety equipment. (20)	○	○	○	○	○	○	○
driving big vehicles like trucks or tractor (21)	○	○	○	○	○	○	○
Walking home alone at night in an unsafe area of town (22)	○	○	○	○	○	○	○
Moving to a city far away from your extended family (23)	○	○	○	○	○	○	○
Starting a new career in your mid-thirties (24)	○	○	○	○	○	○	○
Leaving young children alone at home while running an errand (25)	○	○	○	○	○	○	○
Not returning a wallet you	○	○	○	○	○	○	○

found that contains SR 1000 (26)

SeBIS How often do you take the following actions in relation to your devices? If any of the actions are not applicable or you do not understand what is being referred to in any of the statements, please select Never.

	Never (1)	(2)	(3)	(4)	(5)	(6)	Always (7)
I set my computer screen to automatically lock if I don't use it for a prolonged period of time. (1)	○	○	○	○	○	○	○
I use a password/passcode to unlock my laptop or tablet. (2)	○	○	○	○	○	○	○
I manually lock my computer screen when I step away from it. (3)	○	○	○	○	○	○	○
I use a PIN or passcode to unlock my mobile phone. (4)	○	○	○	○	○	○	○
I do not change my passwords, unless I have to ®. (5)	○	○	○	○	○	○	○
I use different passwords for different accounts that I have. (6)	○	○	○	○	○	○	○
When I create a new online account, I try to use a password that goes beyond the site's minimum requirements. (7)	○	○	○	○	○	○	○
I do not include special characters in my password if it's not required. ®(8)	○	○	○	○	○	○	○

When someone sends me a link, I open it without first verifying where it goes.(r) (9)	○	○	○	○	○	○	○
I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar ®(10)	○	○	○	○	○	○	○
I submit information to websites without first verifying that it will be sent securely (e.g. SSL, "https://", a lock icon). (11)	○	○	○	○	○	○	○
When browsing websites, I mouseover links to see where they go, before clicking them. (12)	○	○	○	○	○	○	○
If I discover a security problem, I continue what I was doing because I assume someone else will fix it (13)	○	○	○	○	○	○	○
When I'm prompted about a software update, I install it right away. (14)	○	○	○	○	○	○	○
I try to make sure that the programs I use are up-to-date. (15)	○	○	○	○	○	○	○
I verify that my anti-virus software has been regularly updating itself. (16)	○	○	○	○	○	○	○

Demographic 5 How would you rate your general computer knowledge?

- ○ not at all knowledgeable (1)
- ○ (2)
- ○ (3)
- ○ (4)
- ○ (5)
- ○ (6)
- ○ Very knowledgeable (7)

Demographic 6 Have you attended information security training sessions/courses?

- ○ Yes (1)
- ○ No (2)

Demographic 7 How would you rate your online security knowledge?

- ○ not at all knowledgeable (1)
- ○ (2)
- ○ (3)
- ○ (4)
- ○ (5)
- ○ (6)
- ○ Very knowledgeable (7)

Appendix J: Post-study for the UK diary study

The final questionnaire! Thanks very much for completing the diary entries, we have received a lot of really interesting data (even the days when you didn't encounter any threats/scams is important to us, as we are investigating just how much of a problem they have become). There's just one last questionnaire with some questions about your experience with the study, with online threats and scams in general and your orientation to the future. When you have completed all 7 days of diary entries and this questionnaire, we will credit you with the extra £3 bonus (Helen will send you a message if you are missing any days). We will also send a link to your Prolific account next week with links to good sources of information about how to deal with online threats and scams and within about four weeks another link with some results of the research, in case you are interested. In the meantime, if you have any questions, just contact Helen via the Prolific messaging system.

Q_ID What is your Prolific ID? Please note that this response should be auto-fill with the correct ID

_____

UO_1 Firstly, a few questions about your overall attitude to online threats and scams Compared to your friends, do you think you are more or less likely to receive online threats/scams?

- ○ much less likely (8)
- ○ (9)
- ○ about the same (10)
- ○ (11)
- ○ much more likely (12)

UO_2 Compared to a typical person of your age, do you think you are more or less likely to receive online threats/scams?

- ○ much less likely (8)
- ○ (9)
- ○ about the same (10)
- ○ (11)
- ○ much more likely (12)

UO_3 Compared to your friends, do you think you are more or less able to detect whether something is an online threat/scam?

- ○ much less able (8)
- ○ (9)
- ○ about the same (10)
- ○ (11)
- ○ much more able (12)

UO_4 Compared to a typical person of your age, do you think you are more or less able to detect whether something is an online threat/scam?

- ○ much less able (8)
- ○ (9)
- ○ about the same (10)
- ○ (11)
- ○ much more able (12)

UO_5 Compared to your friends, do you think deal more or less well with online attacks/scams?

- ○ much less well (8)
- ○ (9)
- ○ about the same (10)
- ○ (11)
- ○ a lot more well (12)

UO_6 Compared to a typical person of your age, do you think you deal more or less well with online attacks/scams?

- ○ much less well (8)
- ○ (9)
- ○ about the same (10)
- ○ (11)
- ○ a lot more well (12)

Q8 Next a few questions about your experience of being in this study Do you think the period of the study was fairly typical in the number of online threats/scams you receive?

- ○ I probably received a a lot less threats in this period (2)
- ○ (4)
- ○ (5)
- ○ Fairly typical (6)
- ○ (7)
- ○ (8)
- ○ I probably received a lot more threats/scams in this period (9)

Q19 If you have any comments to add about why the period might have been typical or not, please add them here:

_____

_____

Q26 If there were any threats or scams that you encountered during the study period which struck you as particularly interesting or problematic, or anything you would like to add about the threats/scams you encountered, please add any comments you would like to make here:

_____

_____

_____

Q9 Do you think your attitude to online threats/scams has changed as a result of being in the study?

- ○ Not at all (1)
- ○ (8)
- ○ (4)
- ○ (6)
- ○ (7)
- ○ (16)
- ○ A great deal (17)

Q20 If you have any comments to make about how your attitude has changed, please add them here

_____

_____

Q21 Do you think you will be more vigilant about monitoring for online threats/scams in the future?

- ○ Much less vigilant (1)
- ○ (2)
- ○ (3)
- ○ About the same as before (4)
- ○ (9)
- ○ (10)
- ○ Much more vigilant (11)

Q22 Do you think you will be better at detecting online threats/scams in the future?

- ○ Much less good at detecting (1)
- ○ (2)
- ○ (3)

○ About the same as before (4)

○ (5)

○ (6)

○ Much better at detecting (7)

Q27 Do you think you will be better at dealing with online threats/scams in the future?

○ Much less good at dealing with them (1)

○ (2)

○ (3)

○ About the same (4)

○ (5)

○ (6)

○ Much better at dealing with them (7)

Q24 If you have any comments about how your behaviour in relation to online threats/scams might be different in the future, please add them here:

_____

CFC Finally some strange questions about your orientation to the future (a type of a personality questionnaire, we will explain all about this in our report on the study). For each of the statements below, please indicate whether or not the statement is characteristic of you:

	extremely uncharacteristic (1)	(3)	(4)	(5)	extremely characteristic (6)
I consider how things might be in the future, and try to influence those things with my day-to-day behaviour (1) **F**	○	○	○	○	○
Often, I engage in a particular behaviour in order to achieve outcomes that may not result for many years (2) **F**	○	○	○	○	○
I only act to satisfy immediate concerns, figuring the future will take care of itself. (3) **I**	○	○	○	○	○
My behaviour will only influenced by the immediate (i.e., a matter of days or weeks) outcomes of my actions. (4) **I**	○	○	○	○	○
My convenience is a big factor in the decisions I make or the actions I take. (5) **I**	○	○	○	○	○

I am willing to sacrifice my immediate happiness or well-being in order to achieve future outcomes. (6) **F**	○	○	○	○	○
I think it is important to take warnings about negative outcomes seriously even if the negative outcomes will not occur for many years. (7) **F**	○	○	○	○	○
I think it is more important to perform a behaviour with important distant consequences than a behaviour with less important immediate consequences (8) **F**	○	○	○	○	○
I generally ignore warnings about possible future problems because I think the problems will be resolved before they reach crisis level. (9) **I**	○	○	○	○	○
I think that sacrificing now is usually	○	○	○	○	○

unnecessary since future outcomes can be dealt with at a later time. (10) **I**					
I only act to satisfy immediate concerns, figuring that I will take care of future problems that may occur at a later date. (11) **I**	○	○	○	○	○
Since my day-to-day work has specific outcomes, it is more important to me than behaviour that has distant outcomes. (12) **I**	○	○	○	○	○
When I make a decision, I think about how it might affect me in the future (13) **F**	○	○	○	○	○
My behaviour is generally influenced by future consequences (14) **F**	○	○	○	○	○

Q25 That's it! If you have any final comments about your participation in this research or online threats and scams, please add them here. Many thanks for all your help. Helen and Najla

_____