THE EFFECT OF PERSONALITY ON SMS PHISHING VULNERABILITY

Rasha Salaheldin Abdelazeem Ibrahim

Doctor of Philosophy

University of York
Computer Science

August 2016

Abstract

In the last decade, cybercrime has sought to bypass technical security in place by focusing in people. Recently more attention has been given to the security of mobile devices. However, very little research has investigated the human factors of mobile phishing. This thesis investigates human aspects in relation to SMS phishing. Based on our findings, we present recommendations and opportunities for research that will help the security community to better understand phishing attacks and educate mobile users against them.

The first study reports the results of a qualitative investigation of what people think and feel about mobile security. The study presents this investigation temporally by means of a series of interviews performed sequentially in multiple stages. A variation was noted in the users' responses and a theory was developed to explain such variation. The study proposed a grounded theory that suggested that human security attitude is strongly influenced by their *agreeableness*, *conscientiousness* and *extraversion* personality traits. The developed theory suggested that this general behaviour is moderated by individuals' knowledge and past error-in-judgement experiences. The theory was tested via three further studies (one lab study and two experimental studies). The results suggest that the personality traits *Assertiveness* and *Extraversion* affect humans' phishing vulnerability.

To the best of our knowledge, the three studies are the first empirical studies of the human aspects involved in SMS phishing.

The thesis embraces both quantitative and qualitative analysis approaches. The quantitative analysis helped in isolating the personality traits *Assertiveness* and *Extraversion* while the qualitative analysis helped us understand how individuals reason about their behaviour.

Table of Contents

1 Contents

List of Tables

List of Figures

Acknowledgements

The author wishes to thank God for all his support and help. I felt I was immersed in his mercy all over the way.

I wish also to express sincere appreciation to my supervisor Professor John Clark for his assistance.

Special appreciation goes to my parents, and my sister for all their patience, support and prayers, to my lovely daughter Malak, for her tolerance, understanding, and support, and for my grandma for being a source of constant and unconditional love.

Special thanks go to my very dear friend Dina Salah for all her support and advice, and for being a source of inspiration and a role model, and to my colleague Ibrahim Shiyam for all his help and encouragement.

I wish also to thank the examiners Professor David Chadwick and Professor Richard Paige for their valuable feedback and comments.

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 an award at this, or any other, University. All sources are acknowledged as References.

List of Publication

1. El-Din, R. S., Cairns, P., & Clark, J. (2015). The Human Factor in Mobile Phishing. *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, 53-65.

2. El-Din, R. S., Cairns, P., & Clark, J. (2014). Mobile Users' Strategies for Managing Phishing Attacks. *Journal of Management and Strategy*, 5(2), 70.

3. El–Din, R. S., & Sugiura, L. (2013). To deceive or not to deceive! Legal implications of phishing covert research. *International Journal of Intellectual Property Management*, 6(4), 285-293.

4. Salah El-Din, R. (2013). Deceive or not to Deceive! Ethical Questions in Phishing Research. *In Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM.

5. Salah El-Din, R. (2012) To Deceive or not to Deceive! Ethical Questions in Phishing Research. In *HCI Research in Sensitive Contexts: Ethical Considerations workshop at HCI 2012*. Birmingham, UK, 10-14 September 2012.

6. Salah El-Din, R., Sugiura, L. (2012) Legal Implications of Phishing Covert Research. In LSPI (The 7th International Conference on Legal, Security and Privacy Issues in IT), Athens, Greece, 2-4 October 21012.

Chapter 1: Introduction

1.1 Background and Significance of research

Phishing is a pernicious practice whereby cyber-criminals seek to obtain sensitive confidential information such as usernames, passwords or financial account details from people under false pretences (Stavroulakis & Stamp, 2010). The criminals may impersonate a trustworthy entity like the victim's bank, mobile operator or even a friend in an electronic communication.

Although fixed computing was the default target for phishing attackers for a long time, phishing scams are now increasingly targeting the mobile domain (Jevans, 2015; Bradely, 2014; Ashford 2014). Security experts have attributed this to a number of factors such as the widespread use of mobile devices, the increasing use of mobile payment and the vulnerability of both mobile phones and mobile users (Anti Phishing Working Group, 2015; Symantec, 2015; Jevans, 2015).

In regards to mobile usage, mobile phones have become an essential tool for communication both globally and nationally. According to the latest statistics, there are around 4.3 billion mobile users worldwide (Statista, 2016). Ofcom, the communications regulator in the UK, has referred to the UK as a 'smartphone society' after its communications market report revealed that 66% of adults in the UK use smartphones, an increase from only 39% in 2012 (Ofcom, 2015). The report also found that 33% of internet users in the UK have rated their smart phone as their primary device for getting online.

This increase in mobile usage has been reflected in mobile payments as well. The term 'mobile payments' refers to payment services performed via cell phones and can include all mobile communication devices (Schierz, Schilke, & Wirtz, 2010). For the purpose of this research, and as our main focus is mobile phones, we will be using mobile payment to refer to electronic payments using cell phones. In this respect, according to the recent Statista report, mobile payments in the UK have increased from 9% to 33% between 2013 and 2015 (Statista, 2016). Worldwide, 50% of consumers are expected to be using mobile phone payments by 2018 (Gartner, 2015).

This widespread use of mobile devices and monetary services has triggered the emergence of mobile attacks. As reported by CSO, mobile security tops the list of most pressing enterprise security concerns (CSO, 2015). According to a recent security report from Kaspersky, early attacks targeted emails on tablets and smartphones and then spread to mobile text messages, multimedia messages and mobile applications (Kaspersky, 2014).

This causes great concern among security experts. Of particular concern is that so many of these phishing attacks succeed in spoofing sender IDs so they appear as if they have been sent from a trusted known source to the mobile user.

Of further concern to security experts is that there are few malware detection mechanisms in place on mobile platforms. Also individuals do not expect security attacks via mobile and hence are more likely to trust links or photos sent to their cell phone, especially if the sender is (or appears to be) someone on their contact list (Jakobsson, 2011). Moreover, mobile users are unaware that their mobile phones can be infected by malware. Dave Jevans, the chair of Anti Phishing Working Group, explains how BYOD (Bring Your Own Device) helped introduce security threats via mobile phones (Jevans, 2015).

Email Drop: While mobile malicious attacks increased, E-mail attacks rates decreased. According to the latest security reports, spam rates (phishing rates and email-based malware) have considerably decreased lately. In 2010, spam rates settled at 82.2%, 80.3% in 2011, 72.1 % in 2012 (Kaspersky, 2012), and at 49.7% in 2015 (Symantec, 2015).

On the other hand, Email Phishing rates have been in decline recently. The overall phishing rate in 2014 was 1 in 965, compared with 1 in 392 in 2013 (Symantec, 2015). This decline in email phishing rates continued reaching 1 in 2703 emails by the end of 2015 (Symantec, 2016). Symantec experts attribute this fall **in email-based malicious** activity to two main reasons: attackers moving to other areas of the risk landscape and the spread of spam filters and anti-phishing software through webmail services (Symantec 2015; Kaspersky 2012).

History of SMishing:

In this section, a brief history of how SMS Phishing (Smishing) emerged is presented. The section shows how SMishing started and lists a number of incidents in different countries, and how the severity of these incidents led to governments to seek to provide legal protection for users.

China: The first incidents of using mass mobile short messages for illegal purposes were in late 2005 in China leading to around 10,000 mobile phone accounts being closed down for sending illegal messages. According to the government investigations, the majority of mobile users in China were showered by unsolicited messages on a daily basis. However, not all offenders could be pursued by law. China had 338 million mobile users, including around 200 million with identities unknown to their mobile operators in

China (because they used pay-as-you- go phone cards). Following this incident of mass-sending of illegal mobile messages, the Chinese government has decided to move forward with a policy that requires all mobile users to register their personal information into the telecommunication system of China. Before enforcing this policy, presenting a form of ID and registering personal information was a requirement for monthly-contract mobile users only. Pay-as-you-go mobile users did not have to go through this process. Accordingly, it was very easy for criminals to buy prepaid phone cards using fake names, and send messages to groups of mobile phone users. Examples of such messages include texts informing users they had won lottery prizes and asking them to send money for shipping and insurance. Users who fell for the message and paid the phisher have never been contacted with regards to for the purported prizes (The State Council of China, 2006).

The Chinese Government believed that enforcing registration for all its mobile users, including prepaid cards users, could help track down criminals, and hence reduce the number of SMS attacks in the long term. However, the new policy has been applied haphazardly, as many mobile phone warehouses did not follow the registration policy. Some mobile operators did not require their cell phone users to register their personal information using a valid ID. This arose mostly out of the operators' fear that they might lose clients. Moreover, in regards to the existing 200 million pay-as-you-go users, it was extremely problematic, logistically, to register them all.

Europe & Australia:

Although, the SMS attacks in China in 2005 were significant, the world did not pay attention to the threat of SMishing until 2006 when cell phone users in Iceland and Australia started to receive their first SMS attack. The SMS message received appeared to be from a dating service provider and led the mobile users to a phishing website. Users who visited the website were infected by a backdoor Trojan downloaded to their devices. The message reads: "We're confirming you've signed up for our dating service. You will be charged $2/day unless you cancel your order: url".

The world's security experts responded quickly warning mobiles users of the new threat. They used titles such as 'SMS Phishing is here' (Hickey, 2006), 'SMishing - an emerging threat vector' (Utter, 2006) and 'McAfee warns of SMishing attacks' (Blau, 2006). Also, the South Australia Office of Consumer and Business Affairs (OCBA) issued a warning to their customers to watch out for this scam (Office of Consumers and Business Affairs, 2008).

In August of the same year, Spain saw a mass-mailing worm called 'VBS/Eliles.A' that performed a similar SMiShing attack. The malicious text message spread among customers of two mobile operators. Targeted users received an SMS purporting to be from their mobile service provider and advising them to download “free mobile phone antivirus software”. Customers who downloaded and installed the software from the link found themselves infected with malware.

Many security analysts expressed their worry about these types of attacks, and how they can introduce different sorts of malware. Once infected, mobile phones can start sending messages to premium rate numbers and hence increase the user’s phone bill dramatically. They also drew users’ attention to similar malware that sends premium–rate messages only once per month to avoid suspicion. Security experts also expressed concern for the security of enterprises as well. They warned that cell phones used by employees to access their enterprise’s network can be a threat to their business too (Karthikeyan 2009, Blau 2006, McAfee 2015).

Other examples of popular SMishing attacks are the Russian malware which in 2012 that sent premium-rate SMS messages. The malware had been masquerading as a game on Google Play (NQ Mobile Security, 2012). Another example of malicious application that has been uploaded as a trustworthy application is the Russian malware that spread in 2013 and 2015 (Minor, 2015). The users who download the game are infected by a malware that sends an SMS message with the user’s personal information.

Some of these messages are premium rate messages that charge the mobile user with high rates, and some can send themselves to other individuals on the mobile user’s contact list, infecting them with malware.

One of the Latest and largest SMishing attacks took place in August 2014 in China, where more than 100,000 mobile users were infected with malware via SMS phishing. 20 Million SMS texts were sent and the cost incurred was around 500, 000 Dollars, as each user was charged around 5 Dollars. Not only does this add additional cost to the mobile user’s bill, but it also downloads a malicious file that intercepts and sends SMS messages to the attackers’ email (Zhang, Wei, & Xue, 2014).

The security researcher Bogdan Alecu has demonstrated how remote SMS attacks can force cell phones to send premium-rate text messages to the sender’s number or to the mobile operator’s message centre. He explained how SIM Toolkit applications can perform tasks such as performing mobile banking, checking credit and voice mail, and calling emergency numbers. Most of the mobile phone devices don’t display any notifications to the user that a SIM Toolkit message was received, nor does any indication appear in the inbox. Alecu has tested these types of attacks on different devices such as HTC, Samsung, LG and BlackBerry. When Windows Mobile 6.x devices and iPhone were tested, they notified the mobile users that a message had been sent. However, they did not offer any method to stop it.

SMishing-related Governments' Regulations:

In 2006, the Korean Government took steps to prohibit sending more than 1000 messages per day. The government assured its mobile phone users that this decision should not affect normal citizens, as it is practically impossible for them to send 1000 message a day. However, this policy is aimed at those who use mobile messages as a means of sending malicious mobile messages via special devices.

In 2009, the first US legislation for blocking unsolicited SMS, the m-SPAM Act, was introduced (Congress, 2009). The Act aims at drawing more government attention to SMS and MMS, in addition to email messages.

The European Union has introduced legislation aimed at both email and mobile messages. This has subsequently been incorporated into local country laws. However, such laws have attracted criticism for doing more harm than good because of their negative effect on responsible marketing companies. Specifically, as the regulation has enforced applying an 'opt-in' approach, it was argued to be helping irresponsible spammers by making users confirm their mobile numbers. Many technical consultants such as Jamie Cowper questioned the effectiveness of such laws and raised the issue that these directives allow various interpretations of the law (Leyden, 2003). Moreover, a number of security corporations such as Brightmail and Mirapoint claim that the majority of unsolicited emails and mobile text messages come from either untraceable sources or spammers acting from outside the European Union (Leyden, 2003). The EU directive has also been described as very weak for making it legal for spammers to send unsolicited messages on a barely opt-out basis. As a result, security experts from the anti-spam corporation Cipher Trust, currently known as Secure Computing Corp, find such legislation insufficient and consequently prefer a three-pronged approach that combines legislation, user education and technology.

Awareness efforts against SMishing used to be restricted to service providers' websites such as banks and mobile operators alerting their clients not to fall for such malicious messages. However, recently, attention to such mobile attacks has been drawn via other media such as newspapers. In one recent incident, published in the Daily Telegraph, a retired vicar had his mobile bill doubled as a result of premium rate text messages (Bown, 2015). Another recent example of this, is the daily newspaper of the county of Gloucester that published, in February this year, the news of the mobile user who lost around £23,000 as a result of a SMishing attack (Boyce, 2016).

The Need to study Mobile Phishing

Mobile phishing has been described as 'The problem on the horizon' in the monthly security report of Trend Micro (Pajares & Abendan, 2013). It has also been regarded as an emerging threat that targets mobile customers (Boodaei 2011, Bortinik 2011) especially that mobile users do not expect to be hacked via their mobile phones, which make them more prone to these attacks. Recent studies that examined users' perception of phishing concluded that: "Emails are very phishy, web pages a bit, phone calls are not" (Jakobsson, 2007) and that phishing attacks can be more convincing on phones than in a desktop browser (Felt et al., 2011). Another factor that may increase the mobile phishing problem is the way most service providers currently communicate with their customers. For instance, when communicating with a financial institution nowadays, users are prompted to speak to an automated phone message and to dial-in identifying information such as their bank account details, date of birth and postal code in order to speak to a customer support agent. That, in itself, trains users to give out their credentials via phone calls (Jakobsson, 2007). Such a method of communication is likely to increase the phisher's credibility especially as users expressed that, in emergencies they would not expect an email, they would expect a phone or a text from whatever service providers trying to contact them (Jakobsson, 2007).

Research efforts on mobile phishing are mainly focused on technical aspects of mobile websites and mobile operating systems. Felt and Wagner conducted a study over 85 websites and 100 mobile applications. The study suggested that phishing risks on mobile platforms were greater than expected.

Via conducting a multi-method set of four studies, our research contributes to an understanding of both users' perception and behaviour towards mobile security in general and SMishing in particular.

The Need to Study SMishing in particular

Among the different forms of mobile phishing, SMishing has unique characteristics that make it very attractive to spammers. These include the success of the mobile messaging channels and the high level of trust associated with texting. Not only is mobile texting very easy to use, but also the level of trust between the mobile operators and their subscribers, in regards to texting, is unprecedented. According to IAB/DMA survey conducted in the UK in September 2010, 63% of mobile users said they were happy to receive both text and multimedia messages from their operators (Direct Marketing Association, 2010). This trust meant that almost all messages received by mobile users are opened and read. The numbers are also easily dialled and clicked. Adding to these, the very cheap cost of sending text message spam and the myriad of billing plans increase the risk of mobile messaging abuse. Worse than this, attackers are currently moving beyond simple spam messages to fraudulent scams, phishing and mobile spyware (Anti-Phishing Working Group, 2015).

1.2 Aim

The aim of the research reported in this thesis is to improve our understanding of why people fall for mobile phishing via identifying victim and detector characteristics that may influence their behaviour. There is a considerable lack of research in the field of SMS phishing and we hope our research can improve our understanding of the psychological aspects of it.

1.3 Thesis Research Hypotheses

This thesis investigates a general research question and three hypotheses.

The research question: what are the Human Factors affecting Mobile Phishing vulnerability?

The Research Hypotheses:

RH1: Individuals' personality traits affect mobile phishing vulnerability.

RH2: Individuals' previous history of error-in-judgement affects mobile phishing vulnerability.

RH3: Individuals' knowledge and awareness about phishing affect mobile phishing vulnerability.

The development of the Research Hypotheses

The research presented in this thesis began with the general research question: what are the human factors affecting Mobile Phishing Vulnerability? The literature review suggested a number of factors such as (age, gender, education, IT literacy, training, and personality traits). However, the literature suffered from a number of drawbacks:

i) The literature on human factors in phishing was inconclusive and contradictory (University of Sydney, 2016).

ii) The literature on mobile phishing was scarce and mostly focused on the technical side of the problem.

The research community (Shields & Rangarajan ,2013; Kolter & Armstrong, 2006; Glaser & Strauss, 1967; Stebbins, 2001; Jaeger & Halliday, 1998; Mulaik, 1987; Borkenau & Ostendorf, 1990; Moody et al., 2011; Wang & Benbasat, 2008; Rezgui & Marks, 2008; Chai, Bagchi-Sen, Morrell, Rao, & Upadhyaya, 2009) suggests that in such situations when the available literature is inconclusive or when a problem has not been clearly defined, an exploratory research is advised.

Accordingly, our first study was of an exploratory nature. It investigated the phenomenon of mobile security in general, and phishing in particular. It generated the three research hypotheses listed above (RH1, RH2, and RH3). The study highlighted the effect of personality traits. Personality is a form of individual difference that refers to characteristic patterns of thinking, feeling and behaving. More details on the generation of each hypothesis are discussed in chapter 3.

1.4 Thesis Methodology

The thesis embraces both experimental and correlational research approaches. In this section, we explain the different research methodologies used in phishing research, the rationale behind using these approaches, and how they were employed in the thesis.

1.4.1 Phishing Research Approaches:

Generally, there are two main approaches for phishing research: the correlational approach and the experimental approach. These are explained below.

a) Correlational Research:

In a correlational approach, researchers analyse what naturally goes on in the world without directly interfering with it, observe natural events or take a snapshot of different variables (Field & Hole, 2003). It mainly focuses on assessing the covariation among naturally occurring variables (Shaughnessy, Zechmeister, & Zechmeister, 1947). Generally, there are three principal correlational methodologies: naturalistic observation, self-report studies, and archives. These are outlined below.

i) Naturalistic Observation:

Naturalistic observation entails observing and recording the variables of interest to the research in their natural environment without any interference by the researcher (Bagley, 2007). In phishing research and under the correlational approach, this method largely involves monitoring honey pot activities. This sort of observation introduces serious ethical and legal considerations. Yet, it gives the experimenter the opportunity to view the variable of interest in a natural setting, can offer ideas for further research and may be the only option in cases where lab experimentation is not possible. Below, we explain the different scenarios that observing honey pots can have, and the ethical and legal implications for each.

Scenarios:

Scenario 1: The researcher is conducting his observational study with the help of some criminals.

Scenario 2: The researcher is working secretly without any criminal contact.

Accordingly, this type of research involves both direct and indirect contact between three kinds of stakeholders; the researcher, victims and attackers.

Below, we demonstrate ethical and legal considerations in relation to each stakeholder.

A) Ethical and legal considerations for the first stakeholder; the victims:

- Anonymity: The victims who were monitored by the researcher have the right to remain anonymous throughout the study and in any publications that may result from the research.

- Confidentiality: The confidentiality of the data observed is an important issue. The researchers may be able to access confidential information of the victims such as; their bank details, their home address, their e-mails, their date of birth, etc. All this information should not be saved or retained.

- Reporting the phishing attack: According to the law, there is no legal obligation whatsoever for a researcher witnessing a crime to report it. However, ethics-wise, reporting a law-breaking incident is a controversial issue; should the researcher stop a phishing attack he is observing and hence jeopardise his study if the attacker is alerted? Or should he just ignore his moral responsibility towards society or at least towards another human who is being attacked?

B) Ethical and legal considerations for the second stakeholder; the researcher:

- Safety: The protection of the researcher is the responsibility of the research institution or the affiliated industry.

- Anonymity: Special internet technologies that enable online anonymity should be in place to conceal the researcher location or usage and to protect him from network surveillance or traffic analysis. An example of these is TOR anonymity network (Dittrich, Bailey, & Dietrich, 2009).

- Special training: For scenario 2, it is advisable that the researcher should take a proper training of the etiquette of getting involved in a criminal environment. It is worth that the researcher seeks advice from an undercover reporter or a criminologist.

C) Ethical and legal considerations for the third stakeholder: the criminal:

- Privacy: Although the data monitored is private criminal data, it is still governed by the Data Protection Act. Accordingly, the researcher is advised to consult a legal professional to make sure his research is in compliance with DPA 1998.

- Anonymity: The criminal has the right to remain anonymous throughout the study and in any publications.

- Informed consent: An explicit consent should be secured with the criminal in advance.

ii) Phishing self-report studies:

Phishing self-report studies involve the use of questionnaires, online surveys, interviews or polls. Participants are often chosen randomly to answer a set of questions about their past phishing experience, recent losses or latest corruptions of systems and credentials (Jakobsson & Fin 2007).

This research approach has a number of limitations, one of which is underestimating the risk of phishing if a significant number of real phishing attacks were missed and not reported by participants (Jakobsson & Fin 2007). This happens when victims are either unaware they have been attacked or do not want to reveal they fell for phishing attacks out of embarrassment.

It is also possible that self-report studies overestimate risk if the participants report non-phishing incidents as phishing. This happens as a result of participants' unawareness of what exactly phishing is. An example of that is someone who finds that his credit card bill contains charges for items he has not purchased. He may suppose this is phishing and report it as so, while it might be an incident of fraud arising from another means (Jakobsson & Fin 2007). Overestimation of phishing risk can also occur if people reported legitimate messages they got from their bank, mobile operator or a real service provider as phishing attacks.

The underestimation or overestimation of phishing risks is likely to be reduced when there is direct contact between researcher and participant. Thus, it is more likely to be a threat for polls and on-line surveys than for interviews (where the researcher can provide clarifications to participants). However, interviews have their own problems when used in security research. For example, people's claimed security practices may not be their actual practices (Dourish, Grinter, De La Flor, & Joseph, 2004). One reason is that participants want to impress the researcher and look smarter in front of him/her. This problem is often referred to as 'the researcher effect'. Here the age, gender or race of the researchers may affect the result they obtain (Field & Hole, 2003).

Although self-report studies have limitations, they are useful in describing people's thoughts, opinions and feelings (Shaughnessy et al., 1947). They can be used as the first step before conducting an experiment, and are also often used when conducting experiments is not possible. Also, the analysis of the self-report data can lead to a construction of a theory via the use of grounded theory approach.

Grounded theory is a systematic research methodology that aims at theory-building based on qualitative data gathered throughout the research (Charmaz, 2006). Grounded theory helps in theoretical formulation via combining systematic levels of abstractions into a framework of interpretations of a certain phenomenon. This framework is iteratively tested and expanded throughout a research study.

An example on the use of grounded theory to investigate phishing is the study conducted by Michael Workman (2007), Wright (2010), and Vishwanath (2011).

b) Experimental Research

In experimental research, there are two main approaches: quasi experiments and naturalistic experiments.

i) Quasi Experiments

Quasi experiments are often used when conducting field experiments is not possible. In a quasi-phishing experiment, a closed lab study is conducted.

Lab studies are often used to measure users' ability to detect phishing. They are also called 'Phishing IQ Tests'. Participants are shown a number of email messages and websites and are asked to distinguish between phishing and legitimate ones.

The main drawback of phishing lab studies is that they use an artificial environment that differs from the real world. Security practices, for example, have rarely been the primary goal of the users, they are not tasks in themselves (Whitten & Tygar, 1999). In phishing IQ tests they clearly are the primary concern. As (Egelman & Cranor, 2010) summarise it, users do not sit down at the computer to "do security". Users deal with phishing while they are performing other activities like checking their emails, navigating through the internet, or walking in a mall if we are talking about mobile phishing. So isolating users from their daily normal activities to sit at a computer just to say which messages they believe are phishing and which are not will likely result in flawed studies.

Moreover, in a lab study, participants do not feel they are at real risk. They know they are part of a phishing study; both the data and the attack are faked. In an observation made by Whalen and Inkpen about their web security lab experiment (Egelman & Cranor, 2010), the participants did not act to protect the data as if it was their own. This means that the knowledge of the existence of the study biases the likely outcome of it (Jakobsson & Finn, 2007) and hence the users' real behaviour is not measured.

There is also a possibility that the results of phishing lab studies are affected by 'evaluation apprehension'. This refers to a special type of anxiety that arises when a subject knows he or she is being evaluated and believes the experiments are testing their abilities (Bagley, 2007).

However, phishing lab studies can play a vital role in phishing education, as the participants are introduced to different scenarios with explanation of several phishing criteria and how to detect phishing. An example of the use of such studies for educational purposes is the anti-phishing Phil game.

Phishing lab studies can also be very useful in preparing for field experiments. They can be used as a first step before conducting in-the-wild studies, as they can provide the researcher with an insight to which phishing messages can be used as phishing stimuli in field experiments.

ii)In-the-wild field studies

In this type of study, researchers simulate a real phishing attack and observe participants' behaviour towards it. In order to do so, researchers need to deceive the participants as to the real purpose of the study.

Using deception in research means that researchers deliberately withhold some of the research procedures, mainly its purpose, from the participants. They aim to avoid the biased conclusions that may result if the participants know they are participating in a phishing experiment.

Not only do these experiments measure the real response to phishing, but they can also measure the threat posed by attacks that are possible but are as yet un-witnessed in the wild and they can assess the success rates of potential countermeasures.

1.4.2 The Thesis Research Methodology

The thesis seeks to understand the psychology of SMS phishing and the factors affecting mobile users' response to phishing attacks. The existing literature lacks research about human factors in mobile phishing and has approached the subject of mobile phishing from a technological perspective. There is very limited exploration of the psychological landscape of mobile phishing and so a preliminary study was conducted to produce a set of systematically related and organized hypotheses. These hypotheses were then tested via conducting three further studies. In this section we briefly explain and justify the research methodology used for each study.

Study 1 - Preliminary Study - Personal Perception of Mobile Security

Research Method: Grounded Theory

Research into SMS security is relatively new. Most research has focused on traditional computing. The available literature about mobile computing phishing was restricted to the technological side, while research on human factors in phishing was inconclusive and contradictory. Accordingly, this study was conducted to provide an understanding of human factors in the mobile environment in general and mobile phishing in particular.

The research method used in this study is grounded theory. Grounded theory was chosen as it is suited to complex phenomena where little is known (Cairns & Cox, 2008). This was very appropriate for our research as we view the subject of mobile security as a much under-researched area that embraces complex interaction between technology and the user's way of life. In this study a set of semi-structured interviews were conducted and analysed. The study proposed a theory of three hypotheses about factors influencing mobile users' vulnerability to SMS phishing. These hypotheses led to the formulation of the thesis research questions which were tested via a further 3 studies.

Study 2- Phishing Lab Study

Research Method: Phishing IQ Test

This study was conducted to answer RQ1. The Study investigates the effect of personality traits on the ability of IT-literate individuals to correctly distinguish between phishing and legitimate mobile text messages.

The research method used in this study is phishing IQ-test. Phishing IQ is a total score derived from a phishing test designed to assess individuals' ability to detect phishing messages. The IQ test takes the form of screen shots of mobile messages which are shown to individuals to classify as either phishing or legitimate messages. Their answers are evaluated and according to the ratio of the correct answers, they are given a score.

Although these types of studies are self-report studies, which means that they provide less ecological validity than phishing experiments, they are very effective in a number of aspects. First, they provide an insight into which phishing messages are "believable" in contrast to which messages are "believed" which can be investigated via phishing experiments (Jakobsson, 2007). This can be very effective in phishing education. Second, they have an advantage over phishing experiments in regards to the number of messages that can be tested. Normally, phishing IQ tests help contrast and measure users' responses to a sequence of phishing messages, whilst only one message is normally tested via phishing experiments. For these two reasons, we have used this research method in study 2. The study results suggested certain personality traits influence phishing vulnerability. But the study also identified the most "believable" phishing messages by the study participants. We used these messages in our phishing experiments conducted via study 3 and study 4 to test which of these "believable" messages will prove to be "believed" in real life experiments. Hence the output of study 2 provided the context for both study 3 and study 4.

Study 3- Phishing Experiment with 809 Scam Simulation

Research Method: Naturalistic Experiment

This study was conducted to answer RQ1, RQ2, and RQ3. The Study investigates the effect of personality traits on the vulnerability of IT-literate individuals to respond to a phishing message purporting to be sent from their bank. Based on the results of study 2, the phishing message that deceived the mobile users most was an 809 scam. 809 scams are phishing messages that trick mobile users into dialling or texting a premium-rate number.

The research method used in this study is naturalistic phishing experiments. Naturalistic experiments are simulated phishing attacks. These types of studies are recommended in phishing research (Jakobsson, 2013) as they provide higher ecological validity than correlational studies. The reason is that in correlational phishing studies, the subjects are aware that they are participating in a phishing experiment and that their responses are being measured. Accordingly, "the knowledge of the existence of the study biases the likely outcome of the study" (Jakobsson & Finn, 2007). Therefore, its results cannot be linked to real life situations. In other words, they cannot be generalized to the real world as they are not a true representative of it.

However, in naturalistic experiments, a phishing message is sent out to a controlled sample of people. Their response to this message is then measured.

Study 4- Phishing Experiment in a University Context

Research Method: Naturalistic Experiment

This study was conducted to test RH1, RH2, and RH3. The Study investigates how personality traits of University students affect their inclination to respond to a phishing message purporting to be sent from their university. In contrast to study 3 which investigated mobile users' responses to premium-rate phishing messages, study 4 investigates mobile users' responses to phishing messages which ask them to provide confidential information. The simulated phishing message asks the students to send their date of birth and first line of address.

As with study 3, the research method used in study 4 is naturalistic phishing experiment.

The author of this thesis regards the experimental approach as the best approach to study individuals' response to phishing attacks. However, given that this approach suffers some drawbacks represented in chapter 5, this thesis will also use the correlational approach to provide context for the experimental studies.

1.5 Summary of Thesis

The thesis starts with a review of the previous research literature reported in chapter 2. In view of current research, we develop our own theoretical understanding of the psychology of phishing vulnerability. Three major studies follow, using different research approaches. The research process throughout the thesis follow the typical empirical research model illustrated in Figure 1. First, a research purpose is established. Second, a theory is generated (or used if it already exists) to frame and organize the research questions. Third, a research methodology is defined. Finally, data is collected and analysed (Shields & Rangarajan, 2013).

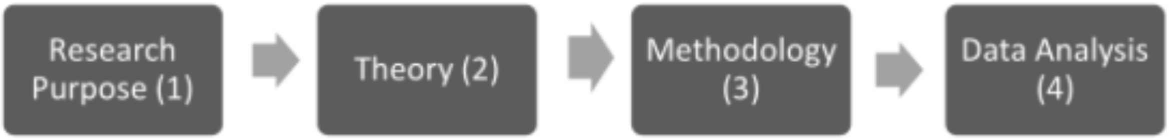


Figure 1: Empirical Research Process model (Shields & Rangarajan, 2013)

We translate the research process in **Table 1** that summarises the chapters' organization in the thesis.

Table 1: Thesis Chapters Organization

Chapter	Content of the Chapter	Research methodology
Chapter 1: Introduction	Research purpose developed	-
Chapter 2: Literature Review	Investigating previous work	Initial, exploratory foci
Chapter 3: Preliminary Study	**Study 1**: Theory development (Generating Research Hypotheses)	Correlational
Chapter 4: Phishing Lab study	**Study 2**: - Testing theory developed by Study 1. - Providing context for Study 2 & Study 3	Quasi-Experimental
Chapter 5: Phishing Experiment 1	**Study 3**: - Testing theory developed by Study 1 in context provided by study 2.	Experimental
Chapter 6: Phishing Experiment 2	**Study 4**: - Testing theory developed by Study 1 in context provided by study 2.	Experimental

The empirical studies of the thesis are summarized below.

Study 1 involves a qualitative study that aims at understanding how the security issues related to mobile phones are perceived and experienced by different mobile user groups. Based on the results of this study, a grounded theory was developed and the thesis hypotheses were generated.

Study 2 involves a lab study that investigates a user's ability to correctly distinguish between phishing and legitimate mobile text messages. This study aims at testing the first hypothesis (effect of personality traits on phishing vulnerability). The result of study 2 provided for the context of both study 3 and study 4.

Study 3 involves an experimental field study that simulates an 809 SMS phishing attack in an IT- company and measures users' responses to it. This study aims at testing the three research questions.

Study 4 involves an experimental field study that simulates an SMS phishing attack in a university environment and measures users' responses to it. This study also aims at testing the three research questions.

2 Chapter 2: Literature Review

This chapter provides a critical review of the literature conducted on human factors in SMS phishing. The aim of the literature review is to answer the following questions:

1. What do we already know in the area of mobile phishing?
2. What are the main factors affecting mobile phishing vulnerability?
3. What are the relationships between these factors?
4. What are the existing theories?
5. Where are the inconsistencies or shortcomings in our knowledge and understanding?
6. What views need to be (further) tested?
7. What evidence is lacking, inconclusive, contradictory or too limited?
8. What contribution can the present thesis be expected to make?
9. What research designs or methods seem unsatisfactory?

2.1 Search Method

This section discusses the search strategy and the selection criteria adopted for the literature review.

a) Search strategy:

Relevant research in regards to humans factors in mobile phishing was identified by searching: The usable privacy and security (https://cups.cs.cmu.edu/soups/) and ACM Special Interest Group on Computer human interaction database (www.sigchi.org/) for initial research material with key articles obtained form:

-Anti-Phishing Working Group, www.Antiphishing.org

-ACM igital library, http://dl.acm.org/

-IEEExplore digital libarray, http://ieeexplore.ieee.org/ Xplore/

-Google Scholar, http://scholar.google.com

-Springer, http://www.springerlink.com/

Conference Proceedings:

The following conference proceedings, have been also searched for research papers on the topic:

- Human Factors in Computing Systems Conference (CHI)

- British HCI

Journals:

In addition, the following journals have been manually searched for papers:

- The International Journal of Mobile Human Computer Interaction

- The International Journal of Human-Computer Studies

- The International Journal of Security Privacy and Trust Management

-Journal of Personality and Social Psychology

- Journal of Personality

Also, the references of primary resources (papers and books) were checked for any relevant studies.

In order to ensure that relevant studies were not missed, the search terms remained broad. These were "mobile security", "phishing", "human factor", “perception” anywhere in the title or abstract. Studies were eligible for consideration in this review if: (a) the focus of the study was mobile, or security; and (b) there was at least one human factor variable measured.

b) Selection criteria

In this step, a detailed examination of research papers was conducted. **Figure 2** shows the criteria upon which papers were either included or excluded to make sure the only relevant scholarly papers are included in the literature review. For the research papers investigating direct associations between personality and security behaviour, the literature review included all peer reviewed ones. In terms of sample size, both research studies which used large samples and those which used small samples were included.

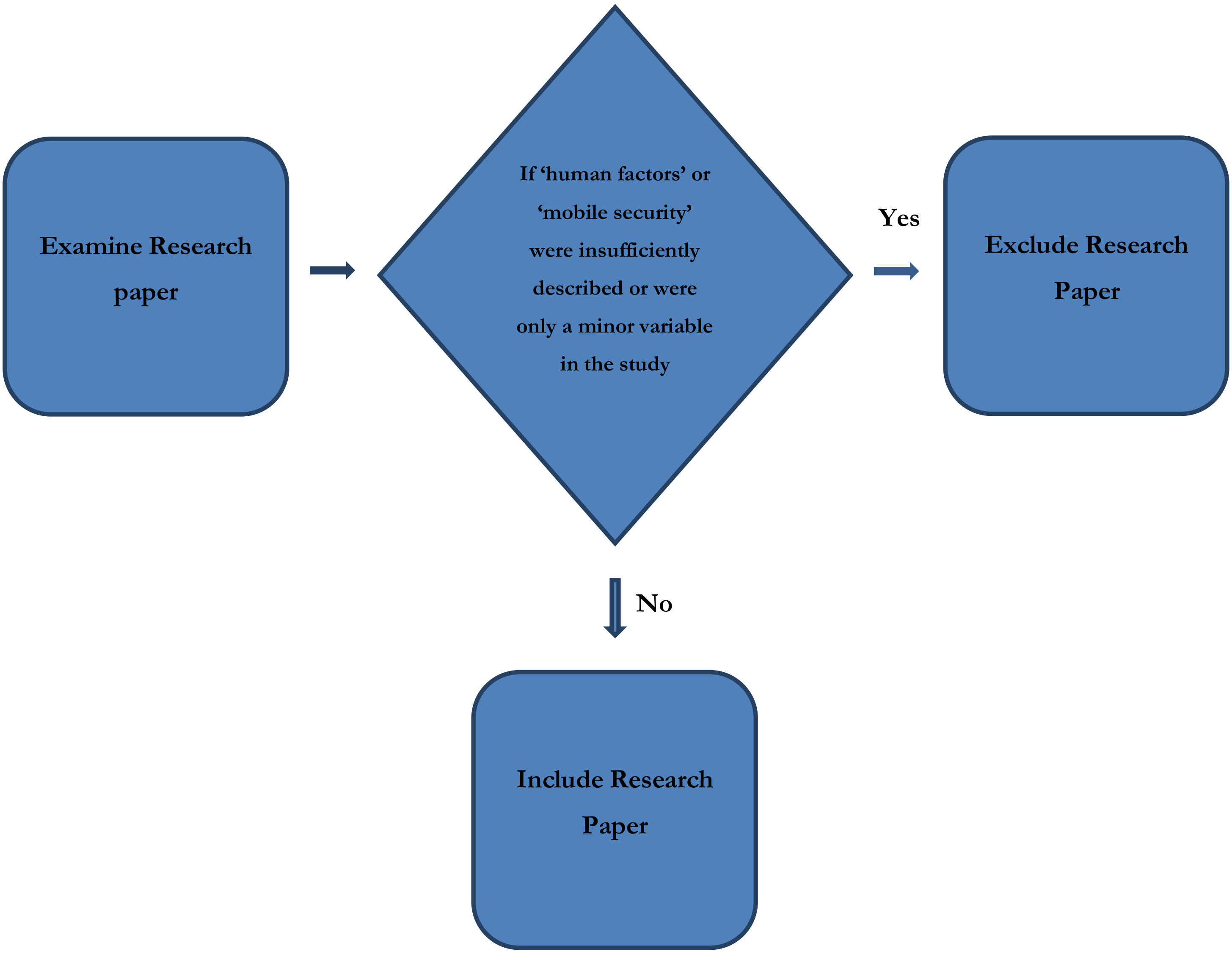

Examine Research paper
If 'human factors' or 'mobile security' were insufficiently described or were only a minor variable in the study
Yes
Exclude Research Paper
No
Include Research Paper

Figure 2: Papers' Exclusion Criteria

c) Literature Review Stages

The literature review went into three stages:

(i) Initial Literature Review: this stage motivated was by an interest in the field. It provided terminology, research resources, and topics yet explored

(ii) Exploratory Literature Review: equipped with observation and initial research questions, this stage produced specific paper references, and potential contribution areas.

(iii) Focused Literature Review: equipped with analysis and refined research questions, this stage produced the final literature review reported in this chapter.

These stages are summarised in **Figure 3** below.

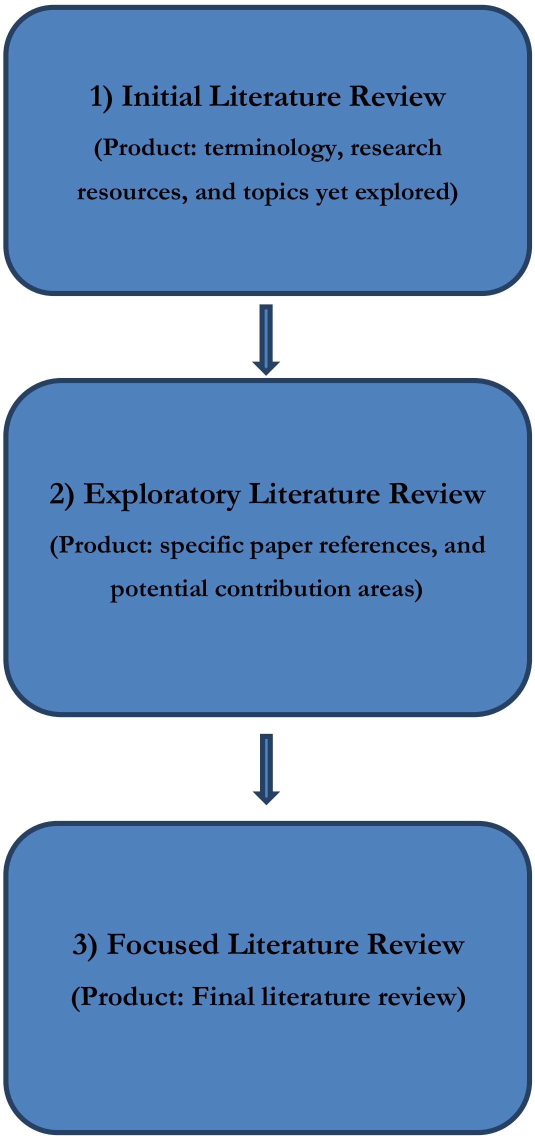

1) Initial Literature Review
(Product: terminology, research resources, and topics yet explored)
2) Exploratory Literature Review
(Product: specific paper references, and potential contribution areas)
3) Focused Literature Review
(Product: Final literature review)

Figure 3: Literature Review Stages

2.2 Background

In this section, we provide a background on behavioural aspects of security in general, before discussing phishing in particular in the following sections.

The research topic 'behavioural aspects of security' has been addressed from different views. Some research has taken the view of risk (how humans perceive risk, how they deal with risk, and the communication process in regards to situations that involve risk). Some research has taken the view of regarding security attacks as persuasion endeavours that involve deception, and hence studied methods of persuasion, how persuasive a security attack can be, and how an individual reacts to different persuasion techniques. Other research has taken the view of studying security from a decision making perspective, studying the different theories that affect human's decision making and the decision making process. We will follow this approach. In our opinion, this approach can provide us with a broader view on the topic of security vulnerability in general, and phishing vulnerability in particular. Many phishing attacks (especially new ones) will not be regarded from the users' perspective as situations that involve risk, but may be seen as making decisions under uncertainty for example. Below we discuss a number of decision making theories that we believe can help us understand how humans make security decisions.

2.2.1 Decision Making Theories

There are many theories that investigate humans' decision making process. These can be divided into three categories:

a) Motivation Theories

b) Thinking Process

c) Deciding

Below we discuss some of these theories that we believe can help us understand the decision making process in phishing.

a) Motivation Theories:

Motivation addresses 'the incentives users have to take, the appropriate action, and to do it carefully or properly' (Cranor, 2008) There are a number of theories that studied human's motivation to make a decision. We discuss two of these theories: cognitive dissonance and certainty effect.

Cognitive Dissonance:

Cognitive Dissonance is the feeling of discomfort experienced by an individual who holds two conflicting thoughts at the same time (Pfleeger & Caputo, 2012). Festinger (1965), the developer of the theory, argues that dissonance 'is a motivating factor in its own right' (p.3). He regards cognitive dissonance as an antecedent condition which leads to dissonance-reduction activity. Previous research has proposed the theory of cognitive dissonance as being central to different forms of persuasion to change beliefs, values, attitudes and behaviour, especially when the experience is related to self-image (Pfleeger & Caputo, 2012).

According to the theory, individuals who experienced discomfort situations would be more likely to change their future behaviour to avoid this dissonance in future events. This can be linked to online security victims in general and phishing victims in particular., and whether the discomfort feelings resulting from losing confidential data or getting infected by a malware, can have positive effect on these users in the future.

Certainty Effect

Uncertainty can be defined as the characterization of a future event with an unknowable outcome (Bailey, 2010). Uncertainty is different from 'risk'. While making a decision, the individual is faced with at least one option characterized by "uncertainty about uncertainty" (Khan & Sarin, 1988, p.265). Here, the distribution of the outcome probability is unknown. While, risk, can be defined as an event where possible outcomes and their given probabilities are fully known, in contrast to uncertainty event, where possible outcomes are known but their probabilities are not known (Khan & Sarin, 1988).

b) Thinking Process:

This section discusses a number of decision making theories that investigate the cognitive process of making decisions. Three theories are discussed: the Elaboration likelihood model, the model of Detection Deception, and the Availability Heuristic Model.

Elaboration likelihood model (ELM)

ELM is a general theory of attitude change. It was developed by Richard Petty and John Cacioppo (Petty & Cacioppo, 1986). It describes how attitudes are formed and persist. As we regard phishing and training against phishing as forms of persuasion, the ELM theory was suitable for our discussion as it also examines how an individual's deep thought of a message can affect its persuasiveness.

The ELM proposes that persuasion efforts can be viewed as emphasizing one of two distinct routes: the central route and the peripheral route (Petty & Cacioppo, 1986). In the accumulated literature, the central route of persuasion was believed to be more enduring than the peripheral route (Petty & Cacioppo, 1986) and hence leads to a permanent change in attitude (Pfleeger & Caputo, 2012). This central route results from an individual's careful and thoughtful consideration of the true merits of the presented information. So it is logical, conscious and requires a great deal of thought. On the other hand, the peripheral route is used when people are more driven by simple cues such as the popularity of the speaker rather than paying attention to the persuasive argument itself (Pfleeger & Caputo, 2012). In this case, any change in attitude is likely to be temporary.

For that, research has focused on means to motivate individuals to use the central route instead of the peripheral one (Petty & Cacioppo 1986). The suggestions include making the persuasive message personally relevant, using fear to make people pay attention, and offering solutions to the fear-inducing situations (Pfleeger & Caputo, 2012).

ELM was applied in different disciplines such as health care, marketing and customers' behaviour. It was used to explain how consumers process and respond to persuasive stimuli such as advertisement messages. Similarly, it was used by some researchers to explain how internet users process and respond to phishing messages (Vishwanath, Herath, Chen, wang, & Rao, 2011).

Availability Heuristic

A Heuristic can be defined as 'an approach or a shortcut that the brain takes to solve a problem' (Finkelstein, Whitehead, & Campbell, 2013, p. 80).

Availability Heuristic refers to the relationship between individuals' estimation of the likelihood of an event and the ease of recalling it. Since this theory was introduced by Tversky and Kahneman in the early 1970s, it has changed the way people look at how decisions are made. The theory basically proposes that the easier instances or associations to an event come to mind, the more likely people will expect that event to occur again (Tversky & Kahneman, 1973). It also suggests that the events that are recent, emotional, easier to imagine or vivid are more likely to be remembered than vague, difficult to imagine, or unemotional events (Finkelstein et al., 2013).

Implication for phishing research methods: According to this theory, phishing experiments are more likely to be remembered and recalled by the trainees than normal phishing training (such as: security alerts and phishing toolbars) as the field experiments have the quality of being vivid as it plays the role of a real personal experience as well as being personally relevant and emotional. The trainee will have the same time to make his own decision as in real life, without him knowing that the message is just a simulation till the trainer contacts the trainee to explain.

The Model of Detecting Deception

The Model of Detecting Deception is a model that applies the theory of deception to the field of Computer Science (Grazioli, 2004). The theory of deception, is a theory that treats deception as a cognitive process that involves examining a number of cues in the deception message. The model of detecting deception is composed of four stages: activation, hypothesis generation, hypothesis evaluation, and global assessment.

Activation: is the first stage in a decision making process, it occurs when an individual faces an unexpected situation. Then, the second stage **hypothesis generation** is activated for the individual to try to develop an explanation for the difference between the expected situation and the observed one. In order for the person to validate his hypotheses, the third stage **hypotheses evaluation** gets activated. Here the person, evaluate the hypotheses he generated to reason the situation. For example, if the individual receives a message asking him for his password, he may develop a hypothesis that evaluates the message as 'a phishing message' and in order for him to evaluate his hypotheses, he may try to contact his IT help desk to confirm. Based on his evaluation, at the end, the person reaches a decision in the **global assessment** stage, where he assesses his evaluation to make a decision.

Deciding: A number of theories studied the process of making decisions, such as the Classic Decision theory, and Bounded Rationality.

In classical decision theory decision making under uncertainty is assumed to be based on pure logic. Under this hypothesis, rational people make logical choices based on objective factors. Applying this assumption to the context of phishing, victims of phishing are often labelled as 'naïve' or 'greedy' (Alseadoon, 2014). However, these labels are unhelpful and shallow generalizations, as they imply that all people are perfectly rational decision makers, despite the fact that previous research has shown that people's decisions tend to be biased and are not purely logical (Kahneman, Slovic, & Tversky, 1982). Kahneman and Tversky (1973) have established a cognitive basis for common errors encountered by humans.

This concept of *bounded rationality* is very likely to be relevant to phishing, because of the risk involved, mainly in how risk is perceived by the users. Slovic (2000) points out that individuals' decision making process under risk is based on their perception of the risk involved and the probability of its occurrence. Applying this to phishing two individuals may receive the same phishing message with the same 'apparent' risk. One of them may take the risk depending on the assumption that his bank would be willing to pay him a refund. The other may be reluctant to take the risk because, for him, the perceived consequences are more severe. Other factors such as the financial position of individuals also play a role in calculating the risk.

Normative decision theories describe how decisions should be made, pinpointing four central processes: belief assessment, value assessment, integration and meta-cognition (Wilhelms & Reyna 2014). The first two steps are basically related to judging the perceived outcomes of a certain decision and evaluating them in terms of fulfilling one's goals. The last steps are related to combining both the assessed and the valued beliefs and comparing them to one's abilities. An important issue that can be concluded from this process is that it is difficult to judge individuals' decisions without knowing their beliefs and values.

The normative rules described in the section above are not always followed by people when they make their decisions. Instead, these rules are sometimes violated. For instance, no one can carry out all comparisons needed for purchasing an item, in order to make an ideally rational decision (Office of Fair Trade, 2012). Alternately people use 'heuristics' which are mental shortcuts that people use to make decisions and form judgements. People use heuristics to turn complex decisions into manageable ones. Usually, heuristics focus one some aspects of a problem and ignore others (Office of Fair Trade, 2012).

There is evidence that simple rules of thumb outcomes can be efficient and sometimes better than those produced using rational approach (Office of Fair Trade, 2012). However, sometimes heuristics lead to systematic deviations from rational choice. These deviations are referred to as heuristics biases or error-in-judgement. It is worth mentioning that people differ in the degree to which they display these biases.

Sources of Errors-in-Judgement

There are several sources of decision making errors which can be linked to phishing. Some of which are related to 'motivation'. Phishers often address human desires and needs. This can reduce individuals' rational processing of the phishing message content. Also, the elements of 'urgency' or 'scarcity' of phishing messages can make individuals ignore phishing cues. Dispositional factors also have an effect. As explained earlier, people with low incomes are more likely to process financial decisions differently than people with high incomes. Another source of decision errors derives from humans' tendency to seek information that confirms their initial hypotheses, as a substitute for information that may prove their hypotheses wrong. This preference for confirmatory information can considerably reduce the quality of the decision outcomes (Office of Fair Trade, 2012). This can be detected in many phishing interactions where the users ignore clear phishing cues due to their tendency to confirm one's own beliefs (Fischer, Jonas, Frey, & Kastenmüller, 2008). Another error-in-judgment source is lack of control over one's emotions. This can be related to phishing scams that offer awards and prizes for example. Self-control is a personality trait so it differs from one individual to another. Other sources of errors may include excitement seeking, reciprocation (which is used mostly in sales and is used by some phishing scams) and liking and similarities (which are used by phishers who may communicate to their victim that they are in the same financial and emotional status as him). Also, there are errors that arise as a result of lack of knowledge, over-confidence and a tendency to obey authority (Office of Fair Trade, 2012).

2.3 Introducing Human Aspects in Information Security

Information security refers to the practice of protecting information in terms of confidentiality, integrity and access (Kruger & Kearney, 2006). Humans play an essential role in this practice, in terms of human error when dealing with technology and in terms of their vulnerability to recent attacks that specifically target humans.

a) Information and Human Error

Hackers have recently moved from attacking the system to attacking the people using the systems to the extent that humans have been referred to recently as the weakest link in security (Schneier, 2000). In this section we discuss a number of human errors that can affect security. Swain and Guttman (1983) classify human errors in relation to security into five categories: 1) acts of omission, referring to the lack of certain security practice such as the failure to regularly change passwords. 2) Acts of commission, referring to wrong security practices such as sharing passwords with others. 3) Extraneous acts, referring to extra unnecessary practices. 4) Sequential acts, referring to errors resulting from performing security practices in the wrong order. 5) Time errors, referring to the failure of individuals to finish a security practice in the right time.

On other classification of security behaviour was proposed by Stanton, Stam, Mastrangelo and Jolton (2005). They classify security behaviour into 1) intentionality 2) technical expertise depicted in **Figure 4**.

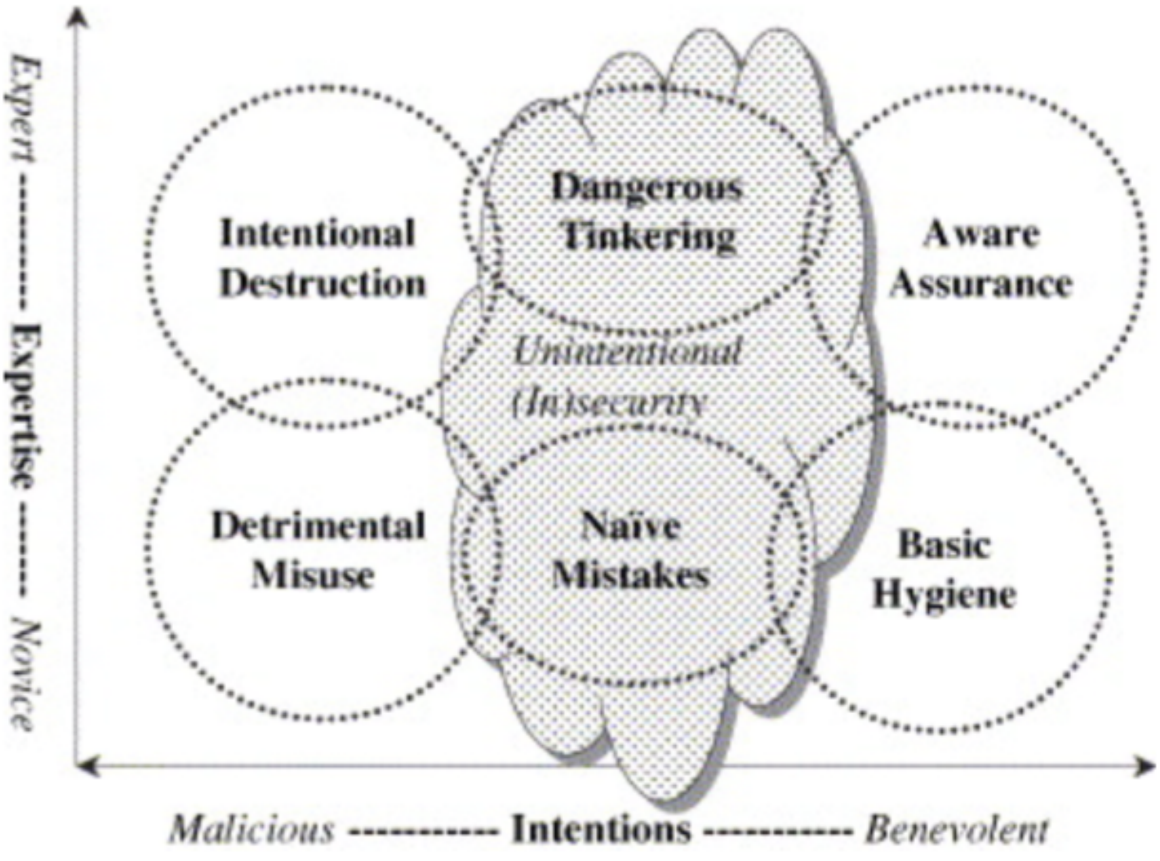

Intentional Destruction
Dangerous Tinkering
Aware Assurance
Unintentional (In)security
Detrimental Misuse
Naïve Mistakes
Basic Hygiene
Expert ------- Expertise ------- Novice
Malicious ---------- Intentions ---------- Benevolent

Figure 4: Two-Factor Taxonomy of end user security Behaviour (Stanton et al., 2005)

Malicious insiders are referred to as 'Intentional Destruction' referring to those who have both technical expertise and the intent to do harm. Detrimental Misuse refers to those who have the intent to harm, but lack technical expertise. Dangerous Tinkering refers to practices that need technical expertise, but with no intention to harm. Naïve mistakes, refers to individuals with low technical expertise and no intentions to harm. However, their practices could result in a security breach (Parsons, McCormac, Butavicius & Ferguson, 2010).

This last type of individual is the type we are most interested in, as Furnell (2005) states, the majority of human errors can be described as accidental. These types of attacks are often related to the way people interact with systems, including using and understanding them.

Norman (1981) refers to another common type of human error: capture error. Norman explains these errors as those resulting when a habitual routine takes over (or captures) an unfamiliar activity, leading to a cognitive failure or mistake (Norman, 1981). For instance, if by mistake an individual presses the button 'Entre' when they know they should not, this can be classified as a capture error, resulting from the habit of pressing 'Entre' which is very common.

Anderson (2008) discusses another type of error: post-completion errors, referring to errors that take place when a person fails to do a necessary 'tidy-up' or 'clean-up' practice that is needed after the main task/objective has been accomplished. These errors usually occur due to inattention and tiredness. An example of this is a user who writes and sends an email, but forgets to log off the system after sending his email. This may result in unauthorized people accessing the system, just because the user forgot to shut it down after completing his main task.

Related to forgetting, a number of researchers have linked 'memory' to human factors in security, building on the limited capacity of human memory and how this may lead to security errors (Besnard & Arief, 2004; Sasse, Brostoff & Weirich, 2001). For example, some users have a long list of passwords to remember, and often these passwords must comply with certain policies to confirm password strength (such as a certain length or a certain combination of characters). This can further reduce ease of remembering. So a person may try to use meaningful items that are easy to remember, such as sequence of numbers for example. As Adams and Sasse (1999) explain, choosing easy passwords, or writing down hard-to-remember passwords is a threat to security.

2.4 Phishing

According to the Oxford English Dictionary, Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online (Oxford Dictionaries, 2014). The word phishing itself originated from the word 'fishing' in a reference to catching something by bait. Where a fisherman lures a fish with a fake worm to a hook, the 'phisher' lures his victims with an impersonated communication (such as email or website) to a trap to catch their sensitive information.

In the literature, there are several definitions for phishing to the extent that there is no consensus over one certain definition. For instance, according to the definition adopted by the Anti-Phishing Working Group (APWG), phishing is "a form of online identity theft that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials" (Anti-Phishing Working Group, 2007). Jakobsson, perhaps the world's leading phishing expert, defines phishing as "a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently, retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion" (Jakobsson & Myers, 2006). The US

Department of Homeland Security defines phishing as "online identity theft in which information is obtained from an individual" (Dunham, 2008).

As the previous definitions have indicated, phishing is a form of *identity theft*. According to the Oxford English Dictionary, identity is the fact of being who or what a person or a thing is and also the characteristics determining who or what a person or thing is (Oxford Dictionaries, 2014). Stealing an identity can be carried out both online and offline. According to CIFAS (2013), identity theft and account takeover account for around two out of three frauds. The previous definitions of phishing have also indicated that phishing employs *social engineering* techniques. Social engineering is a broad concept that has been used in different domains such as politics and social sciences. However, in computer science, social engineering refers to techniques used in order to manipulate people into performing actions or divulging confidential information (Mitnick, Simon & Wozniak, 2006). Hence, social engineering mainly uses deception to gain the sort of information that is used later for impersonation to gain unauthorized access to information or resources (Kajava & Siponen, 1997).

Although the available research involves many definitions for phishing, most of these definitions do not rigorously identify the phishing attack channel (Dunham, 2008) as the medium may diverge according to the setup of the attack. Therefore, one may find phishing in several forms: email, phone calls or mobile phishing. Even in the latter alone, there are many channels over which mobile phishing attacks can be launched. Examples of mobile-targeted attacks include Bluejacking (via Bluetooth), SMishing (via short message services) or Vishing (via mobile phone calls).

2.5 Human Factors in Phishing

While the technical literature on phishing is rapidly increasing, little is known, comparatively, about the behavioural and psychological nature of such attacks. Recently, more research efforts are being directed to this area. In this section, we discuss some of these efforts. Recently, more research has been undertaken to determine how, why and in what situations individuals fall for phishing. The first step starts by investigating the phishing techniques the attackers use and then studying the individuals' responses to these techniques.

The most commonly used approach is called the bait-hook technique. Here the attacker sends unsolicited emails purporting to be from a legitimate entity. These emails represent the 'Bait' side that direct the users to a bogus website that looks like a legitimate website and where the users are asked to enter their confidential information (Wright et al., 2010). These websites are the 'Hook' side. The 'Bait' depends on exploiting certain human vulnerabilities some of which are the desire to obtain gain, avoid loss, or help others. Examples are phishing attacks that deceive the victims by presenting a false offer of a fake prize, asking the victims to donate for a phoney cause, or impersonating a legitimate entity or figure such as the victims' managers or IT-Support in order to encourage them to provide personal information such as user names and passwords. For that, attackers depend on triggering emotions such as greed, fear, heroism or obeying authorities (Halevi & Nasir, 2013). Some of these techniques have been borrowed from sales and marketing and have proved to be effective. An example of a marketing technique employed by hackers is adding the sense of urgency to the phishing message to persuade the victim that the attacker is offering a scarce opportunity that needs an immediate response (Adam & Sasse 1999).

Factors of a phishing message:

Generally, a phishing message has 3 main factors: the sender, the receiver and the phishing message itself (Lee & Song 2007, Hamar 2011). Below we discuss how these elements have been investigated in phishing research.

2.5.1 The Source Factor (The sender: 'phisher')

The phisher is a significant component of the phishing process, and in order to fully understand the phishing process, the phisher needs to be studied as well. However, because of the risks involved in interacting with phishers (as explained earlier), most phishing research focuses only on the message and receiver factors. In one of the few attempts to conduct research on the sender of phishing attacks, Jakobsson (2010) pretended to be a victim and contacted some Nigerian scammers. His research identified some characteristics of phishers. For instance, he found out that most of them use PayPal, some use Western Union and some use credit cards. He describes them as bullies who would become mean and threatening if their victims expressed second thoughts. They send angry emails and report the victim email to the payment provider. Although, these findings are rare and very important, they cannot be generalized to phishing attackers. As Jacobsson acknowledges, the scammers he contacted were interested in cameras not laptops, and were from Nigeria; this implies that they were specialized in certain kinds of items. This may indicate that the results are less likely to apply to other forms of phishing or scams. This is supported by other research investigating Nigerian scam letters (Cukier, Nesselroth, & Cody, 2007; Kienpointner, 2006). Their results concluded that Nigerian scams are of a specific and distinct nature.

Phishers behaviour can be investigated by monitoring honeypots (Li & Schmitz 2009; Gajek & Sadeghi, 2008). However, this sort of activity raises many ethical and legal issues, such as whether the researcher should warn the phishing victims or not as well as the safety of the researcher (which also applies for Jakobsson's study).

2.5.2 The Message Factor

The content of the phishing message has been studied by a sizable body of research (Dhamija, Tygar, & Hearst 2006; Downs, Holbrook, & Cranor 2006; Dong, Clark, & Jacob 2008; Rusch 1999; Jakobsson 2007; Dhamija 2006; Vishwanath et al. 2011; Downs et al. 2007).

Researchers mainly investigated why people fall for phishing by studying what is known as 'phishing cues'. According to Oxford English dictionary, a cue is defined as *'a signal for action'* and as *'a feature of something perceived that is used in the brain interpretation of the perception'* (Oxford Dictionaries, 2014). In phishing research context, phishing cues refer to the visual deception signs of the phishing stimuli that can give users an indicator that the stimuli are not authentic. In other words, these signals alert the user that the message is a phishing attempt. Examples of phishing cues include absence of legitimate logos, language errors and fake uniform resource locators (URLs).

A very well-known research investigation into phishing cues was conducted by Dhamija, Tygar and Hearst (2006). Their research is considered the first to use phishing IQ tests. The study examined users' ability to identify genuine websites and fraudulent ones from a list of websites. The study used a small number of participants (22 users). The researchers suggested that visual cues play a big role in deceiving users. This led to their participants making wrong decisions 40% of the time. They also found that browser-based cues like address bars and status bars were overlooked by users. These results were consistent with those of later research on phishing cues who also found that the users ignore the security indicators and concentrate more on the visual representation of the websites (Jakobsson 2007, Mann & Oorschot 2008, Downs et al. 2006). Security indicators can help the users assess the authenticity of the visited websites (e.g. padlock icon). However, a minority of users use them to check websites authenticity (Downs et al. 2006; Dhamija et al. 2006). Alseadon (2014) highlighted the importance of both checking the security indicators as well as understanding them. Downs et al. (2006) have found that only a minority of users know what these indicators mean. What increases the phishing risk is that some hackers exploit users' faith in browsers security indicators by faking security indicators using visual tricks (Herzberg & Jbara 2004). Examples include faking the padlock icon and the location bar.

Dong, Clark and Jacob also investigated phishing cues (Dong, Clark and Jacob, 2008). They have developed a model of the user's decision making process during phishing interaction (illustrated in **Figure 5Error! Reference source not found.**). The model identified two main areas of weakness in users' selection of cues and their interpretation of cues. So, basically, they were referring to users' insufficient selection of information to construct an accurate perception about the message and the misinterpretation of the information selected. An example of this is a user receiving a phishing message pretending to be from his bank but without the bank logo. If the user accepted that as a system problem, then the user has misinterpreted the message cues. The same applies for phishing messages that involve grammar and spelling mistakes.

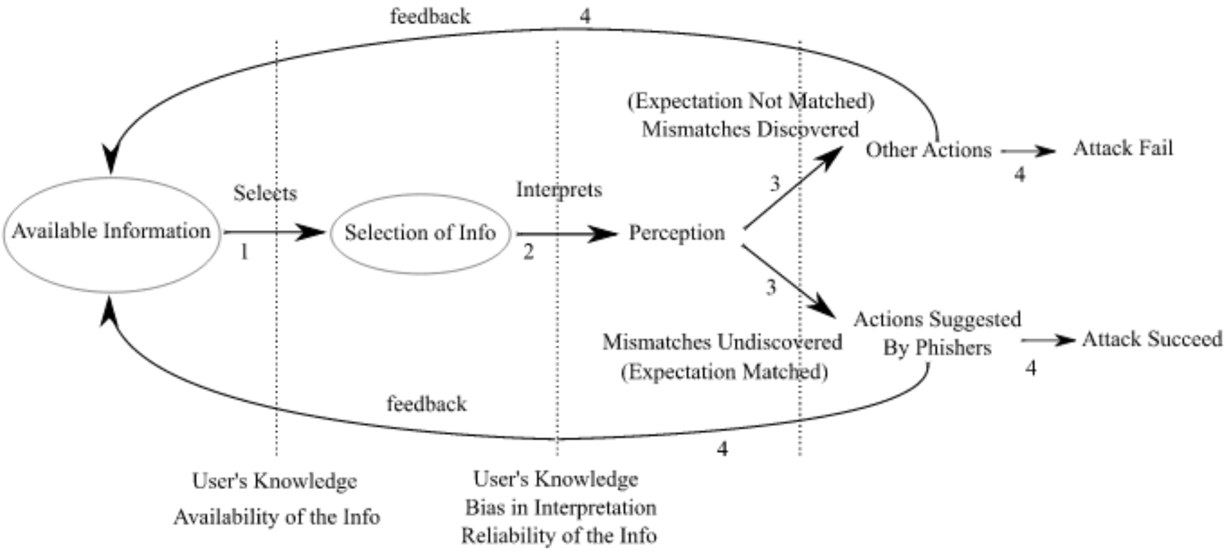


Figure 5: Decision Making Model in Phishing interaction (Dong et al., 2008)

Studying phishing messages can also help understand how they work. Understanding how phishers succeed in convincing their victims can help with protecting them. The techniques phishers use, have been referred to as 'social engineering techniques' (Rusch, 1999). An interesting investigation into these techniques classified them into three areas: emotions, attitude and belief, and persuasion and influence techniques (Rusch, 1999).

-Emotions: here, the phisher plays on the victims emotions such as excitement, fear, or a desire to help others at the beginning of an interaction (Office of Fair Trading 2009; Dhamija et al.; 2006, Rusch 1999, Al-Hamar 2010). Examples include asking for donations for natural or personal disasters or offering unique awards and prizes. Rusch (1999) argues that these sorts of attacks succeed if the victims use their 'peripheral route' to persuasion, which is superficial and emotional, instead of their 'central route', which is logical and systematic. This is consistent with a number of research studies which applied the ELM model (Petty & Cacioppo, 1986) to phishing (Xu, & Zhang 2012; Vishwanath, Herath, Chen, Wang, & Rao 2011). They agree that using their peripheral route, victims fall for phishing appearance and design.

-Attitudes and beliefs. Here Rusch (1999) suggests that the victims fall for phishing based on focusing on the apparent honesty of the message sender, without carefully analysing the content.

-Persuasion and influence techniques: here the victims are influenced by several persuasion techniques such as authority, scarcity and reciprocation (Lee et al. 2007, Rusch 1999, Office of Fair Trading 2009).

2.5.3 The Receiver Factor

The receiver of the phishing message is a very important factor in understanding phishing. Recently, more research has been undertaken to determine 'who' falls for phishing. These types of research are often referred to as vulnerability studies (Office of Fair Trade, 2009). These studies aim at discovering which groups within society are more susceptible to phishing. Some of these studies focused on demographic factors (such as age and gender), some focused on online experience such as knowledge, and technical background, and some on other individual differences such as personality. These studies are discussed in further detail in the following sections.

The receiver has been considered an important factor in the phishing process to the extent that some researchers refer to the users as the '*weakest link'* (Schneier 2000, Glick 2010, Lintovois 2013). This suggests a discussion about individual differences and their effect on users' vulnerability. Below, we discuss research conducted on individual differences in phishing.

Some researchers argue that if for every phishing message some users are 'detectors' while others are 'victims', then there must be individual factors of the users themselves that are responsible for such division (Alseadoon et al., 2012). Accordingly, a branch of research has focused on demographic differences such as age and gender (Dhamija 2006; Jagatic et al. 2007, Sheng et al. 2007, Kumaraguru et al. 2007). Another branch has focused on personality traits (Alseadoon et al 2012; Halevi et al. 2013; Moody et al. 2011).

Yet, again, there was no consensus among phishing scholars as to how individual differences affect phishing vulnerability. While some concluded that young age groups (18-25 years old) are more vulnerable (Jagatic et al. 2007, Kumaraguru et al. 2007), others' research concluded the opposite, that young people are more alert and good at detecting phishing (Mohebzada et al. 2012). The same applies to gender: females were found more susceptible then male in some studies (Sheng et al. 2007, Jagatic et al. 2007, male and female were both found to be equally deceived by phishing in other studies (Mohebzada et al., 2012), whilst the field experiment of Mohebzada revealed that 60.9% of males fell for their simulated phishing attack compared to 39.1% of females (Mohebzada et al., 2012). In their two large scale phishing experiments over around 10,000 university members, Mohebzada et al. also concluded that there is no correlation between demographics and susceptibly to phishing.

Another study of similar design was that of Wright, Chakraborty, Basoglu and Marett (2010). Their research investigated the individual factors influencing the detection of phishing emails as well as the cognitive process involved. To accomplish this goal, the researchers used Grazioli's theory of deception as their source of message cue detection. The theory proposed cues such as exaggerated claims, implausible scenarios and poor grammar and spelling. Two types of factors were of influence: experience with technology and disposition to deception; the former included computer self-efficacy, web experience and security knowledge. The latter included trust, risk perception and suspicion. The research hypotheses were tested empirically by conducting a field study among 446 undergraduate students. The study examined the students' ability to detect a phishing email asking them to reveal a security code that was assigned to each student in an earlier stage. The email pretended to be sent by an administrator in the University asking for the security code due to a problem in the system database. The results of the field study were compared to the results of a survey the students had completed earlier to measure their disposition to deception factors. A quantitative analysis has been performed followed by a qualitative study that used the theory of deception as a basis to determine how the factors studied have affected phishing detection. The study concluded that only two individual factors are dominant in the process of phishing detection: web experience and trust. Participants with relatively good web experience were able to detect inconsistent cues and those with low trust scores were more suspicious and concerned about the sensitivity of the information requested.

Although the email purporting to have been sent by an administrator in the University, neither the concept of *conformity to the views of others* nor *authority obedience* was discussed. Also, there are many concerns regarding recruiting students as research subjects. Therefore, the researchers suggested replicating the study in different setting to confirm the results.

Related research was conducted by Vishwanath, Herath, Chen, Wang and Rao (2011). The research investigates individuals' vulnerability to phishing. The theory of interpersonal deception was used as the foundation for the research. Theory of deception and Elaboration Likelihood Model (ELM) were used to help in hypotheses development which resulted in testing certain email-related factors (i.e. email source, grammar and subject urgency) and their effect on phishing vulnerability. Other non-email related factors tested included level of involvement, number of emails normally received by each participant and computer self-efficacy. Two phishing emails were sent to a sample of 321 undergraduate students. The first email asked the students to complete a web survey about their email usage. The second email asked them to verify their login details. The research concluded that attention to the urgency of the email and the subject line were more likely to positively affect participants' vulnerability to phishing than their attention to the source of the email. The research considered the contextual variables that are expected to affect individuals' phishing susceptibility indirectly by affecting their cognitive and information processing activities. The researchers self-criticized their use of students as participants and the limitation of using two, yet similar, phishing stimuli (similarity is represented in the type of information requested and level of the threat). However, the researchers overlooked discussing the limitation of using the interpersonal deception theory. The theory propositions have received a number of critics. Its components have been described as not systematically related. Its variables have been regarded as being scattered and not cohering into a meaningful framework (DePaulo, Ansfield, & Bell, 1996). Moreover, the theory was mainly developed to describe face-to-face deception, which does not apply to phishing attacks.

A related scenario-based study was that of Downs, Holbrook, and Cranor (2006). The study combined scenarios with interviews to relate phishing vulnerability to users' past history of scams exposure. The researchers found that this exposure has reduced their participants' susceptibility to fall for phishing. However, they admitted that due to the small size of the sample (20 participants), these findings are limited.

In the following year, the same researchers conducted another study with a bigger sample size of 232 participants (Downs et al., 2007). The same conclusion was reached in regards to the negative effect on their phishing vulnerability of users' past experience with the internet in general and scams in particular. Although the increase of the sample size was notable, the participants viewed only 5 images of emails. This again limits the confidence and generalisability of the study results.

The effect of personality:

The effect of Personality on phishing vulnerability has recently gained researcher attention. In a study conducted by Exeter University, socially-isolated participants tended to be more vulnerable to phishing. Some viewed the monetary scams a gamble they need to take in order to win the prize (Office of Fair Trade, 2012). They attributed their participants' behaviour to a lack of emotional control. Similar traits were studied by Halevi et al. (Halevi et al., 2013). They have studied the effect of personality traits on both Facebook activity and phishing vulnerability of 100 students of a psychology class. They used the short form personality questionnaire "NEO-IP FFM" to get quick personality measurements of their participants. The form was completed online with other information about the recruits such as their age, work experience, online activity and their emails as well. These emails were used in the experimental part of the study. Here an email was sent to the students. The email offered an Apple product to the first students to click a link in the email. The link opened a page that has a login button. Students clicking this button were considered vulnerable to phishing attacks. The personality results were compared to both the phishing experiment results and to the students' Facebook activity they provided in a survey about the type of data they post on their Facebook accounts. The study suggested that females who scored high on Neuroticism were more vulnerable to phishing scams as well as to face book addiction. Yet, no correlation to any personality traits was found. The study justifies that as women are more likely to express their emotions specially fear, which was investigated by questions that measured the recruits' personality. The author has to disagree with this as NEO-IP has been tested and validated so as gender and age factors will not affect its result. The study found a correlation between high Facebook activity and phishing vulnerability. It suggests that individuals who spend more hours on the Internet and feel comfortable on social networks, are more likely to respond to phishing attacks, as they feel comfortable on social media and are used to expressing themselves via online communication. The study also found no correlation between people's computer expertise and their ability to detect phishing emails. The study suggested that field experiments are more helpful than surveys and IQ-tests in understanding an individual's phishing susceptibility.

Chuchuen and Chavarasuth (2010) compared how individual personality traits affected responses to different phishing strategies. The study used the DISC personality model that classifies individual personality into four quadrants: Dominance, Influence, Steadiness and Conscientiousness (explained in more details later in the chapter). The study found that Influential people are more likely to fall for link manipulation attacks while people who are of 'steady' personality were more likely to fall for spear phishing attacks (Chuchuen & Chanvarasuth, 2010).

One of the studies that relate phishing to personality was that of Parrish et al. (Parrish et al. 2010). Based on the 'big five' personality framework, the study suggested a number of traits that affect individuals' susceptibility to phishing attacks. However, no central explanatory mechanism was ever described. The researchers did propose predictions for a correlation between the dependent and independent variables. Yet, these predictions were based only on their interpretations of previous literature. But this, by itself, does not qualify as a model or a theory. Simply aggregating the definitions of the traits does not give each proposed relationship the strength that their connectedness can provide. The traits were identified and classified but there was no analysis, correlational or experimental research done that act as explicatory glue that connects them together. Accordingly, their efforts fell short of a model they we could not pin down the best causal explanation of why conscientiousness, for example, may be the personality trait most negatively correlated with phishing vulnerability, as they stated. Or why giving away sensitive information can be roughly equated with extraversion. The research supports the hypothesis that extraversion leads to increased vulnerability based on two contradictory research results of Workman, in opposition to Weirich and Sasse, about the relation between sociability and passwords disclosure.

Another example of experimental phishing research is that conducted by Moody, Galletta, Walker and Dunn (2011). The researchers conducted an exploratory study where they identified candidate constructs that may act as potential drivers for phishing susceptibility. 13 constructs were selected from previous phishing literature and were then compared to another list of constructs produced by a Delphi method study. For the Delphi study, 75 graduate students were asked to produce and order reasons that may affect individuals' vulnerability to phishing attacks. Stimuli being investigated were links in emails both from known and unknown sources. The participants' answers were refined and ordered iteratively until a final ranked list was generated. This included 16 candidate reasons. Only the 12 common constructs out of the comparison between the two methods were the base the research of Moody et al. (2011) built upon. The main part of the research was an ethical phishing experiment. Individuals' personality traits and Internet experience were measured. Two phishing email versions were sent to the participants asking them to click a link in a very simple message: "check this out". The first version was sent from a known source to the participants while the second was sent from an unknown one. The study found that trust had no significant effect over phishing vulnerability. And interestingly, unfocused participants were less likely to fall for the phish.

The use of a very simple message "Check this out" helped avoid message effect confounds. However, in analysing the participants' data, no single personality framework has been used. Instead, different traits were measured, where each branched from different personality taxonomy. Using a single framework would have ensured that no repetitive measures were included.

Another study conducted by Pattinson, Jerram, Parsons, McCormac, and Butavicius (2012) used the role play method. The research investigated users' response to phishing attacks. It analysed their behaviour while interacting with both phishing and legitimate emails. 117 students accessed a web-based three-section questionnaire. In the first section, participants were shown 50 email messages (half were legitimate and half were phishing). The second section collected demographic data about the participants such as their age, gender and level of education. The third section comprised a personality test (BFI) and a cognitive reflection test (CRT). The participants were asked to detect phishing messages and describe their response to every email. Participants who scored high in extroversion trait (extroverts) and in openness trait were best at managing phishing emails. Participants with high scores in agreeableness were worst at managing legitimate emails; they treated them as phishing ones. Although the researchers discussed research methodology limitations as well as the use of students as participants, there was no mention of the BFI personality test limitations. BFI is the shortest instrument in use to measure individuals' personality. It also does not enable the researcher to measure certain traits, in relation to phishing, such as 'trust' for example. The reason is that the BFI measures only the Big Five Factors (BFF) but not their sub-category traits.

2.6 Efforts against Phishing

Parallel to research efforts to understand why people fall for phishing, there have been many efforts to combat phishing attacks from both technical and human perspectives. In the next two sections we discuss some of these efforts and how effectiveness they were.

2.6.1 Introducing technical efforts against Phishing

Several studies focused on the technical solutions of phishing (Smith & Anthony 2005, Dhamija et al. 2006, & Pattinson et al. 2012). This includes the development of automated systems or software programs that act as anti-phishing tools to help users identify spoofed websites. Examples include spam filters and URL filters. Some of these tools check URLs against reported black-listed phishing websites. However, with the increase in phishing websites, this is not an easy job. Another approach is a heuristic-based approach; here websites are filtered by using certain algorithms that are based on users' experiences. However, this approach is regarded by some researchers as 'unreliable' because it is based on the likelihood of a website being a phishing one (Zhang et al., 2007).

Some phishing-detection tools use a visual similarity approach for websites detection. Here the automated system sends a warning alert to the user if the visual similarity between websites exceeds a certain threshold. An example of these is a program developed by Liu, Deng, Hua and Fu (2006). Yet, this system requires the legitimate websites' owners to register their sites and keywords, in advance, for the system (Wright et al., 2010). Another approach has investigated the addition of anti-phishing tool bars that could be added to users' browsers to alert users of phishing websites. An example is the browser add-on, TrustBar, developed by Herzberg and Gbara to alert users from un-trusted websites via logos and warnings (Herzberg & Gbara, 2004). Example of tools that used other techniques is "trusted paths" software to help users make sure of authentication process between their browsers (Smith & Anthony 2005). Another example is CANTINA, which is a software based on TF-IDF algorithm that is used for labelling and detecting phishing websites (Zhang et al., 2007).

2.6.2 Effectiveness of Technical Efforts against Phishing

A number of studies have emerged to evaluate these automated systems (Wu et al. 2006; Anti Phishing Working Group 2007; Dhamija 2006; Cranor et al. 2007; Sheng et al. 2007; & Zhang et al. 2007). The main purpose was checking their usefulness in real world applications. Wu et al. (2006) have evaluated three anti-phishing tool bars. Their findings indicated that the toolbars were of help to only 35% of the users visiting phishing websites. The reason was that some users ignored the toolbars warnings while others did not notice them at all. However, this result changed when the authors tested pop-up warnings instead, in a follow up study. The pop-up warnings blocked access to the phishing websites unless the users countermanded them. Yet, the users were not good in interpreting the security warnings. Accordingly, the authors concluded that it is very hard for individuals to distinguish between phishing and authentic websites. A similar conclusion was suggested by (Anti Phishing Working Group 2007; & Dhamija 2006) who tested the ability of 22 users to detect phishing websites from 20 websites in the first study of this sort. They found that anti-phishing browsing cues in place were unsuccessful in alerting the participants. 68% proceeded even when they were presented with fraudulent certificates pop-up warnings. 23% of the participants ignored the status bars, address bars and all other security indicators. Good phishing websites tricked 90% of the recruits (Dhamija, 2006).

2.6.3 Training Efforts against Phishing

Another branch of research has focused on training users (Sheng 2007; Jagatic et al. 2007; & Kumaraguru 2007). Their main goal was educating users on how to detect and avoid phishing attacks. Different approaches have been applied. These included printed materials, such as books and booklets (Jakobsson, 2007), online materials (HSBC 2012; eBay 2012; Vodafone 2012; On guard online 2012), embedded training (Kumaraguru, 2007) where users are trained during their normal daily jobs via emails and pop-up messages and contextual training (Jagatic et al., 2007) where users are provided with phishing education material after a simulated phishing attack. Very few studies conducted contextual training (Jagatic et al.2007, Alseadoon et al. 2012). A problem with these sorts of training is that most of them lack demographic and background information about the participants. Figure 6 below is an example of embedded training.

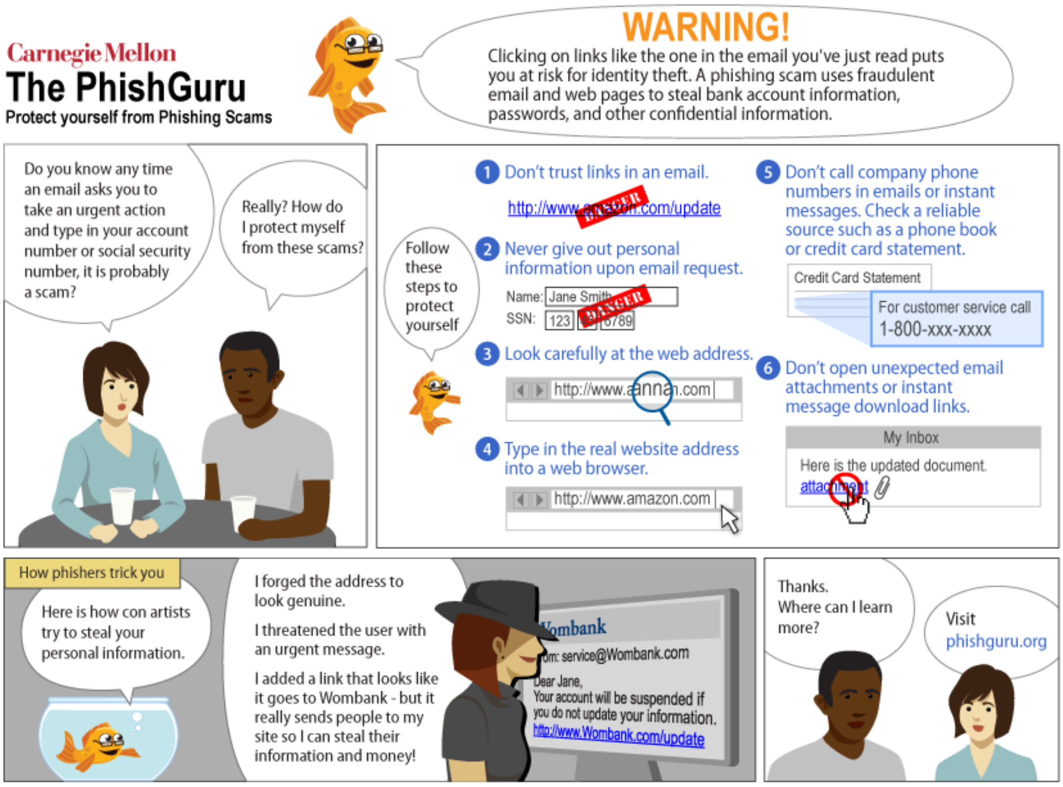

Carnegie Mellon
The PhishGuru
Protect yourself from Phishing Scams
WARNING!
Clicking on links like the one in the email you've just read puts you at risk for identity theft. A phishing scam uses fraudulent email and web pages to steal bank account information, passwords, and other confidential information.
Do you know any time an email asks you to take an urgent action and type in your account number or social security number, it is probably a scam?
Really? How do I protect myself from these scams?
Follow these steps to protect yourself
1 Don't trust links in an email.
http://www.amazon.com/update
DANGER
2 Never give out personal information upon email request.
Name: Jane Smith
SSN: 123 45 6789
DANGER
3 Look carefully at the web address.
http://www.aannan.com
4 Type in the real website address into a web browser.
http://www.amazon.com
5 Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.
Credit Card Statement
For customer service call 1-800-xxx-xxxx
6 Don't open unexpected email attachments or instant message download links.
My Inbox
Here is the updated document.
attachment
How phishers trick you
Here is how con artists try to steal your personal information.
I forged the address to look genuine.
I threatened the user with an urgent message.
I added a link that looks like it goes to Wombank - but it really sends people to my site so I can steal their information and money!
Wombank
From: service@Wombank.com
Dear Jane,
Your account will be suspended if you do not update your information.
http://www.Wombank.com/update
Thanks. Where can I learn more?
Visit phishguru.org

Figure 6: The PhishGuru: Example of Embedded Training

Traditional training, such as books and web-based material, was regarded to have limited effect (Kirlappos and Sasse 2012; & Jakobsson 2007). Recently, other untraditional methods, such as computer games (Kumaraguru, 2007), mobile games (Love, 2005) and comics (Srikwan & Jakobsson, 2008) have been introduced as innovative training approaches. An example of comic education is illustrated in Figure 7 below.

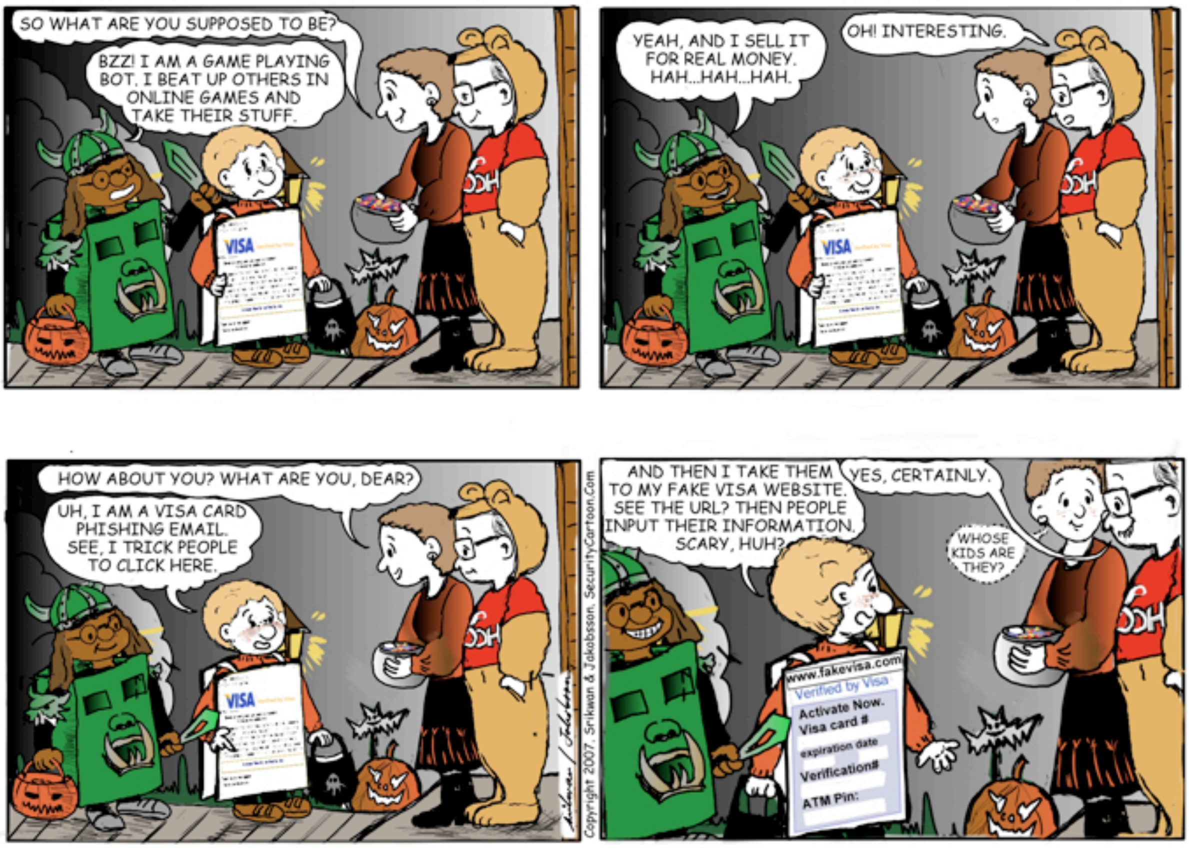

SO WHAT ARE YOU SUPPOSED TO BE?
BZZ! I AM A GAME PLAYING BOT. I BEAT UP OTHERS IN ONLINE GAMES AND TAKE THEIR STUFF.
YEAH, AND I SELL IT FOR REAL MONEY. HAH...HAH...HAH.
OH! INTERESTING.
HOW ABOUT YOU? WHAT ARE YOU, DEAR?
UH, I AM A VISA CARD PHISHING EMAIL. SEE, I TRICK PEOPLE TO CLICK HERE.
AND THEN I TAKE THEM TO MY FAKE VISA WEBSITE. SEE THE URL? THEN PEOPLE INPUT THEIR INFORMATION. SCARY, HUH?
YES, CERTAINLY.
WHOSE KIDS ARE THEY?
VISA
www.fakevisa.com
Verified by Visa
Activate Now.
Visa card #
expiration date
Verification#
ATM Pin:
SDH
Copyright 2007. Srikwan & Jakobsson. SecurityCartoon.Com

Figure 7: An Educating Phishing Cartoon (Securitycartoon.com, 2012)

2.6.4 Effectiveness of Training Efforts to Phishing

The effectiveness of training was also evaluated by many studies mostly via the use of phishing IQ-Tests (Srikwan &Jakobsson 2008; Halevi & Nasir 2013;, Sheng et al. 2007). Research was divided on the effectiveness of phishing training. While some studies stressed on the importance of continually reminding the users about the threat of phishing via training and security awareness sessions (Pattinson et al. 2012; Kumaraguru et al. 2007), other studies (Görling 2006; Sheng et al. 2007) posed doubts about the usefulness of security education. Some, such as Görling (2006), suggested that security education is limited and cannot be a general solution to security problems. Yet, this opinion was not supported by any practical studies of his; rather he formed this attitude based on a review for recent research in security education. For example, he referred to Adams & Sasse study (Adam & Sasse, 1999) to bring up discussion about weak passwords and their resulting problems and how such studies motivated research on user education and security awareness. Yet, he believes these movements had short-term effects. He demonstrated this judgment by discussing the results of Dhamija's phishing IQ-test study mentioned earlier (Dhamija, 2006). He regards it as a proof of how hard and time consuming for non-expert computer users it is to apply the training they get to scrutinize the websites they visit for phishing indicators. He also based his opinion on the fact that the study found no correlation between phishing vulnerability and factors like education, age or gender. What Görling has missed is that Dhamija study was not measuring the effect of phishing-tailored training in specific. Instead, users' general level of education and weekly hours spent on computers were the variables tested in the study in regards to 'Education'. Accordingly, we cannot generalize the results of the study or even relate it to either security training in general or phishing training in particular. It is also worth mentioning that Görling's objection is not to security education in itself, but rather in treating it as the default way to address security problems, as users themselves may not be interested in getting educated. He argues that user education alone can never protect users to a large degree. Instead, he calls for borrowing knowledge from other disciplines, especially those concerned with behavior such as HCI and Safety research. The same suggestion was adopted by Brostoff and Sasse (Brostoff & Sasse 2002).

Evaluating the same approach, Sheng et al. studies about phishing training have found positive feedback. Yet, at the same time, the training resulted in users becoming more suspicious of genuine stimuli, as most participants mistakenly rated them as phishing ones during the process of detecting phishing emails and websites (Sheng et al., 2007).

2.7 Mobile Phishing

Small size, high connectivity and mobility have led to mobile phones becoming one of the most widely used devices all over the world. Yet, these same factors have made mobile phones subject to different security threats. According to the Anti-Phishing Working Group, mobile device crimes have evolved as a result of the widespread of mobile payment and mobile banking services (APWG, 2013). It compares the rapidly advancing mobile market to the corresponding decline in PC sales. With global mobile payments predicted to exceed $1.3tn and mobile devices predicted to exceed 2m by 2015 (APWG, 2013), mobile phishing certainly requires more attention.

Although mobile devices have their own specific limitations (discussed in section 2.4), they share similar threats with fixed devices. This includes Masquerade, eavesdropping, authorization violation, loss or modification of transmitted information or sabotage (Schiller, 2003). What makes these issues need further investigation for the mobile context is the vast spread of mobile phones usage in business. More enterprises' employees rely on their mobile devices in general and on their cellular phones in particular, for running business operations. Yet, few numbers of these organizations really protect these devices. According to Muir (Muir, 2003), less than 10% of mobile devices used by major organizations, have serious protection for stored data.

2.8 Technical vulnerabilities of Mobile Phones

The small screen, the small keypad, process limitations and power restrictions are examples of the significant technical differences between traditional and mobile computing. These differences likely affect security. This is discussed briefly below.

Screen Size: The small screen means that webpage address bars are often automatically hidden to make room for other contents; a phisher can take advantage of such a vulnerability (Jakobsson, 2011). The Anti-phishing Working Group also warns that phishing is advanced via the constraints of small screens (Armin et al, 2013).

Keyboard: The small keypad of the mobile handset makes text entry time-consuming and error-prone. It also encourages mobile users to use short passwords and PINs rather than using strong passwords (Jakobsson, 2011). Also, spelling mistakes and hitting wrong buttons are more likely to occur with a small keypad or touch screen. For this reason, the Anti-Phishing Working Group argues that the usability of small devices keyboards is a serious facilitator for the success of Fraud and Phishing attacks targeting mobile users (Armin et al, 2013).

Constant Connectivity: Mobile phones are always 'on' and with the availability of 3G services, the hackers have opportunity to access the data traffic and make use of IP data traffic flat plans without the mobile users discover as no extra cost will occur (Armin et al, 2013).

Battery power: The limitations of mobile phones battery power often obstruct users from using Anti-Virus products. Accordingly, the limited battery resources of the mobile phones affect malware detection (Jakobsson, 2011).

2.9 Human vulnerabilities of Mobile phones

As for the behavioural differences, in terms of security, mobile users do not give their mobile phones the same attention and care they give their traditional computing devices. Previous research has shown that many mobile users do not understand the threats associated with their smart phone. Although they may be concerned about information privacy, few understand what this means in terms of granting permission to access certain data. This is very important nowadays specially with the introduction of quick response codes (QR), which may have hidden malware if they are not sent by a trusted source (APWG, 2013).

Another behavioural aspect is the fact that mobile phones are more strongly associated with social activities than traditional computers are (Jakobsson, 2011). In a recent study of university students that investigated phishing most of the students said they fell for the phish because it claimed to be sent by a friend (Jagatic, Johnson, Jakobsson, & Menczer, 2007).

2.9.1 Forms of Mobile Phishing

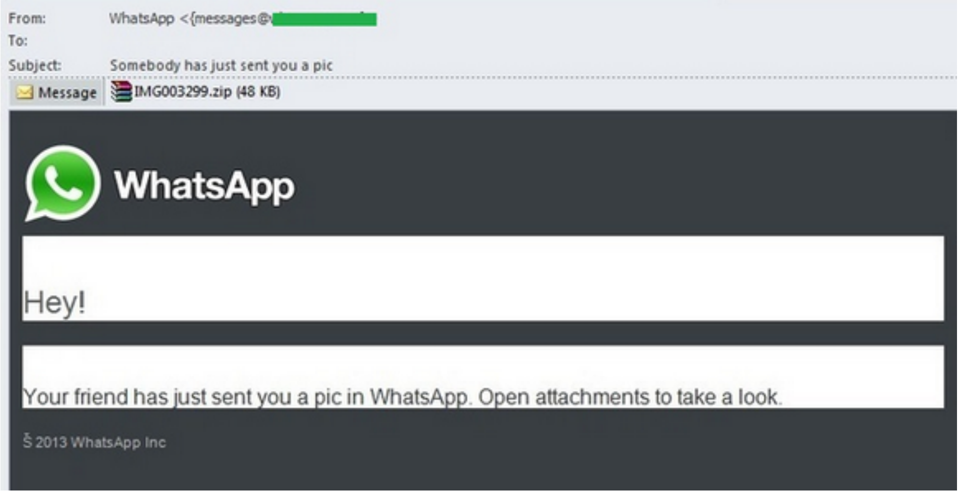
Phishing on mobile phones can take several forms, e.g. Vishing, Smishing, premium-rate numbers, mobile applications phishing, and normal mobile e-mail phishing. Examples of these forms are discussed below.

Vishing is the criminal practice of using social engineering over the telephone system seeking confidential information such as user names, passwords and banking details. It stands for Voice Phishing. It uses both e-mail messages and Voice over IP (VoIP). The attacker sends bulk e-mails that ask the e-mail receivers to call a certain number, such as that of their bank customer support. On calling the number the victims are directed to an automated system designed by the attacker. They are then asked to verify their bank security credentials. The first reported Vishing incidents took place in April 2006 (Butler, 2007).

SMishing is a form of phishing that uses mobile short message service to mount phishing attacks. It stands for SMS Phishing. Here the attacker asks for the mobile users' confidential information or resources either directly or via asking his victims to click on an SMS link (Hickey, 2006). SMishing can also spread malware. An example of this is an incident that took place in September 2006 when mass mobile messages were sent via an SMS gateway to mobile users in Spain.

Premium-Rate Telephone Numbers is a type of phishing attack where the victims are encouraged to either text or call a premium-rate number. The users are motivated by either an emergency or a fake prize. These attacks started in the United States where the attacker used numbers that started with 809 that imitated the North America numbering plan. Currently there are several variations of these numbers, but the attacks are often referred to by '809 scams' or 'premium-rate numbers attacks'.

Mobile Applications Phishing is a new channel for phishing. Due to their increased popularity recently, they have become a target for phishing attacks. Figure 8 shows an example of a mobile application phishing attempt.



From: WhatsApp <{messages@[redacted]

To:

Subject: Somebody has just sent you a pic

Message IMG003299.zip (48 KB)

Hey!

Your friend has just sent you a pic in WhatsApp. Open attachments to take a look.

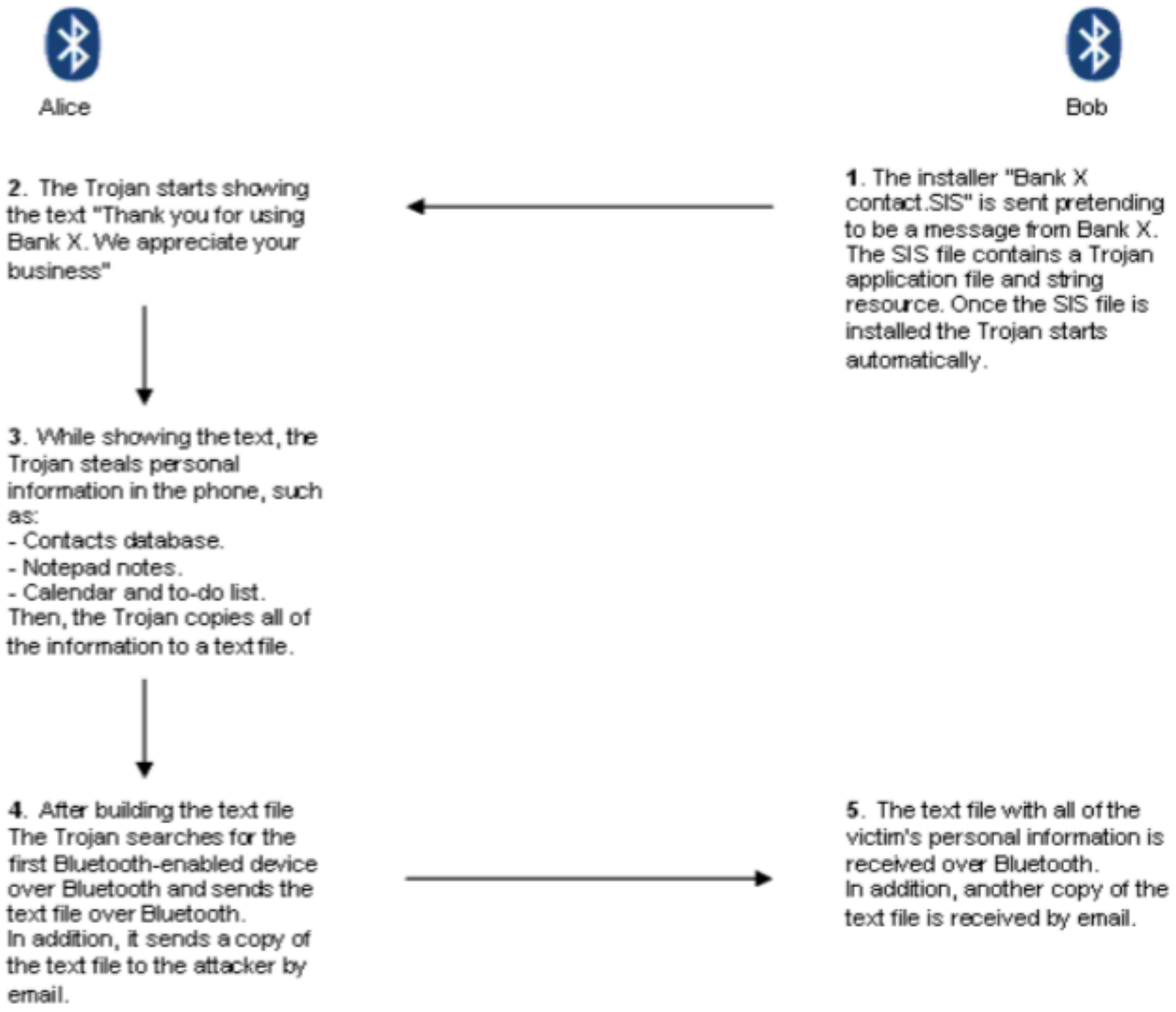
Š 2013 WhatsApp Inc

Figure 8: A WhatsApp Phishing Example (Kasperskylab, 2014)

2.9.2 How Mobile Phishing Works

Usually, the attacker sets up an automated dialling system to either call or text his victims. Sometimes these victims are either individuals from a particular region or area code, or individuals whose phone numbers are stolen from their banks or credit unions. The victims receive messages like: "There's a problem with your account," or "Your ATM card needs to be reactivated" (FBI.gov, 2014). The victims are then directed to a phone number or website where they are asked for personal information. In the case of premium-rate numbers, the victims are charged with higher prices for either texting or calling. Sometimes the victims are encouraged to click a link that downloads malicious software to their smartphone. Through this software, the attacker can access anything on the phone and even conduct financial transactions online using the victim's banking details.

Figure 9 depicts a scenario of mobile phishing using Bluetooth. Bob is an attacker who sends a file to Alice, the file purported to be from Alice's bank. However, it contains a Trojan. The Trojan accesses the personal information of Alice and sends it to Bob.



1. The installer "Bank X contact.SIS" is sent pretending to be a message from Bank X. The SIS file contains a Trojan application file and string resource. Once the SIS file is installed the Trojan starts automatically.

2. The Trojan starts showing the text "Thank you for using Bank X. We appreciate your business"

3. While showing the text, the Trojan steals personal information in the phone, such as:
- Contacts database.
- Notepad notes.
- Calendar and to-do list.

Then, the Trojan copies all of the information to a text file.

4. After building the text file The Trojan searches for the first Bluetooth-enabled device over Bluetooth and sends the text file over Bluetooth.
In addition, it sends a copy of the text file to the attacker by email.

5. The text file with all of the victim's personal information is received over Bluetooth.
In addition, another copy of the text file is received by email.

Figure 9: Bluetooth Attack Scenario

2.10 The importance of Context in Phishing

All forms of mobile phishing discussed above can be performed via context-aware phishing, generally referred to as 'spear phishing'. Spear phishing can be defined as an attack that targets a specific group at a specific time (Dunham, 2004). Three contexts are of distinct relevance to spear phishing: time, space and technology.

The time of delivery of an attack and the time of its interpretation determine whether the attack works as expected or not (Dunham, 2004). Imagine an email asking you to follow a link for electronic voting when there is no election taking place at that time. The message would certainly lose its credibility. Conversely, if a phishing message, asking the user to click a link for car accident insurance claim, is received by a person who has just had a car accident, the probability that she would trust the message is much higher.

The second context of importance to the attacker is the technological context. This context is related to the device on which the victim receives the phishing message. The type of technology used by the victims is highly correlated with the way they interact with it in terms of security. For example, one of the reasons why computer users might be deceived by phishing is their lack of understanding of the way computers work (Jakobsson, 2007). This certainly applies to all kinds of technologies the users may not feel confident in using, and smart phones are not an exception.

The third context is the space one. The spatial context denotes the physical surroundings of the victim at the time of the phishing attack. This often refers to the place at which the victim receives the phishing message but more generally concerns the situation as a whole; the overall atmosphere around the victim, the location, the activity performed, noise and even weather. A perfect example of how the location affects users' responses to phishing is a Bluetooth phishing scenario. Imagine a bank client who has just finished a transaction in his bank X. The minute he steps outside the bank he receives on his Bluetooth-enabled phone a file named 'Bank X contact.sis'. The client believes the file was sent by his bank, most probably something that has to do with the transaction he has just finished few minutes ago. The truth is that the file was sent by a phisher sitting back in his car outside the bank snarfing for clients using Bluetooth devices. The file was actually a Trojan (Dunham, 2004). Another example of spatial context is sitting in a café and connecting to the available wireless networks. One of them is named after the café itself while in fact it has nothing to do with it.

As the examples given above indicate, many of the context-aware attacks can be launched against both fixed and mobile domains. However, despite similarities of threats, traditional security solutions do not necessarily work for mobile environments (Jakobsson, 2011). Instead, both the mobile environment and the mobile users need to be studied for the to enable development of suitable solutions to address mobile platform needs. We will discuss briefly these differences both the technical and the behavioural ones.

Reflection on the Literature:

- The literature confirmed the gap in research on human factors on mobile phishing in general and SMS phishing in particular.

- Empirical research on mobile phishing is scarce and falling behind in terms of identifying underlying psychological processes.

- Research in human factors in phishing is inconclusive and contradictory (the same conclusion was reached by the University of Sydney cyber security Project, 2016). Such contradiction is represented in research about human factors in phishing, in regards to which individual factors (including personality traits, gender, age) are more likely to affect human phishing vulnerability. A similar observation holds in regards to the effectiveness of educational endeavours against phishing.

2.11 Background on personality

Personality is a form of individual difference that refers to characteristic patterns of thinking, feeling and behaving (Kazdin, 2000). Cognition, emotions and ways of behaving make every individual distinctive (APA, 2013). Revelle (2007) describes Personality as 'an abstraction used to explain consistency and coherency in an individual's pattern of affects, cognitions, desires and behaviours'. Although what a person feels, thinks, or does changes from moment to moment and from situation to situation, it still shows a patterning across situations and over time. This patterning can be used to describe, understand and even to predict a person's behaviour (Revelle, 2007).

2.12 What are personality theories?

The development of systematic ways of describing personality has been a goal for personality researchers. However, in this regard, they stand in different theoretical positions. The two main lines of personality theoretical approaches are 'Personality Traits Theory' and 'Personality Type Theory'.

The two approaches endeavour to systematically categorize individuals. Yet, they address this in different ways. The main difference between the two approaches is that the type theory classifies individuals into discrete categories according to their qualities, while the trait theory is established on the basis that all individuals share these same qualities but to differing degrees. For example, where a type theorist would argue that 'thinker' and 'emotional' are two types of people, a trait theorist would demonstrate that there is a dimension with every individual rating somewhere along this spectrum.

Below, the two theories are explained with an emphasis on the theory the thesis follows.

2.12.1 Type Theory of Personality:

The classification of personality into types is rooted back to the Greek physician Hippocrates (c. 400 B.C.) whose theory, 'The Four Temperaments' (illustrated in
Figure **10**) is believed to be the earliest known theory of personality. In his theory, Hippocrates characterized individuals on the basis of four body types, each associated with different personality characteristics:
1- The sanguine, represents optimistic and social personality type, associated with blood.
2- The choleric, represents the angry and short-tempered type, associated with yellow bile.
3- The phlegmatic, represents the peaceful and relaxed personality, associated with phlegm.
4- The melancholic, represents the sad and depressed personality type, associated with black bile (Mattew, Deary & Whiteman 2003)

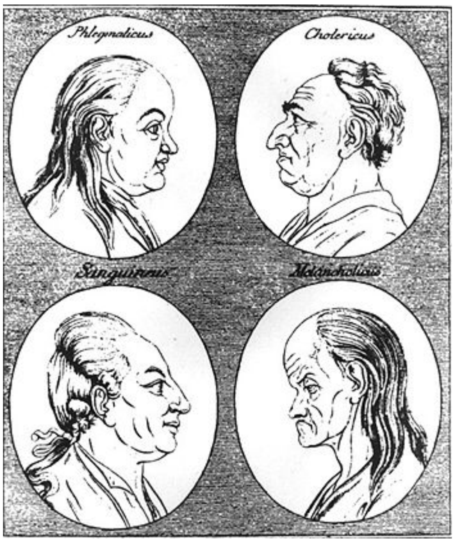


Figure 10: The Four Temperaments (Lavater, 1778)

Hippocrates' theory remained influential in Western Europe and later spread to Latin America via Spain (Foster, 1994).

Among the most influential type theories are those of William Sheldon, Carl Jung and Ernest Kretschmer. Sheldon's theory is similar to Hippocrates' system in terms of its classification of individuals according to their body types. Sheldon classified human's personality into three categories:

1- The Endomorph (heavy and easy-going)
2- The Mesomorph (muscular and aggressive)
3- The Ectomorph (thin and intellectual or artistic).

As for Kretschmer's theory, it relates body shapes with personality type and in an extreme form with vulnerability to mental illness. The classification is composed of three types:

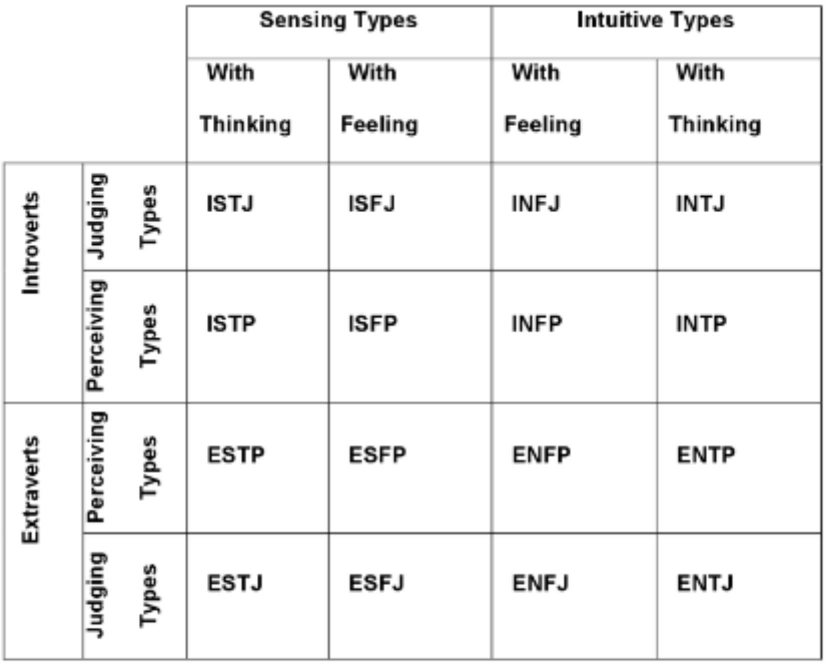
1- Pyknic type: Individuals with short and rounded body are friendly and sociable, but in extreme forms are more likely to suffer Manic Depressive Psychosis (MDP).
2- Athletic type: Individuals with slim body type are introvert and reserved, but in extreme versions of these qualities can suffer Schizophrenia.
3- Dysplastic type: Individuals whose body shape is neither rounded nor slim, but suffers hormonal unbalance. In extreme cases, their behaviour will be unbalanced.

However, this association of personality and body physique is no longer influential in the study of personality. An example of this is Carl Jung's theory that put great emphasis on psychological functions and attitudes rather than body constitution. The theory classified psychological functions into four categories: thinking, feeling, sensation, and intuition. He believed there are basically two sorts of attitude: introvert and extrovert.

From Jung's point of view, the two attitude types operate in conjunction with the four functions. Accordingly, Jung distinguished humans into eight types:

1- Introvert sensation
2- Extrovert sensation
3- Introvert intuition
4- Extrovert intuition
5- Introvert thinking
6- Extrovert thinking
7- Introvert feeling
8- Extrovert feeling

These eight personality types of Jung's theory were the roots of the 16 personality types of Myers-Briggs personality questionnaire. Myers-Briggs instrument is based on the assumption that individuals' behaviour variation that may seem random is based on certain preferences that shape their life experiences. In addition to Jung's types, Myers-Briggs (MBIT) added two factors that govern individuals' preferences. These two factors are judgement and perception. MBTI types are illustrated in Figure 11 below.



		Sensing Types		Intuitive Types	
		With Thinking	With Feeling	With Feeling	With Thinking
Introverts	Judging Types	ISTJ	ISFJ	INFJ	INTJ
	Perceiving Types	ISTP	ISFP	INFP	INTP
Extraverts	Perceiving Types	ESTP	ESFP	ENFP	ENTP
	Judging Types	ESTJ	ESFJ	ENFJ	ENTJ

Figure 11: MBIT Types (LeBlanc, 2008)

Although MBIT is widely popular in the business sector such as career counselling and professional development, it has been heavily criticized scientifically. Hence/expectedly, one of the few disciplines that do not use MTBI is Psychology (Burnett 2013). The MBTI has been totally ignored by the APA, the prestigious American Psychological Association (Pittenegr, 2011). Being ignored by the field of Psychology has been attributed to a number of reasons. Firstly, not only, does MBTI typology extract all its information from a single source, which is Carl Jung's theory, but also a number of scholars argue that typecasting people was not the aim of Jung himself (Burnett 2013, sharp 2001, Andrews 2014). For example, Sharp says:

> *"Jung did not develop his model of psychological types for this purpose. Rather than label people as this or that type, he sought simply to explain the differences between the ways we function and interact with our surroundings in order to promote a better understanding of human psychology in general, and one's own way of seeing the world in particular" (Sharp 2001:p.16).*

He also asserts that "Type tests concretize what is inherently variable, and thereby overlook the dynamic nature of the psyche" (Sharp 2001:p.18-19).

The problem is that as soon as Jung's theory has been published, his ideas have been quantified into tests and adopted by the fields of HR, job performance and training and development. MBTI is an example of that. For almost 50 years, MBTI has been used by nearly 2 Million users worldwide yearly including both jobseekers and employers. Examples of MBTI users include companies, universities and government agencies.

Nevertheless, The MBTI Foundation itself has given warning on its official website that its test should not be used as an instrument for recruitment or for assigning job activities (Myers-Briggs, 2016). Yet, in many organizations the test is compulsory to the extent that some employees are scared that they might miss a job opportunity based on their MBTI typology results (Burnett 2013 Garcia 2010).

The second reason why MBTI is not used by the Psychology discipline is that MBTI does not accommodate many of the central standards of psychological tests (Pittenger, 1993). Although MBTI is a big business that makes around 20 million dollars a year and that it is so entrenched in the business workplace, its test validity and reliability have received much criticism. Several reports have criticized its test-retest reliability (Carskadon 1977, 1979; Howes & Carskadon 1979; Stricker & Ross 1962, Kummerow 1988, Walck 1992). Also MBIT construct validity has received consistent criticism from several factor analysis studies (Sipps, Alexander, & Freidt 1985; McCrae & Costa, 1989; Saggino, Cooper, & Kline, 2001; Saggino & Kline, 1996; Sipps & DiCaudo, 1988; Stricker & Ross, 1962; Thompson & Borrello, 1986; Lorr 1991). In addition, the psychometric properties of MBTI have been also criticized for inconsistency (Caulley 2000, Pittenger 2005).

Burnett (2013) conceives that the biggest flaw in MBTI is its unduly simplified explanation of human personality. He states that "MBTI provides limited & simplified view of human personality which is a very complex and tricky concept to pin down". Grant (2013) agrees with Burnett that MBTI depends singularly on binary choices which are not mutually exclusive. For example according to MBTI, a person is either an introvert or extrovert, a thinker or feeler, there is no middle ground, despite that statistically, MBTI data is normally distributed rather than bimodal, disproving the either-or claim of MBTI (Burnett, 2013).

Nevertheless, according to recent research, individuals with strong reasoning qualities are also better at managing and understanding feelings (Côté & Miners, 2006). In this regard, Burnett (2013) enumerates several stories about employees who denounce the test and feel that it does represent their personality. Burnett attributes the firm establishment of MBTI in the human resources field to the investment and training involved. He also said the test remains popular because it is known to be popular and hence a comforting and safe choice to make Accordingly, people presumed it to be a reliable test. Hence, the test's popularity became self-fulfilling and self-preserving. The same conclusion has been reached by Pittenegr (2005) who has spent around 18 years studying MBTI describing the test as being popular because it is popular in his Psychology Consulting Journal article '*Cautionary Comments Regarding the Myers-Brigg Type Inventory".*

2.12.2 Trait Theory of Personality:

Under this theory, personality is classified into traits or dispositions. Psychologists define personality traits as styles or patterns of thinking, feeling, and behaving (McCrae & Costa 1970, Kassin 2003, Shoda & Smith 2004). These styles are usually summarized in terms of number of elements representing the principal dimensions of personality (McCrae & Costa 1970).

This approach was first adopted by Gordon Willard Allport in 1936. His trait-names guiding theory was the basis for successive trait theorists. Working with Henry S. Odbert, Allport developed a list of 18000 English words that represent personality traits. Subsequently, they shortened the list to cover around 4500 traits. Allport divided these traits into three main levels:

a) Cardinal:

Cardinal traits are on the top of the hierarchy representing key personality tendencies of individuals that are derived from genetics and early learning history of a person (Harris & Mowen, 2001). Cardinal traits shape and control an individual's behaviour and are the governing passions, such as a need for money, fame etc. It is very rare to find individuals whose personality is ruled by one trait. Instead an individual's personality comprises multiple traits.

b) Central:

Central traits are next in the hierarchy. They are the basic building blocks that shape most of humans' behaviour. They are conceived to emerge from the cardinal traits but are not as overwhelming as cardinal traits. Example of central traits would be honesty and need for cognition.

c) Secondary:

Secondary traits are the bottom of Allport's Hierarchy. These are qualities that can only be recognized in specific situations so they are not usually as noticeable or consistent as the cardinal or central traits. Examples include certain likes or dislikes.

Building on the work of Allport and Odbert, Cattell was able to produce a reduced list of traits. He shortened the 4,500 personality traits into 171 traits. He also collected different samples of life, experimental and questionnaire data. Applying factor analysis to this data, Cattell was able to generate sixteen dimensions of human personality traits. His model is known as the '16 personality factor model'. It includes:

1) Warmth
2) Reasoning
3) Emotional Stability
4) Dominance
5) Liveliness
6) Rule-Consciousness
7) Social Boldness
8) Sensitivity
9) Vigilance
10) Abstractedness
11) Privateness
12) Apprehension
13) Openness to Change
14) Self-reliance
15) Perfectionism
16) Tension

Based on his personality theory, Cattell designed the 16PF personality assessment measure. He organized these 16 personality traits into a hierarchy that is composed mainly of high and low level traits where low level traits are grouped under the high level factors which represent global common traits. At least five "common" factors were derived by factor-analysing the 16 traits (Cattell, 1995). These factors are currently known as the big-five.

The big five is the most commonly-used personality model at the moment. Along with Hans Eysenck's theory, it is considered one of the current two general trait theory approaches. Both models are discussed below.

Eysenck's theory is a personality theory that is based on physiology and genetics where biological processes result in behaviour changes (Kar, 2013). The theory is based on three dimensions:

a) Extraversion/Introversion
b) Neuroticism/ Stability
c) Psychoticism/Socialisation

What made Eysenck's theory stand out is that it provided both descriptive and causal facets of personality. Not only did Eysenck's model provide description of personality, but it also gave causal explanation for such description. For example, Eysenck explained biologically the cause of extraversion as an increased activity in the ascending reticular activating system (ARAS). Eysenck explained that ARAS stimulates the cerebral cortex. Such stimulation causes higher cortical arousal which Eysenck attributed extraversion to, where extroverts are identified by lower levels of ARAS activity than introverts (Eysenck, 1990).

In regards to Neuroticism, Eysenck attributes it to activation thresholds in the sympathetic nervous system or visceral brain (Eysenck, 1990). The visceral brain regulates emotional states such as fear and hostility. Levels of activation of the visceral brain can be measured via heart rate, blood pressure, sweating and breathing rate (Eysenck & Eysenck 1985). Eysenck explains that individuals who tend to score high in neuroticism have higher activation levels and lower thresholds in the visceral brain. So, they can become easily depressed if they encounter extremely minor stresses. On the other hand, emotionally stable individuals tend to act calmly under similar levels of stress which Eysenck has associated with their low activation levels and higher thresholds in the visceral brain ((Eysenck, 1990).

In relation to Socialisation, Eysenck explains the relation between gonadal hormones and Psychoticism. He attributed psychotic behaviour to increased levels of testosterone hormone and low levels of monoamine oxidase (MAO) enzymes.

Big Five Personality Trait Model

The Big Five Model is a taxonomy of personality traits and is comprised of five broad dimensions. The emergence history of the Big Five is unique. The Big Five model which is also called the Five Factor Model (FFM) was reached by nearly four sets of research teams working independently but formulating the same model of personality traits. The four groups of researchers were working for decades as part of systematic efforts to organize the language of personality. These four teams are:

a) Cattell
b) Tupes and Christal
c) Norman and Goldberg
d) Costa and McCrea

Although each group of these researchers took slightly different routes, they all reached the same conclusions: most human personality traits can be represented by five broad personality dimensions. This was reached using Factor analysis.

Each of the big dimensions is broad and embodies a range of more primary traits. Each big domain covers six sub factors underneath it.

The big five domains are:

A) Agreeableness
B) Conscientiousness
C) Extraversion

D) Openness

E) Neuroticism (John, Naumann, & Soto 2008)

Below, the sub factors (facets) of each domain are described as per the NEO-IP-R manual (Wendy, 2007).

A) Agreeableness: the kinds of interactions an individual prefers from compassion to tough mindedness

- Trust: belief in the sincerity and good intentions of others
- Straightforwardness: frankness in expression
- Altruism: active concern for the welfare of others
- Compliance: response to interpersonal conflict
- Modesty: tendency to play down own achievements and be humble.
- Tender-Mindedness: attitude of sympathy for others.

B) Conscientiousness: degree of organization, persistence, control and motivation in goal directed behaviour.

- Competence: belief in one's self-efficacy.
- Order: personal organization
- Dutifulness: emphasis placed on importance of fulfilling moral obligations
- Achievement Striving: need for personal achievement and sense of direction
- Self-Discipline: capacity to begin tasks and follow through to completion despite boredom or distractions.
- Deliberation: tendency to think things through before acting or speaking.

C) Extraversion: quantity and intensity of energy directed outwards into the social world

- Warmth: interest in and friendliness towards others
- Gregariousness: preference for the company of others
- Assertiveness: social ascendancy and forcefulness of expression
- Activity: pace of living
- Excitement Seeking: need for environmental stimulation
- Positive Emotions: tendency to experience positive emotions

D) Openness to Experience: the active seeking and appreciation of experiences for their own sake

- Fantasy: receptivity to the inner world of imagination

- Aesthetics: appreciation of art and beauty
- Feelings: openness to inner feelings and emotions
- Actions: openness to new experiences on a practical level
- Ideas: intellectual curiosity
- Values: readiness to re-examine own values and those of authority figures

E) Neuroticism: identifies individuals who are prone to psychological distress

- Anxiety: level of free floating anxiety
- Angry Hostility: tendency to experience anger and related states such as frustration and bitterness
- Depression: tendency to experience feelings of guilt, sadness, despondency and loneliness
- Self-Consciousness: shyness or social anxiety
- Impulsiveness: tendency to act on cravings and urges rather than reining them in and delaying gratification
- Vulnerability: general susceptibility to stress

2.13 Choice of Psychological Instruments in this Thesis

The Psychological instruments were selected after considering other instruments available to measure personality traits. This section details the rationale for choosing each instrument.

2.13.1 Choice of the Domain: The Five Factor Model (FFM)

For the purpose of better understanding human characteristics and the patterns of how individuals respond to surrounding stimuli, research has been conducted for many years to produce a taxonomy of such characteristics. After decades of research, the field of personality psychology has now achieved a consensus on a general taxonomy of personality traits: this is the Five Factor Model (FFM) (John et al. 2009, John and Srivastava 1999, Costa and McCrae 1992). The five factor model of personality assessment has bi-polar factors: Agreeableness, Conscientiousness, Extraversion, Openness, and Neuroticism (Goldberg, 1981). There is a consensus among psychometrics researchers on the use of FFM model. It has been used extensively for research. Figure 12 shows a comparison between the FFM and other personality dimensions. The figure shows how FFM model has been almost dominating personality research in the past years.

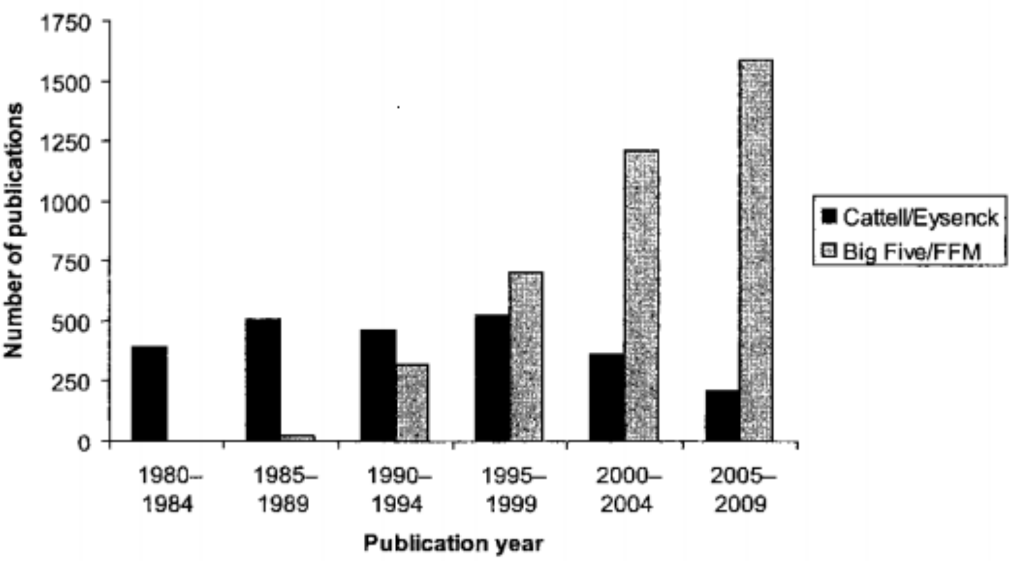


Figure 12: Comparison between usage of FFM and other trait models

2.13.2 Choice of the instrument: The International Personality Item Pool (IPIP)

Consistent with prior research in the field of personality, a survey instrument was utilized for data collection. There are a number of instruments available for the measurement of FFM such as NEO PI-R, NEO FFI, BFI, TDA, BFAS and IPIP.

In this thesis, measures for the big personality traits FFM were based on the international Personality Item Pool (Goldberg 1999, Goldberg 2006, IPIP 2013). IPIP is a scientific collaborative effort undertaken by researchers from Oregon Research Institute to provide personality measures to the public domain (Korzaan & Boswell, 2008). The rationale for selecting IPIP was mainly based on the research goal of study 3. As we were mainly keen to find the personality trait responsible for phishing vulnerability, a broad level Big Five instrument would not be of benefit to the research (as these cover only Agreeableness, Conscientiousness, Extraversion, Openness, and Neuroticism). Instead, we need to make a finer distinction of traits like trust, friendliness, altruism and cautiousness. This necessitated that we use subdomain scales such as NEO IP-R or IPIP, as they cover both the five broad domains as well as the six subdomains of each of the big five. However, the length of both scales was another essential criterion for selection. NEO IP-R is very long (240 items) compared to IPIP which is a 120 item scale. Another advantage of the IPIP scale was that it is arranged in descriptive sentences, rather than merely non-described adjectives.

Table 2 below illustrates a comparison of the instruments considered for measuring personality in the study. The selection criteria among these instruments were based on the following:

-Level of detail measured by each instrument

-Reliability of the instrument

-Language used for the instrument items

-Length of each inventory

Table 2: Comparison of the Instruments Considered for Measuring personality

Instrument	Number of items	Applicability	Rationale
NEO PI-R	240	NEO PI-R inventory was developed by Paul Costa and Jeff McCrae. It measures not only the Big Five Factors, but also six subordinate dimensions of each of those factors	Very Long Questionnaire
NEO-FFI	60	NEO-FFI was developed by Paul Costa and Jeff McCrae as a short version of NEO PI-R. It measures only the Big Five Factors.	Does not measure the Big Five subdomains.
BFI (Big Five Inventory)	44	BFI is an inventory that consists of both short phrases and adjectives. It measures only the Big Five Factors.	Does not measure the Big Five subdomains.
TDA (Trait Descriptive Adjectives)	100	TDA inventory was developed by Lew Goldberg. It consists of adjectives only. And was later reduced to 40 item Big Five mini-markers by Saucier.	The language was the problem here, as TDA uses adjectives without proper explanation. This is likely to cause misunderstanding especially with non-native English speaking participants.
BFAS (Big Five Aspect Scales)	100	BFAS inventory scores the Big Five as well as 2 subdomains of each.	Does not have any measure for the trait 'trust' which is expected to be of effect to our study of phishing.
IPIP	120	IPIP was developed by Lew Goldberg. It is structured to work as analogues to NEO PI-R scales.	IPIP measures the Big Five Factors and the subdomains of each. It uses descriptive sentences rather than merely adjectives.

Our comparison shows the reasons for which we chose IPIP. Mainly covering all the big five personality domains as well as sub-domains was the main feature for our choice. Also the adequate size of the questionnaire (120 questions) compared to either small measures (40 questions such as BFI) or very long questionnaires (200 such as Neo-PI-R). Also IPIP provides online interpretation for the results and authorized translations of the test to other languages, which was important as the questionnaire was provided in both Arabic and English languages.

3 Chapter 3: Preliminary Study-People's Perception of Mobile Security-Grounded Theory

This chapter reports the findings of an investigation that aims at formulating a theory that explains why people fall for mobile phishing. The hypotheses generated by this theory are then tested in three further studies reported in chapters 4, 5 and 6.

The nature of this study is exploratory. It aims at understanding how the security issues related to mobile phones are perceived and experienced by different mobile user groups.

3.1 Introduction

Researchers have been interested in understanding which human factors affect individuals' vulnerability to phishing and the cognitive process responsible for responding to phishing attacks. A number of scholars have referred to this type of research as the 'psychology of phishing' research (Office of fair trading 2009, Woollacott 2014, Wlasuk 2012, Dutton 2015, Schneier 2008). The British Psychological Society defines psychology as "the scientific study of human mind and behaviour: how we think, feel, act and interact individually and in groups" (BPS 2016). However, the existing literature summarized in chapter 2 has fallen short in incorporating the psychology of mobile phishing. Accordingly, an exploratory study was needed to lay the groundwork for our research on mobile phishing, and lead to further studies presented in later chapters in this thesis. Below we explain the general objective and the specific objectives of this study.

3.2 Study Objectives

3.2.1 Study Objectives Development

In this section, the development of both the general and specific objectives of the study is discussed.

a) The development of the general objective of the study:

The research presented in this thesis started with the general research question: what are the human factors that affect individuals' vulnerability to mobile phishing? The literature review suggested a number of factors such as (age, gender, education, IT literacy, training, and personality traits). However, the literature suffered from a number of drawbacks:

i) The literature on human factors in phishing was inconclusive and contradictory (University of Sydney, 2016). While a number of studies suggested that males are more likely to fall for phishing, some studies suggested no difference between male and female, and other studies suggested that females are more vulnerable. While some research suggested that young age mobile users are more vulnerable, other research suggest totally the opposite. Similarly, some studies proposed that security education can improve individuals' ability to detect phishing attacks, whereas some research suggested totally the opposite.

ii) The literature on mobile phishing was very rare and mostly focused on the technical side of the problem, such as investigating mobile websites and mobile operating systems. Human aspects in mobile phishing are almost absent from the literature.

The research community suggests that in such situations when the available literature is inconclusive or when a problem has not been clearly defined, an exploratory research is advised. Scholars regard exploratory research as 'hypothesis-generating method' that can be used to sharply define the research problem and suggest hypotheses (Shields and Rangarajan 2013, Kolter and Armstrong 2006, Glaser and Strauss 1967, Stebbins 2001, Jaeger & Halliday 1998, Mulaik 1987, Borkenau & Ostendorf 1990).

Examples of studies that followed such an approach in security research are the exploratory studies of Moody et al. (2011), Wang and Benbasat (2008), Rezgui & Marks (2008), and, Chai, Bagchi-Sen, Morrell, Rao, & Upadhyaya, S. J. (2009).

Accordingly, the general objective of this study is to acquire an insight into the phenomenon of mobile phishing in order to develop the research hypotheses that aim to answer the question: why people fall for phishing in terms of what human factors affect their behaviour towards mobile phishing attacks.

b) Specific Objectives Development:

As the main objective of the current study is to suggest research hypotheses that explain people's behaviour in response to mobile phishing attacks, it is important that the study investigates the potential drivers for such behaviour. In order to understand human's behaviour, security researchers stress the importance of understanding how people perceive security and make decisions (West, 2008); how they weigh the cost of the loss (e.g. cost of purchasing an anti-virus software) against the value of the gain (e.g. protecting one's valuable data from security breaches).

A sizable body of security researchers underscore the importance of differentiating between thinking and feeling in regards to risk perception (Gelder 2007, Schneier 2008, Severs 2012, Slovic et al. 2004, Klabach 2006, Jakobsson 2007). Modern research in cognitive psychology indicates that there are two main ways via which people evaluate risks: via 'rational analysis', or, via 'feelings' (Slovic et al. 2004).

Schneier (2011) emphasizes that "Security is both a feeling and a reality and that they are not the same". The reality of security is mathematical. It depends on using algorithms, calculating the probability of several risks and evaluating the effectiveness of available countermeasures (Schneier 2008, West 2008, Schneier 2011, Slovic et al. 2004). Hence, it uses the human's analysis system (Slovic et al. 2004). We can, for example, calculate how secure a house is, based on crime rates in the neighbourhood area, and a person's door locking habits. We can calculate the probability of a person's vulnerability to identity theft, based on some data such as his online habits.

On the other side, the 'feeling' of security does not depend on mathematical calculations of risks and countermeasures, but on the person's psychological reaction to them (Schneier, 2011). Scheneier (2011) gives an example of two people who live in the same neighbourhood, and share very similar safety habits. One of them feels that he is at high risk of burglary and lower risk of identity theft while the other feels totally the opposite.

Slovic et al. (2004) explains that by describing that feeling of security mostly depends on the human's experiential system. This system deals with risk as a feeling that tells us weather to trust certain online transaction or to confidently download a certain application. This system relies on feelings issued from images and associations linked by the person's experience to his/her past emotions (Barret & Salovery 2002, Slovic et al. 2004, Epstien 1994).

Both feelings and thoughts are essential factors in making decisions that involve risk. Recent years have seen a major change in the way psychologists view the importance of these two factors and how they interact, and how emotions are products of cognitive processes and that thought is a necessary condition of emotion (Lazarus, 1982, Campos & Sternberg 1981).

In light of that, the current study's specific objectives will investigate both thoughts and emotions in regards to mobile security, as follows:
Specific objective 1: to investigate how study's participants think of mobile phone's security issues.
Specific objective 2: to investigate how study's participants feel about mobile phone's security issues.
Specific objective 3: to investigate study's participants' previous experience of mobile phone's security issues.
Specific objective 4: to investigate study's participants' current practices of mobile phone's security.

Accordingly, the present study reports the results of a qualitative study that investigates what people think and feel about mobile security. The chapter presents this investigation temporally by means of a series of interviews performed sequentially in multiple stages.

3.3 Research Methodology

This section provides an overview of the design of the study including the data collection methodology and data analysis methodology.

3.3.1 Research Approach

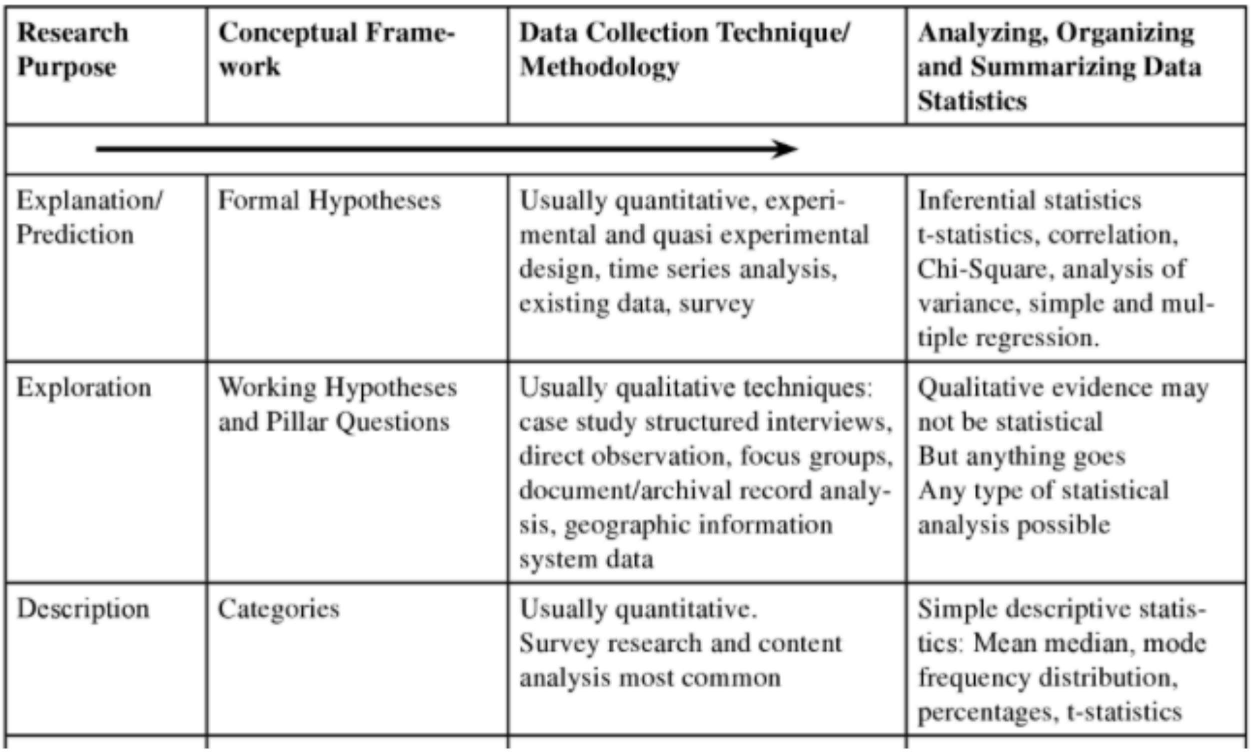
The study used a qualitative research approach. This approach was chosen based on the objective of the study and the nature of the research. As explained earlier, the main objective of this study is to *acquire an insight into the phenomenon of mobile phishing in order to develop the research hypotheses that aim to answer the question: why people fall for phishing in terms of what human factors affecting their behaviour towards mobile phishing attacks.*

Hence, this study is exploratory in nature. Shields and Rangarajan (2013) explains that exploratory research is used when a research problem has not been clearly defined. It's usually conducted before we know enough to suggest hypotheses that would explain the research phenomenon. The main purpose of exploratory research is to acquire insight and become familiar with the research topic and to collect preliminary rich quality information which will help shape the research problem, identify its main issues, and develop the research hypotheses (Kolter & Armstrong 2006).

Qualitative research methods are recommended for exploratory research (Myers 2000, Kothari 2004, Mack, Woodsong, MacQueen, Guest, & Namey 2005). Myers (2000) states that "One of the greatest strengths of the qualitative approach is the richness and depth of explorations and descriptions".

Shields and Rangarajan (2013) summarized this in their guidance table for researchers (Table 3 below). They explain that qualitative research is recommended when we seek to generate hypotheses and explore phenomena, as the second row in the table illustrates, in contrast to quantitative methods which are recommended when we seek to confirm hypotheses about the phenomena (illustrated in the first and third rows). As our main goal for this study is to develop research hypotheses, qualitative methods are most suited to our exploratory study.

Table 3: Guidance on the Selection of Research Methods (Shields & Rangarajan, 2013)



Research Purpose	Conceptual Framework	Data Collection Technique/ Methodology	Analyzing, Organizing and Summarizing Data Statistics
→			
Explanation/ Prediction	Formal Hypotheses	Usually quantitative, experimental and quasi experimental design, time series analysis, existing data, survey	Inferential statistics t-statistics, correlation, Chi-Square, analysis of variance, simple and multiple regression.
Exploration	Working Hypotheses and Pillar Questions	Usually qualitative techniques: case study structured interviews, direct observation, focus groups, document/archival record analysis, geographic information system data	Qualitative evidence may not be statistical But anything goes Any type of statistical analysis possible
Description	Categories	Usually quantitative. Survey research and content analysis most common	Simple descriptive statistics: Mean median, mode frequency distribution, percentages, t-statistics

The ultimate goal of qualitative research is to provide an illustrative overview of a phenomenon. It is designed to help in understanding and describing human experience. Qualitative research methods were initially designed to study the versatility of human aspects, e.g. motivation, understanding, feeling, perception (Shull, Singer, & Sjøberg, 2008) as these aspects are hard to quantify via quantitative methods. Quantitative methods are best used for testing theories with hypothesis that are already defined, this is done via comparing data in a systematic way. Hence, quantitative methods will not be suitable for the present study which is still in the phase of formulating a theory and understanding the research phenomena.

Qualitative methods are often used to answer the 'why' question by providing richer and more enlightening results for the researchers than quantitative methods. Given that phishing attacks, in specific, take advantage of both technical and social vulnerabilities (Jagatic, Johnson, Jakobsson, & Menczer, 2007), we found that qualitative methods are suited to our study as qualitative research lends itself to topics that involve both technical and human aspects (Buston, Parry-Jones, Livingston, Bogan, & Wood, 1998).

As the specific goals of our study (explained in section 3.1.1) are to understand how users think and feel about mobile security, qualitative research will be satisfactory for our research.

Nevertheless, we are aware of some weaknesses of qualitative research. For example, qualitative methods suffer from, being more time consuming and exhausting than quantitative methods. Qualitative data is also harder to summarize and depends to a large extent on the skills of the researcher (Kothari, 2004).

3.3.2 Data Collection

Our method of collecting data was semi-structured one-on-one face-to-face interviews. This method was chosen based on the objectives of the study. Interviews are a widespread method of collecting qualitative data. They are normally used to collect different types of data (e.g. historical data, past experiences, opinions and attitudes) (Harrell, & Bradley, 2009). Semi-structured interviews include a combination of both closed and open-ended questions, designed to extract anticipated information as well as unforeseen ones (Shull et al., 2008).

As the main objective of the study is to develop hypotheses that explain why people fall for phishing, interviews were found to be very suitable to our research. Kothari (2004) states that in-depth interviews are notably important in behavioural research where the goal is to discover the underlying motives of human behaviour. Also, interviews are recommended when we are interested in how people feel or think about a particular issue. This exactly maps with our specific objectives (explained in section 3.1.1) as our aim is to understand how users think and feel about mobile security related issues.

Other methods include the use of questionnaires and online surveys. But these methods suffer lack of interaction between the participants and the researcher. Since we aim to understand users' perception of mobile security and how far they are aware of mobile phones threats and vulnerabilities, using interviews is better suited than online surveys as interviews can help elicit users' opinions and examine their level of awareness (Sharp, Rogers, & Preece, 2007).

To some extent, the non-verbal responses and users' facial expressions helped reveal whether the participants were really aware of the security threats involved while using their mobiles or were just pretending as a result of embarrassment. Face-to-face semi structured interviews helped in following up relevant responses and in developing a second version of survey questions in later stages of the study. This reflexivity to the interviewees' answers helped in forming the grounded theory.

However, interviews suffer from some drawbacks including the researcher effect, social desirability bias and evaluation apprehension (Bagley, 2007). The researcher effect is a problem that affects the ecological validity of the results as the participants want to impress the researcher and look smarter in front of her. They claim to do something, regarding their security practices, but in reality they do something else (Field, & Hole, 2003). Here the age, gender or race of the researchers may affect the result they obtain. The social desirability bias refers to the desire of most people to present a favourable impression of themselves to other people and this may lead them to distort their answers to some questions (Eysenck, 2004). The evaluation apprehension refers to a special type of anxiety that arises when participants think the researcher is testing their abilities or evaluating their performance (Bagley, 2007). Any change in the participants' responses as a result of such belief leads to flawed studies.

As measuring the participants' awareness was of significant importance to the research, we had to mitigate these drawbacks. Measuring awareness in itself creates interesting challenges. For instance, it is important to measure what the interviewees know as well as what they do not know. This requires optimizing responses based on individuals' knowledge rather than their guessing (Ciochetto, 1995). Accordingly, it is indispensable to enhance the likelihood of having a respondent answer "don't know" when the issue is unfamiliar rather than having them make a guess.

Research in the literature has discussed this problem and has shown that respondents may even venture opinions about non-existent, fictitious issues rather than admitting that they "don't know" about the issue. This implies that unless questions regarding knowledge are structured so that respondents feel comfortable reporting a "don't know", there is a likelihood that a portion of respondents will affirm knowledge that they do not have (Bishop, Oldendick, Tuchfarber, & Bennett, 1980).

Different methods were suggested by the literature to counteract this problem. One is to frame knowledge and awareness questions in terms of *opinion questions*. Here, respondents are not asked directly if they possess specific knowledge, instead they are asked in a softer format what their opinion on the topic is. Sudman and Bradburn (1982) believed that adopting this opinion statement would increase *"do not know"* responses.

Another suggestion was the usage of *full filters* to increase the number of *'do not know'* responses. Using full filters, questions were added to first ask if the participant has an opinion on the topic and then in a separate question ask what that opinion is (Schuman, & Presser, 1996). Although this seems to encourage the participants to admit if they do not know about certain topic, in line with the goals of our study, the use of filter questions did not seem appropriate since our questions were not actually opinion questions. Instead, they were awareness ones.

We could not treat awareness questions as opinion questions. Awareness can be defined as knowledge that something exists, or understanding of a situation or subject at the present time based on information or experience (Cambridge dictionary, 2016), whereas opinion is mainly a thought, a belief, or a judgement about someone or something (Cambridge dictionary, 2016). The interview questions in discussion here are the questions under 'Mobile Awareness' section (Appendix A). We regard them as awareness questions, as they measure the users' knowledge about certain mobile security issues such as SMishing and Vishing. These questions do not ask the users about their opinion. An example is question 15 which investigates the users' awareness of the existence of mobile phone viruses. Phrasing this awareness question as opinion one, and adding a filter question in earlier stage in the interview asking the users if they have an opinion about such topics, will not be practical.

Moreover, the awareness questions were vital to the study as previous research suggested that one of the reasons that users fall for mobile security attacks in general and for mobile phishing ones in particular is their lack of awareness of possible mobile phone threats (Jakobsson 2011, Kaspersky 2015). In an Amazon survey only 32% users believe that smartphones can be subjected to attacks similar to those affecting computers. A recent study that examined level of trust in online communication, suggested that "emails are very phishy, webpages a bit, phone calls are not" (Jakobsson et al., 2007, p.5). As this suggests that users trust mobile communications, it was very important to investigate their level of knowledge about mobile security threats.

As an alternative, we decided to incorporate the encouragement into an introduction to the question. For example, the awareness question format consisted of framing the topic in terms of a question that requires a 'yes' or 'no' answer. In an attempt to encourage the interviewee to voice a *'do not know'*, if that is the case, the interviewer added an introduction that stated that not everyone has heard of some of the issues. An introduction read:

"I am going to ask you about some terms about security. Not everyone has heard about these issues. If you have not heard about any of these issues I read, feel free to tell me so."

Using this kind of introduction, we encouraged the participants to convey the truth other than pretending to be well-informed about certain security-related terms or issues.

The effectiveness of the technique we used was measured via:

a) Measuring the number of users who uttered the 'I do not know' to awareness questions.

b) Adding confirmatory questions after awareness questions. For example, if the users stated that they are aware that mobile viruses exist, the confirmatory questions ask them:

    - How they knew about mobile viruses.

    - If the user of any friend or family member has been affected by a mobile virus before.

    - How they think a mobile virus can affect their phones.

3.3.3 Interview Questions Overview

The study is conducted in the form of Face-to-face semi structured interviews. The interviews collect data on six aspects; basic computer security awareness, basic Computer security habits, basic mobile security awareness, basic mobile phone value and previous incidents. For the interviews questions See Appendix A.

Development of interviews Questions:

The interviews were divided into six sections. Every section covers certain aspect of interest to the study. The questions for these sections were selected based on the objectives of the study and on previous research about security, phishing, and, mobile security.

Corbin & Struat advise that the researchers begin the research with partial framework of local concepts in the situation they are studying. They suggest that these concepts give the researchers a beginning foothold on their research.

Studies about the psychology of security indicate that users think that they are less vulnerable to risks than others and that bad things are less likely to happen to them (Gupta 2008; Slovic, Fischhoff, & Lichtenstein, 1986; West 2008). This suggests that users are aware of possible risks and threats but still they think they are less susceptible to them. On the other hand, studies about mobile security indicates that users are not aware of security issues related to their mobile phones, and that they do not expect that their smart phones can be affected by similar threats that traditional computers are affected to (Kaspersky 2015, Jakobsson et al., 2007, Jakobsson, 2011). Accordingly, investigating the level of awareness about mobile security, and whether users treat their mobiles differently than how they treat their computers, in regards to security precautions, were essential to understanding why people fall for mobile phishing. Finally, it was necessary to understand if users put their knowledge into practice or not by asking questions about their security habits both on mobile and traditional computing platforms, to investigate if there is any difference in their security practices.

Accordingly, the interviews' questions covered areas in regards to: users' knowledge and habits in regards to both computer security and mobile security. The goal and definition of each aspect is explained below:

Basic Computer Security Awareness

Computer Security Awareness is defined here as individuals' knowledge and sufficient understanding to comply with computers' security policies. Security awareness is regarded as an important line of defence against security attacks (Al-Hamar, Dawson, & Al-Hamar, 2010). In terms of computer security awareness, this section investigated the participants' awareness of two things:

-Computer security.

-Possible computer security threats.

Basic Computer Security Habits

The second aspect of importance to the study is how users make security decisions. After measuring individuals' knowledge and understanding of computer security threats via the questions of the first aspect, it is important to do a reality check to see how users put their knowledge into practice. This section discusses users' adoption of counter-attack measures to mitigate the risk of possible computer security threats. Examples of these measures included password usage and sharing as well as anti-virus usage and updating.

Users' computer security habits are then compared to their mobile security habits in order to investigate if they regard both of equal importance.

In addition to the questions that looked into users' security experience in real life, the interviews contained questions that explored users' responses to security-related scenarios.

Basic Mobile Security Awareness and Perception

Since mobile phones' security issues are different from those related to computers, it is of great importance to understand the antecedences and consequences of users' perception to mobile information security (Ying, Dinglong, Haiyi, & Rau, 2007). The questions mainly measure mobile users' perception of risk.

This section starts with investigating the type of mobile services mostly used by the participants. In terms of mobile security awareness, this section investigated three things:
-Mobile phone security (Physical security & Information security)
-Possible mobile phones' security threats.
-Users' concerns regarding the use of certain mobile services such as Internet, Bluetooth and Short Message Service.

Additionally, the interviews discussed mobile security roles and responsibilities.

Basic Mobile Security Attitude

The aim of the mobile security attitude questions is to study everyday situations and which levels of risks individuals maintain as acceptable in regard to the security of their mobile phones. The questions investigate mobile users' Habits and strategies and the association between security measures and risky behaviour. In addition to the questions that looked into actual users' security experience in real life, the interviews contained questions that explored users' responses to possible mobile security-related scenarios.

Mobile Phone Value

The aim of mobile phone value questions is to assess the worth of the mobile phone to its owner and the significance of information stored.

Previous Incidents

The aim of previous incidents questions is to investigate the participants' security history and if they have been subjected to any security attacks.

3.4 Research Method: Grounded Theory

The research methodology used in this study is grounded theory. Grounded theory is a qualitative research method that aims at theory-building based on qualitative data gathered throughout the research (Charmaz, 2006).

Grounded theory was originally applied by Glaser and Straus (Cairns & Cox, 2008). It was initially restricted to qualitative studies then it was later used, by Corbin and Straus, for both qualitative and quantitative research (Strauss & Corbin, 1990). Accordingly, grounded theory encompasses quantitative data provided by questionnaires or experimental studies as well as qualitative data gathered via interview, focus groups or observations.

Grounded theory helps in theoretical formulation via combining systematic levels of abstractions into a framework of interpretations of a certain phenomenon. This framework is iteratively tested and expanded throughout a research study. This means that the research does not need to finish the data collection phase in order to build a theory. Instead, the theory can be developed as soon as the first segments of data are collected, even after the first interview (Cairns & Cox, 2008). Producing a tentative theory helps the researcher gather more data in regards to the confirmation and growth of his/her theory. So, the first interview may lead the researcher to an initial theory and subsequent interviews help refine and limit that theory. Each theory is iteratively tested via new interviews and questions until the theory reaches saturation. Every interview is analysed to either develop or reject previous theories. The result is a theoretical formulation of reality under investigation (Cairns & Cox, 2008).

Before going through the process itself, the rationale behind choosing such methodology will be explained. Firstly, as we view the topic of mobile phones security as a much under-researched area that embraces complex interaction between technology and the way of life, and as grounded theory methodology is suited to complex phenomena where little is known (Cairns & Cox, 2008), we believed grounded theory would be practical to our research. Secondly, we went into this research unequipped with a predefined set of hypothesis. Instead, the research started with the general research question: why do people fall for mobile phishing? Then as the available literature was found to be inconclusive (University of Sydney, 2016), this exploratory study was needed to act as a 'hypothesis-generating study' that can be used to sharply define the research problem and suggest hypotheses (explained in more details in the introduction and research method section 3.1, 3.2 and 3.3.1)

As grounded theory does not require prior hypotheses to be set in advance (Cairns & Cox, 2008), grounded theory was convenient to the research. Though, the absence of a pre-defined theory helped broadening the research and allowed the data to be tested and retested to identify any source of initial contradictions. Using grounded theory, we were able to break down the data, conceptualize it and then put it back together in new ways. Thirdly, grounded theory iterative way of research helped to identify valid and complex relationships in shorter time frames. Fourthly, grounded theory permits the concept of reflexivity and hence allowed the researcher's influence to be improved gradually as the theory was developed step by step throughout the study.

Charmaz (2006) defines Reflexivity as "the researcher's scrutiny of his or her research experience, decision and interpretations in ways that bring the researcher into the process and allow the reader to assess how and to what extent the researcher's interests, positions and assumptions influenced inquiry" (p.188). Cairns and Cox emphasized the same concept and that "the subjectivity of the researcher is an essential part of the production of an interpretation" (Cairns & Cox, 2008, p.139).

Although reflexivity is a widely accepted concept which is central to qualitative research (Lambert, Jomeen, & McSherry, 2010) it can carry potential risks to objectivity. However, it is the responsibility of the researcher to ensure integrity both in conducting the research and during the writing up (Bott, 2010). To ensure objectivity in this study, and following the guidance of Mann (2006) and Herz (1997), reflexivity was regarded in this research as a means of involving the researcher's active interpretations of experiences in the field. The researcher was keen to make a balance between using her experience to impact on how she tells the stories of others and distancing herself from the collected data.

Establishing rigour and objectivity in qualitative research has been referred to as trustworthiness.
Below, are the strategies employed by the researcher to ensure objectivity via trustworthiness.

Table 4: Strategies to Ensure Objectivity in the Research

What scholars recommend	How the researcher applied it
Miles and Huberman (1994) recommend that methods adopted and decisions made should be acknowledged within the research report as well as the reasons for favouring a certain approach over the other.	-The researcher explained in details the research approach in section 3.3.1 -The selection of the research method and the reason for favouring a certain approach was reported in **Table 3**. - The rational for choosing a certain personality instrument was reported in section 2.13.2 -To ensure that it was the participants views that were reported rather than the researcher's point of view, a standard personality test (IPIP) was used.
Shenton (2004) recommended 'Triangulation' as a powerful technique that facilitates validation of data through cross verification from two or more sources. Bogdan and Biklen (2006) defines triangulation as the application and combination of several research methods in the study of the same phenomenon. Shenton (2004) explains that triangulation can be performed in several forms such as research methods, and data sources triangulation.	-Research Methods triangulation: The data collected via the interviews in the main study was supported via the use of a personality instrument (IPIP) in the face value study to help explain the attitude and the behaviour of the participants as well as to verify particular details the participants supplied in the interviews. - Data Sources triangulation: The study involved a diverse range of participants (such as: Undergraduate students, postgraduate students, IT and non-IT employees and housewives). This helped make sure that individuals viewpoints and experiences can be verified against others, so that a rich picture of the behaviour of the participants can be constructed based on the contributions of a range of people. Also the sample covered different nationalities which helped reduce the effect on the study of particular factors distinctive to a certain country.
Shields and Rangarajan (2013) recommended that participants should be able to contribute their ideas and experiences without the fear of losing credibility in the eyes of the investigator.	-The researcher has put in place measures to reduce the 'researcher effect' to a minimum (reported in page 62-63).

Bott (2010) and Shenton (2004) recommended to make it clear to the participants that they can withdraw from the study at any point of time.	-The researcher explained to the participants that they have the right to withdraw from the research any time. This is also reported in the participants' consent form (appendix A).
Shenton (2004) recommended to highlight the independent status of the researcher to the participants, so that they can provide their opinions frankly.	The researcher emphasised her independent status to the participants and after the interviews she sent them the draft of their answers so that they confirm that the researcher's interpretations reflects their answers. None of the participants had any objection about the reported interviews.
Katsirikou and Skiadas (2012) and Shenton (2004) recommended frequent discussions with someone who is responsible for the work in a more supervisory capacity can help draw the attention of the researcher to any flaws. He suggests that such discussions can also help the investigators to recognise their own biases and preferences.	-Frequent debriefing sessions took place between the research and her supervisor. These sessions involved discussions of the interviews and provides the researcher an opportunity to test her developing ideas and interpretations as well as watching against any biases.

Reflecting on that, the research presented in this study has gone into three types of cycles of data gathering, analysis and theorizing. These cycles stopped, when the theory reached saturation. Three signs indicated such saturation. First, each new item of data was fitting into existing theory. Second, the theory rightly was justifying the data. And third, the theory was successfully engaged in different types of mobile security-related interaction such as Internet browsing, mobile authentication and phishing attempts handling.

3.4.1 Sample

The sample included 15 participants: 4 housewives, 5 non Computer Science undergraduate students and 6 Computer Science Postgraduate students.

Sampling Procedures

The process through which the interviewees were selected was theoretical sampling. In theoretical sampling, the required participants are deliberately chosen (Cairns & Cox, 2008). The reason for using such sampling technique is that our interest was not to cover all possible variations as much as proving or refuting any tentative theories built throughout the study. The grounded theory needed to be tested at all times. Hence, we had to choose the sample knowingly to test each theory. The whole process was iterative, thus it was validated by continual comparisons with the raw data. When gaps were identified in the framework, they were filled by further investigation using theoretical sampling.

Regarding the sample size, 15 mobile users were interviewed. We are quite aware there has been a debate among the HCI community regarding the ideal sampling size. While some researchers encourage using large size samples, others led by Nielson (2012) support the small size of between five and ten participants.

Since the appropriate sample size is the one that adequately leads to comprehensive interpretation of the studied phenomena (Marshall, 1996), and as generalization was not the goal of our investigation, we considered interviewing 15 participants would be sufficient. This number was not decided in advance, on the contrary, as our methodology was grounded theory, one interview after another was conducted until we felt that our theory had reached saturation then we discontinued our interviewing process.

The sample selection had three phases. In the first phase, the initial interviews suggested that a disturbing history of security-related incidents is a candidate variable of importance to the study, I was keen to gather data with view to validating and expanding the theory. Further analysis recommended interviewing users with different levels of security awareness. Hence, the sample, in the second phase, included people with little to average levels of knowledge, such as housewives and undergraduate students, and people with high knowledge level, represented by Computer Science postgraduate students and university staff of the security group in a Computer Science department.

The sample included both male and female participants. Being over the age of 18 and being a UK mobile phone user for at least 1 year at the start of the study were the prerequisite factors for selecting the participants. The reason for this is to make sure that the participants are familiar with of mobile phones different features (such as text messages) and also that they are aware of some service providers in the UK who were mentioned in the interviews such as banks and gas and electricity companies.

Accordingly, the research does not investigate novice users' vulnerability to cyber security attacks, and this can be studied in future research, as recommended in section 7.6

3.5 Data Analysis Process

This section discusses the process of analysing the data produced by the interviews. For our grounded theory, iterative theorizing has been used which means that the research went into three cycles of data gathering, analysis and theorizing. Throughout the study, constant comparative analysis was employed and any evident gaps or inconsistencies that emerged were then addressed by further data collection via theoretical sampling. These steps were repeated until conceptual saturation is confirmed.

We employed three-stage analysis of the collected and transcribed data; open coding, axial coding and selective coding.

3.5.1 Open Coding

The first step in the grounded theory study is coding. Coding involves labeling segments of data with a short name that sums up and justifies each piece of data (Charmaz, 2006). Fragments of data including actions, interactions and incidents, which are conceptually similar, are joined together into *"categories"*. This type of coding is open because there are no predetermined codes set in advance (Cox & Cairns, 2008). Instead, the researcher is always open to all possible theoretical directions designated by the empirical data.

In open coding phase, we identified meanings and actions in the interviews' transcripts data. Coding helped in moving beyond concrete statements of the participants to analytical interpretations. Using constant comparative analysis, we compared the data with the categories to ensure consistency in the coding process. If new segments of data did not fit into the developed categories, a new category was created. The open coding stage was finished when there were no new categories emerging from the data. Table 5 below shows a random sample of our codes which demonstrates meanings and actions in the participants' data. The codes in this table are initial codes so they stick closely to the data, show actions and provide explanation. Our qualitative codes show how we selected, separated and sorted data in segments to develop abstract ideas.

Table 5: Open Codes

Codes
Remembering past upsetting security problems.
Having insurance for mobile handsets.
Backing up mobile data.
Updating mobile antivirus frequently.
Getting mobile phone stolen
Mobile loss in transportation
Personal computer was infected by virus
Virus infection occurred directly after anti-virus expiration.
Upgrading anti-virus regularly.
Scanning entire computer.
Behaving more securely.
Having no anti-virus.
Having no password for laptops.
Having no password for mobiles.
Taking no backup of personal data.
Having password only for computers at work.
Having no password for computers at home.
Depending on technical support team.
Tendency to respond to Vishing attacks.
Tendency to respond to SMishing attacks.
Tendency to give away mobile PIN to mobile customer support team.
Tendency to trust mobile phishing messages by 70-100% level of trust.
Selecting anti-virus software that is free.
Selecting anti-virus software already downloaded on the device.
Selecting anti-virus software according to its efficiency.
Understanding that mobiles are not that much different from computers.
Understanding mobile handsets shortage of computational power.
Understanding mobile handsets shortage of energy.
Understanding mobile handsets weak encryption algorithms.
Understanding that SMS is not encrypted while being transmitted.
Understanding that acquiring special devices, the SMS can be read on the way.
Feeling confident to deal with security problems of their mobile phones.

3.5.2 Axial Coding

The second step in the analysis was conducting axial coding. In this stage, our aim was finding connections that relate the categories that emerged from open coding together in order to form and develop the theory. These relationships served as a guide to trigger gathering further data for analysis via theoretical sampling. To give coherence to the emerging analysis, we mainly looked for:

Categories that represent a core phenomenon.

Causal conditions (causes of the phenomenon).

Strategies (actions of the participants).

Consequences (outcome of these strategies).

For that we followed the model introduced by Strauss and Corbin (1990):

Causal conditions=> core phenomenon => context => strategies =>consequences

Table 6,

Table 7, and **Table 8** below show a sample of our codes which demonstrates causal conditions in the participants' data. The causal conditions demonstrated in the table are the user's history and previous experience, individual differences, and security awareness respectively.

Table 6: Sample of Axial Coding (History and previous Experiences)

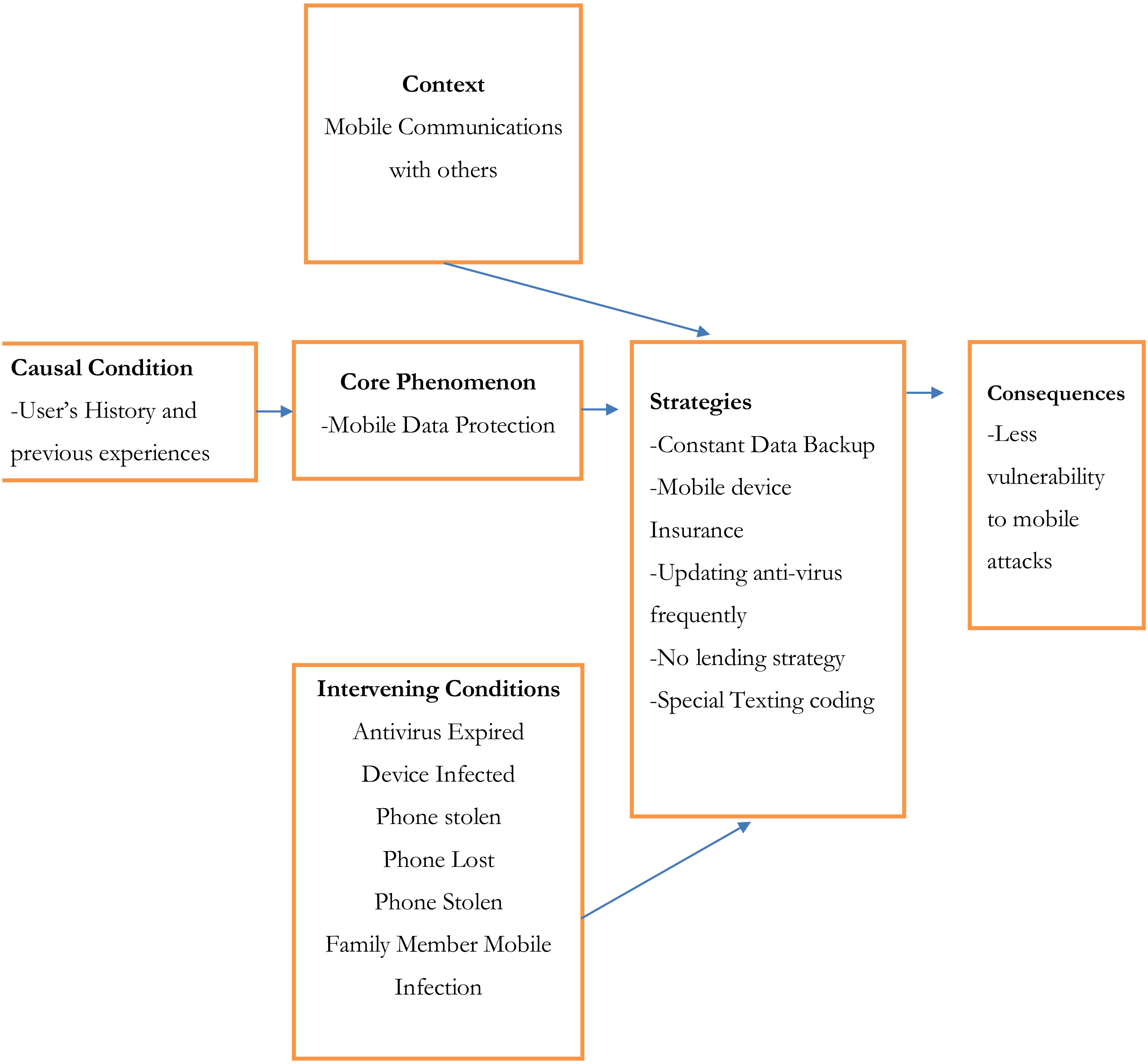


Table 7: Sample of Axial Coding (Individual Differences)

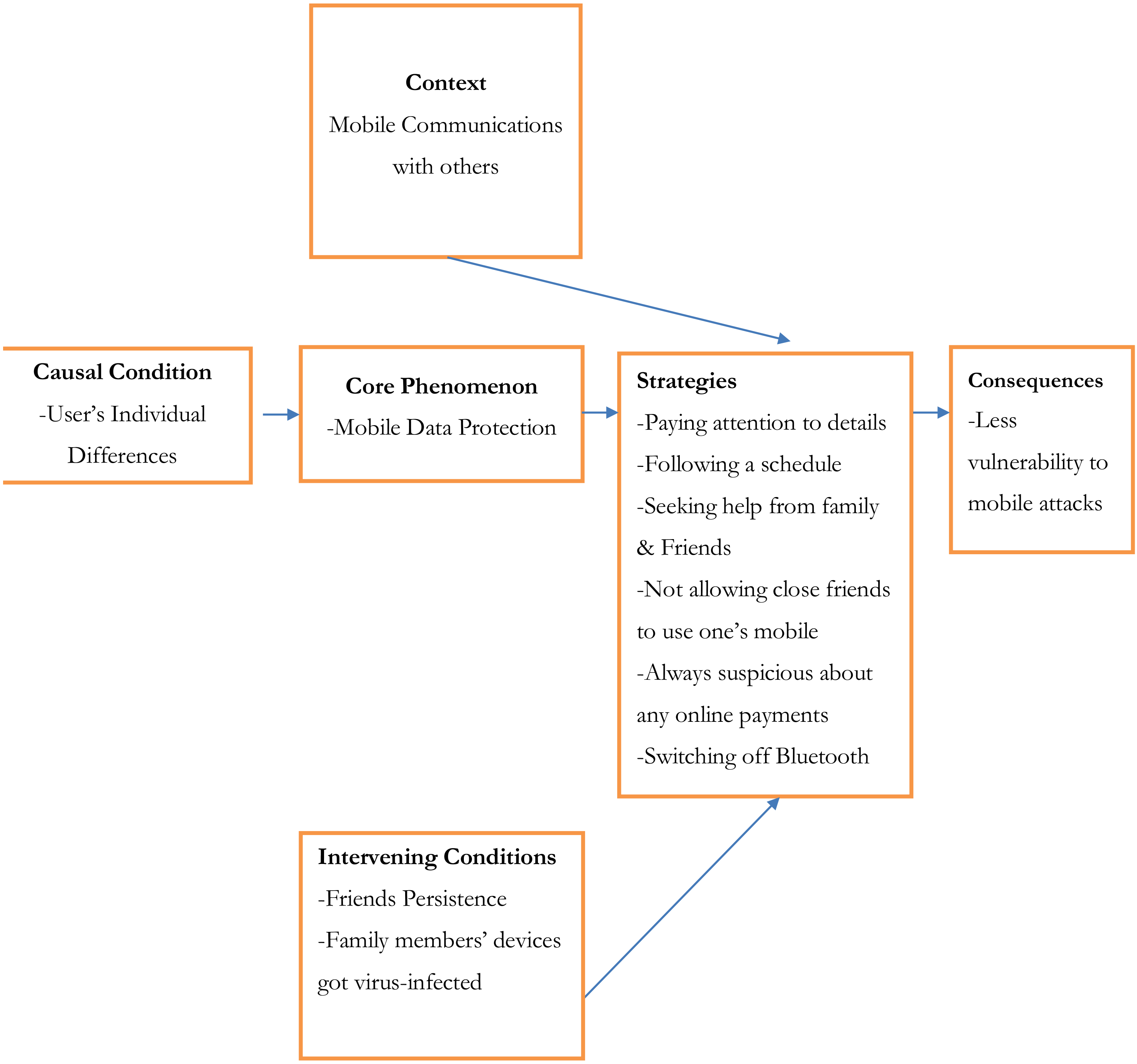
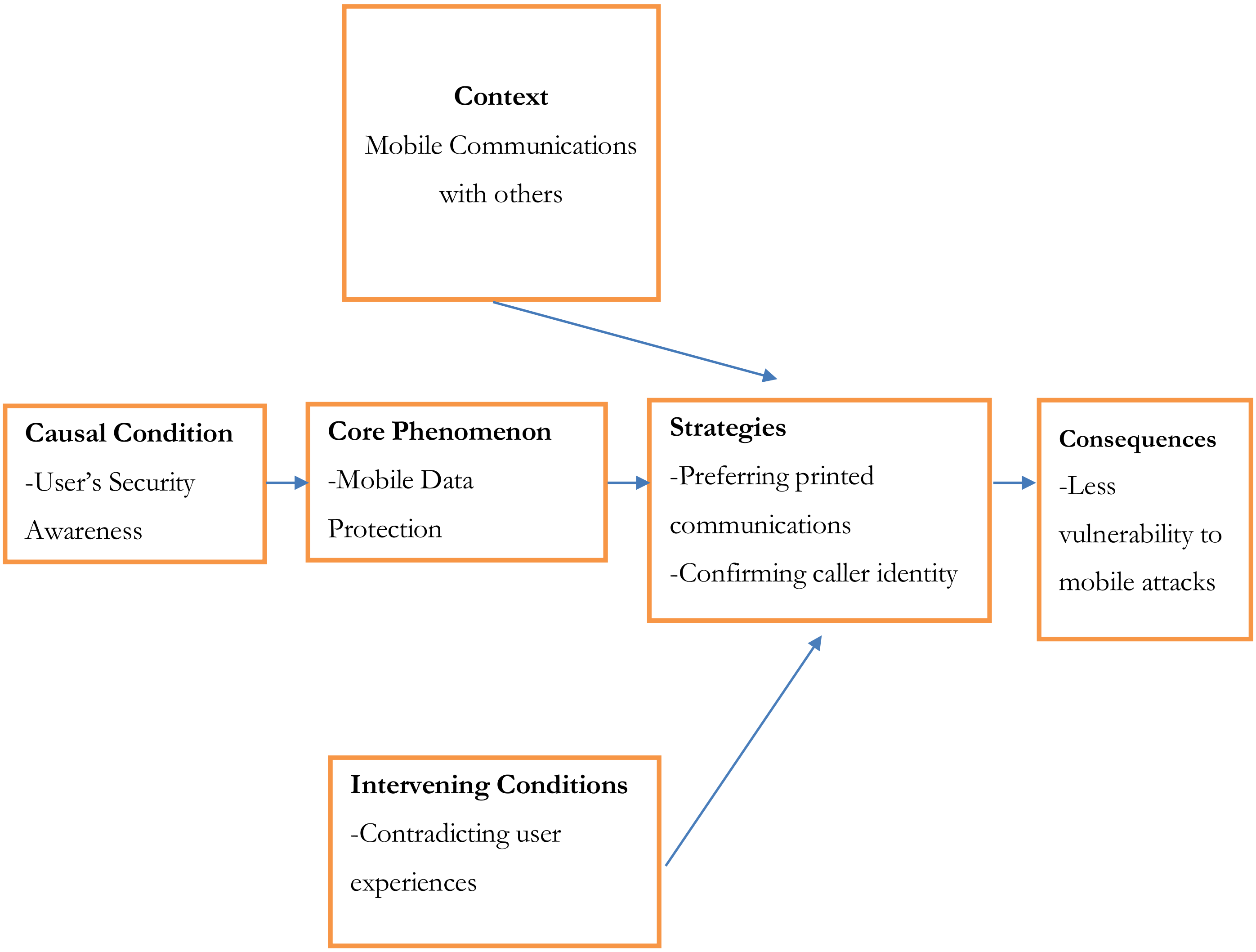

Context
Mobile Communications with others
Causal Condition
-User's Individual Differences
Core Phenomenon
-Mobile Data Protection
Strategies
-Paying attention to details
-Following a schedule
-Seeking help from family & Friends
-Not allowing close friends to use one's mobile
-Always suspicious about any online payments
-Switching off Bluetooth
Consequences
-Less vulnerability to mobile attacks
Intervening Conditions
-Friends Persistence
-Family members' devices got virus-infected

Table 8: Sample of Axial Coding (Security Awareness)


Context
Mobile Communications with others
Causal Condition
-User's Security Awareness
Core Phenomenon
-Mobile Data Protection
Strategies
-Preferring printed communications
-Confirming caller identity
Consequences
-Less vulnerability to mobile attacks
Intervening Conditions
-Contradicting user experiences

3.5.3 Selective Coding

Selective coding is the process of integrating and refining the theory. In this step, the core categories and the high level story line are defined (Cox & Cairns, 2008).

Core category is the conceptual phenomenon around which all other categories are integrated. In our study, examples of these include protecting users' personal data, protecting users' devices, feeling confident to handle security problems.

Story is a descriptive narrative about the central phenomena of the study.

3.6 Research Results

This section presents the results of the research study. Three themes have been elucidated that comprise a theoretical framework of user-perceived mobile security and causes behind their security-related behavior: Users' characteristics, users' history and past security experience and users' level of security awareness. In each of the subsections below, we identify a significant pattern, and provide some relevant interviewees quotes.

3.6.1 Users' characteristics

The study's sample included participants from different domain-specific knowledge and technology efficacy. Also the interviews revealed that the participants are different in regards to their history and past security experiences.

Based on previous research (Microsfot 2006, Symantec 2006, xin and Qinyu 2007, Jagatic et al., 2006), we expected that the interviews' responses of the users who are more technology and security aware, will indicate better compliance to sound security practices than less-aware users. However, this was not the case. Users with similar levels of security knowledge and alike security history responded differently to the same questions and scenarios. Reactions to the interview questions that involve risk met the defining features of the dispositional trait of 'trust'. This was consistent across situations encountered by the participants in the past and scenarios examined in the interview. For example, the answers of some users who admitted that they had been victims of security attacks in the past still indicated high vulnerability to phishing attacks in the future. Their reactions were the same regardless of the situation/context or person they are interacting with. The users who displayed low levels of trust maintained this characteristic with both friends and also with strangers in the questions that investigated online communications with external trustees.

Another example is the characteristic of self-discipline. Some users showed a high level of discipline in terms of keeping sound frequent security strategies. Most of these users showed a leadership attitude in taking care in regards to the management of the security of their devices, even for those who did not have solid IT knowledge. But, they still sought help via following the instructions manual or via relatives and friends to fix passwords and install anti-virus software for their devices. On the contrary, other users whose specific domain is IT stated that they do not have passwords for any of their devices. They admitted that even for devices at work, if the IT-support team did not fix it for them, they would not have fixed it themselves. They were less concerned, and their relaxed attitude applies not only to the security of their computing devices, but also pertains to most of their general life activities, as revealed by the analysis of the data transcripts.

This suggests that individual characteristics can play a role in determining the way people behave in regards to security. Characteristics can be defined as a typical quality of a person (Cambridge dictionary, 2016). Scholars have studied the role of certain dispositional characteristics tendencies on decision making in various settings that involve risk (Vishwanath 2011, Alseadon 2014, Bailey 2010).

Table 9 illustrates a small part of the interpretative process taken to arrive at the concept of individual characteristics. From several discussions in the interviews on the subject of users' security practices, words and phrases have been extracted literally. Related codes were grouped together. We gained a strong sense of *'actions'*, *'thoughts'*, and *'feelings'*.

Table 9: An Example of the Interpretative Process Leading to the Theme individual Characteristics

Source	Quotes	Open Code	Axial Code	Selective Code	Theoretical Code
Interview 1, line 20	I scan it all the time	Scanning	Actions (Users' actions drive security)	Responsibility/ Self-discipline	Individual differences
Interview 2, line 15	You can't trust anyone these days	Low Trust	Feelings (Users' lack of trust)	Suspiciousness	Individual differences
Interview 3, line 17	'I always have the fear that I'll lose or forget it somewhere'	Fear	Feelings (Users' fear of data loss)	Extreme fear	Individual differences
Interview 7, line 20	No one would attack me	Feeling safe	Thoughts (Users believe they are not at risk)	Optimism about others	Individual differences

Analysing the participants' answers resulted in identifying two groups according to their level of discipline they showed in regards to security. The first group had high levels of self-discipline, the second group had low levels of self-discipline. These groups are discussed below.

First Group: Self-disciplined Participants Group

A) Discipline: A particular segment of the participants had a disposition to behave in certain way, in terms of security, regardless of their state of general security knowledge. Analysing the data transcript of these participants indicated a widespread occurrence of a quality of high self-discipline. These participants acted dutifully towards the security of their computers and mobile devices and preferred planned rather than spontaneous behaviour. Examples of their behaviour include: keeping back-ups of their mobile phones data, having insurance for their mobile handsets, updating their computer anti-virus frequently and having passwords for all their devices regardless of the number of the devices they own.

"I have 15 PCs and I have password for all of them" **Participant J, Q5**
"I have Passwords for all my 6 PCs" **Participant L, Q5**

Even individuals with a low state of computing knowledge were keen to successfully implement information security management for their devices via self-care and self-management.

"I do not have solid computer background, but I followed the instructions in the manual for both the password and anti-virus, I also shared with my friend"**, Participant V, Q8**

"I asked my brother in law to install an anti-virus for me"
Participant F, Q8

For some of these users, this quality of discipline was not limited to security-related incidents in specific, but rather extended to the participants' normal life patterns as well.

"I love order" **Participant Ho, Q54**
"I am so organized" **Participant V, Q54**
"I pay attention to details" **Participant H, Q54**
"I like to follow a schedule" **Participant J, Q54**

They tended to refer to the word *'control'* repeatedly in their quotes.

"At home, it's me who takes care of everything" **Participant H, Q54**
"I am always prepared" **Participant Ho, Q54**
"Security threats for me means things I receive on my computer without my desire" **Participant F, Q1**

Individuals with self-discipline quality, unlike other participants who used to download only 'free' anti-virus applications, used to pay for their anti-virus software.

"I've antivirus for my 6 computers and I've paid for them all" **Participant L, Q7**

B) Suspiciousness

For those participants, we noticed they share a temperament of suspiciousness which applies not only to their intellectuality but also applies broadly to their emotions, actions and reactions. They were inclined to scepticism. This quality of scepticism seemed to encounter generally at a particular time, place or incident, normally when dealing with another party. Those participants tended to be independent mostly because they do not trust the others are capable of getting the job done.

For example, these individuals took responsibility for protecting their own mobile phones even if other party, such as their mobile operator, would handle this issue. They conspicuously expressed their lack of trust in others.

"You can't trust anything these days" **Participant F, Q21**
"I use online ordering, however, each time, I do it with a lot of worrying" **Participant H, Q?**
"I do not trust anyone calling me" **Participant J, Q24, Q25**

These participants refused to lend their mobile phones to others even friends who ran out of battery unless they are very close friends

"No lending" **Participant L, Q37**
"Never" **Participant J, Q30**
"If she is my friend, then I probably have the contacts she wants, why would I give her my mobile then, I refuse. I think it is not necessary" **Participant F, Q30**
"Only for best best friend" **Participant F, Q37**

Some of these participants even used special coding mechanisms when texting. Their aim was that if someone gets access to their messages, he will not be able to understand them.

"The way I write it is private, so if you do not know me, you would not understand it" **Participant F, Q20**
"I store my bank details in a secret way, so it is not obvious it is card detail" **Participant V, Q14**
"I just text one word, like yes or no" **Participant F, Q20**

Concerning mobile phishing attacks, when we examined their tendency to fall victims of phishing attacks, they stated they would never respond to any message or call asking for information. *"I'll have doubts about 'who' is the caller"*. Although some were not aware of SMS ID spoofing, they reported they will not respond to the phishing scenarios the interview offered. They justified their position of the proposed phishing message by saying:

"People are really creative these Days" **Participant F, Q25**.
"No, because I do not trust them" **Participant V, Q24**.
"And why would others know my password" **Participant V, Q24**.
"I do not think it is necessary for them to know" **Participant F, Q24**
"Only if I changed my network, and even then, I'd not do it over the phone, I'd go to the store" **Participant F, Q24**

Their behaviour was typical of sceptical people who are more likely to put in much effort in investigating the situation, such as double-checking the authenticity of the caller, searching online, or calling from another number, before believing what they are told.

"They have to convince me" **Participant J, Q24**.
"When I receive an important SMS, I call the sender myself to check if it was him who really sent the message" **Participant Ho, Q25**

Some of these participants had no previous knowledge regarding the existence of mobile viruses. When this information was provided to them via the interview questions, they became 'very worried'. This was very obvious throughout the second half of the interview. Their responses to the following questions reflected their fears. For instance, when later asked if they had experienced a virus on their mobile phone, their answer was neither 'yes' nor 'no'. Instead, we got the answer *'Not yet'* **Participant F, Q53** while others said *'May* be', **Participant V, Q53**. They also declared their determination to install a mobile anti-virus as soon as the interview was finished. When asked if they ever had security concerns while connecting to the Internet via their mobile phone, some said *'Now I Do'*. Moreover, some showed their satisfaction that their current mobile does not have the ability to connect to the Internet. "*Luckily this phone does not have Internet on it*", they said.

In questions exploring their general security attitude, their answers revealed their worries. An example of such was their reaction when their anti-virus expired and they got viruses. Participants' answers were: *'I got really scared'*, 'I *deleted all my laptop files', 'I uninstalled and re-installed everything'*.

These findings show excessive feeling of digital danger as well as suspiciousness. Some of these subjects were spending much time worrying about extra security checks that were not necessary such as uninstalling the operating system and installing another one. They were sacrificing losing uninfected files by deletion through the new installation process for more additional assurance and relief that their devices are virus-free.

The security behaviour and security strategies mentioned above were common among users within this group for users with both high and low state of awareness in regards to security.

Second Group: Undisciplined Participants Group

The other group of participants had what can be described as a lax attitude towards security. At the same time, they were very friendly and very trusting. They had a prevailing quality of indiscipline. They were the sort of people who leave their belongings around, forget where they had put their house keys, and lose the keys of their cars. It was a similar situation regarding their own handbags, as per their answers to the interview questions (Question 54, which asked the participants to describe themselves in terms of order and discipline).

This prevailing frame of mind of low self-discipline was reflected in those participants' security behavior. They acted poorly in terms of having no anti-virus software for their PCs, having no password for their laptops or their phones and taking no back-up for their data. They have passwords only for their PCs at work but not at home.

"Technical support did, if he didn’t, I would not” **Participant D, Q6**
"Only at work, not at home" **Participant Rs, Q5**
"No Passwords" **Participant Ab, Q5**

They defended their behaviour of not having a password for their laptops and mobile phones by saying:

"I'd like quick, just turn it on and you know" **Participant Ab, Q6**
"No one would attack me". **Participant Rs, Q6**
"I am not taking it anywhere" "No one else can use it" **Participant Ab, Q7**

Regarding phishing, their answers to the interview's phishing scenarios suggested they are more likely to become vulnerable to such attacks. They showed high tendency to respond to Vishing and SMishing attacks. Regarding Vishing, when asked if they would give their password to the mobile company support over the phone, they said:

“Yes, if I got it from unknown number” **Participant D, Q24**.
"Yes, I will give it to the operator customer support" **Participant Re, Q24**

As for SMishing, when assessing their vulnerability of becoming deceived by a forged message pretending to be sent from their bank, some of them said they would trust the message by 100% and some said 70%!.

In regards to lending their mobiles to others or swapping SIM cards in case of battery shortage, participants in this group seemed to have no problem with that.

"Yes, I did it many times" **Participant Re, Q30**
"I have never come across that, but why not if needed" **Participant R, Q30**
"Yes, I'm used to swap SIM cards with colleagues at work" **Participant Rs, Q30**

The security behaviour, high tendency of responding to mobile phishing attacks and poor security strategies mentioned above were common among users within this group for users with both high and low state of awareness in regards to security knowledge.

3.6.2 Users' History as a Moderating Variable between Individual Differences and Security Attitude

It was noticed that two participants who belong to the second group explained highly desirable security behaviour. The common criterion between these two participants was that they both had a history of upsetting security-related problems.

In this section we discuss the second theme suggested by the interviews interpretations. This theme is in regards to the extent users' history and previous experience with security-related issues, can affect their security attitude and their future behaviour.

Table 10 illustrates a sample of the interpretative process followed to reach the theme of previous history of security-related incidents. From several discussions in the interviews related to the subject of users' security practices, words and phrases have been extracted literally. Related codes were grouped together.

Table 10: Examples of Interpretative Process leading to the Theme Upsetting Security History

Source	Quotes	Open Code	Axial Code	Selective Code	Theoretical Code
Interview 4, line 11	It expired and then I got 2 detections of viruses	Virus infection	Thoughts (Relating delay in S/W upgrading to getting viruses)	Figuring out causes and consequences	Upsetting Security History
Interview 4, line 12	And now, I scan my entire computer all the time	Scanning	Action (Users' change behaviour)	History shapes future	Upsetting Security History
Interview 8, line 17	'I lost my mobile, dropped from my pocket	Loss of device	Feeling(upset)	Loss of devise feeling upset	Upsetting Security History
Interview 8, line 21	I have backup of my mobile contacts	Backup	Action (Taking backup)	History shapes future	Upsetting Security History

The interpretation of these interviews showed these participants' unpleasant security-related history. One of them had her phone stolen, and her computer was infected by a virus in the past. The other has lost her mobile phone before and has witnessed her brother's mobile phone being virus-infected. Now, they have passwords for their mobile phones, backing up their data on another media and updating their antivirus software frequently.

This interpretation suggests that these unpleasant memories affected the way they feel and act in later incidents. For example, one of those participants got a virus on her computer as soon as her anti-virus software expired. Accordingly, she related her bad security attitude 'delay in updating the antivirus program' to the consequence of getting her PC infected.

"It expired and then I got 2 detections of viruses"

'I always have the fear that I'll lose or forget it somewhere' **Participant Z, Q53**

This experience changed her behaviour to more reliable future security practices. For example, she said she never forgot to upgrade her anti-virus software since then.

” And now I scan my entire computer all the time” **Participant Z, Q11**

” I've never thought of security till my brother phone was infected" **Participant Hur, Q16**

This suggests that users' upsetting memory affect their future decisions via a learning process or as Ingvar (1984) called it '*memories of the future*' where people's past experiences program their future actions by forming the basis for anticipation and expectation for both short term and long term future. (Costanzo and MacKay, 2008) interpreted Ingvar’s concept ‘memories of the future’ as a process of learning fostered by the brain to eventually help individuals to be better prepared for unexpected situations when an urgent decision is needed to be made. Scholars such as Alberto and Troutman (2003) and Comer (2004) regard learning as the acquisition of a new behaviour.

3.6.3 Users' Level of Security Awareness as a Moderating Variable between Individual Differences and Security Attitude:

It was noticed that one of the participants, participant Rch, who is a house wife, was very careful in regards to mobile phishing attempts. This was strange as the rest of her answers revealed that her general state of security knowledge is low. Yet, her bank has warned her that they will never ask for any confidential information over the phone. Their only communication method with her was mail. This was confirmed with participant G who had an unrealistic optimism regarding the security of his mobile, yet his computer security background made him alert in regards to phishing and virus attacks.

In this section, the third theme suggested by the interview interpretations is discussed. This theme investigates the effect of awareness from concerned parties on the participants’ security behaviour.

Table 11 illustrates a sample of the interpretative process taken to arrive at the theme of Security Awareness. From several discussions in the interviews on the subject of users' security practices, words and phrases have been extracted literally. Related codes were grouped together.

Table 11: An Example of the Interpretative Process leading to the Theme Security Awareness

Source	Quotes	Open Code	Axial Code	Selective Code	Theoretical Code
Interview Rch, line 17	My bank already told me, we do not ask about this information online	Bank awareness	Thoughts (Security awareness	Phishing awareness	Security knowledge and Awareness

The analysis of the data revealed that the participant had incorrect information regarding security of mobile phones short messages. For example, she believes that her short messages are private and no one has access to it even in the mobile operator databases. She also revealed that her knowledge about security is very low.
"Security of my phone?!! I do not know, I do not know"

She also had lax attitude towards security in general.
"I protect my mobile by locking it, but most of the people know how to unlock it anyway"

However, in regards to mobile phishing attempts, she stated that she would never give her mobile password or her bank details over the phone. She confirmed that the reason is that her bank has communicated this matter to her before.
"I'll probably ask them to mail me in a letter"
"Not sure if that is the right person who is calling"

Similar responses were recorded from participant R whose behaviour indicated a lax attitude towards security. She admitted she is used to swapping her mobile SIM cards with colleagues at work many times. She also does not have a password, anti-virus, insurance or back up for both her mobile and her laptop. Despite that she stated she would 100% believe both an email and a mobile message with sender ID entitled

'HSBC', she asserted she knew for certain she would never respond to any of these messages by providing her bank details. Participant R studies security as major and is very familiar with phishing attacks.
"In my study, I came through many of these fake scams"
"I know for sure, this may be a security attack"
"I would prefer if I call them back after using the number I have"

This suggests that awareness regarding mobile phones security, either through education or through service providers such as mobile operators or banks, can act as a moderating variable that alters the impact of dispositional characteristics effect on their security attitude. Hence, this helps users make more rational mobile security decisions.

Based on the discussion above, we suggest the following theory: "Human security attitude, represented in both situational decisions and frequent security strategies, can be attributed to individual differences. This general behaviour is moderated by individuals' past security experience and their level of awareness in regards to security-related knowledge".

This theory proposes that the primary factor affecting security behaviour is personal characteristics, and that it is more important in making security decisions than how knowledgeable an individual is. The theory does not neglect the fact of the effect of experience-related factors but it proposes that personal characteristics have the greater effect. This was supported by those who were very well-educated in terms of security knowledge, yet, this knowledge was not mapped into their security practices.

Other Findings

It was important to investigate if any technological factor has affected the participants' security attitude, like having an old, new or hard-to-use mobile handset. In an effort to examine if the type of mobile users' handset played a role in forming their perception and security practices, an investigation has been made. **Table 12** shows a summary of users' handsets types.

Table 12: Summary of users' Handset Types

Number of Users	Type
5	Nokia Smart Phone
5	iPhone
2	Old Nokia Phone
1	Samsung Smart Phone
1	BlackBerry 9700
1	Sony Ericsson Smart Phone

Only two participants did not have smart phones, but own very old phone types. They stated that having an old handset affected their security practices. For example, one of them stated that she could not download mobile anti-virus to her handset or configure a password either. While the other participant said he configured a PIN for his mobile. However, this last participant felt that because his handset is old, it is not at risk of being stolen by thieves.

Below are examples of these two participants' responses to questions investigating about their mobile passwords and actions they would do in case their mobile phones were stolen.

'No password, with this type of mobile, it's hard', **Participant Ab, Q33**

'I do not think anyone would steal my handset', **Participant J, Q32**

However, it is worth noting that all other answers of participant J indicate high level of discipline. For instance, he has passwords and anti-virus for all his computers. On the other hand, Participant Ab's other answers indicated a low level of discipline dealing with her computers as well. For instance, when she was asked why she does not have anti-virus for her computer, she answered that no one else would access it.

These responses from both participants suggest that users' behaviour in regards to security is not always limited by the technology they used. As the interviews revealed, keen and disciplined users did their best in securing their devices. Hence, we will not regard the handset type of effect to our results, especially that only two users had old devices.

3.7 Discussion

In section 3.3, three main themes of results are mapped: Individual differences, security history and security awareness. In this section we discuss these three themes in more depth. For each theme, we discuss how and why effects on human's security behavior are expected to operate and ultimately under which conditions.

3.7.1 Individual differences

The interviews discussed two types of security behaviour: frequent security strategies and situational security decisions. In this regard, the results indicated that individual differences can be related to security behaviour and trust judgements. In specific, two personal predispositions were of particular relevance; self-discipline and trust. In this regard, a sizable body of research show evidence that these two personal features are closely related to individuals' *personality.*

For the interpretation of these features in terms of individuals' personality, we use the Big Five model. The Big Five Model is a framework that provides a relatively comprehensive representation of human's personality (McCrae & Costa, 1997; John et al., 2008; Mondak, 2010; Mondack, Hibbing, Canache, Seligson, & Anderson, 2010). It covers five basic factors of personality traits; Agreeableness, Conscientiousness, Extraversion, Openness and Neuroticism (Mccrea & Costa, 1999) (Mccrea & Costa 1997). We suggest that utilizing these factors can provide multiple perspectives on what types of individuals might be less vulnerable to security attacks.

Below, we evaluate the two qualities highlighted by the grounded theory, *self-discipline* and *trust* using the lens of human personality.

Linking Self-discipline and Trust to the Big Five Model:

a) Self-discipline

The capacity to exert discipline or control over one's desires has been referred to as self-discipline or self-regulation (Timpano & Schmidt 2013; Skinner 1953) and it is necessary for humans in order to achieve their goals. A thorough examination of the Big Five Factors found that *conscientiousness* personality trait is the closest trait in relation to discipline.

Conscientiousness is a broad dimension of personality which is extremely robust (Lee & Klein, 2002). It describes a collection of traits including organization, responsibility, dependability and cautiousness. An individual who is not conscientious may be disorganized, careless and impulsive. On the contrary, the conscientious individual is purposeful, strong willed and self-controlled. The Conscientiousness trait encompasses six main basic features: competence, order, dutifulness, achievement striving, self-discipline and deliberation.

Linking these basic characteristics of a conscientious person to the results inferred from the self-disciplined interviewees confirms our suggestion that conscientiousness is much related to self-discipline. These interviewees who used to set passwords for all their devices, no matter how many personal devices they own, and keenly update their anti-virus software, are more likely to score high in conscientiousness. Moreover, self-disciplined users showed leadership attitude. They had the inclination to lead and felt responsible for taking care of the security of their mobile phones. They valued their own opinions and were keen to implement information security management via self-care and self-management even for those who did not have solid computing knowledge.

This analysis is consistent with previous research that confirmed positive relation between conscientiousness and self-efficacy (Martocchio & Judge, 1997). Self-efficacy refers to *the judgement individuals make about their capabilities to orchestrate future performance on a specific task* (Gist & Mitchell, 1992). Our analysis was also in line with previous research that confirmed that highly conscientious individuals approach learning and training with greater task-specific self-efficacy than low conscientious individuals (Martocchio & Judge, 1997). Task-specific self-efficacy stands for an individuals' intention to allocate mental or physical effort to achieve a targeted level of performance (Kanfer, 1990). Individuals, whose self-efficacy beliefs are high, normally exert greater effort to master challenges (as in the case of the participants who sought help via manuals and relatives) than individuals whose self-efficacy beliefs are low (Locke & Latham, 1990). Evidence has been provided by research in regards to similar tasks. An example of which is Gist, Schwoerer, & Rosen (1989) who proved that self-efficacy had positive effects on compilation in software training. In line with Gist et al.(1989), we maintain that self-efficacy represents the mechanism through which Conscientiousness manifests itself in security training. On the other hand, low self-efficacy individuals have a tendency to dwell on their personal deficiencies. (Bandura, 1994).

Accordingly, in light of the results of this study and previous literature, we hypothesize that individuals who are responsible and unwilling to compromise may be more likely to have sound security strategies and to be less vulnerable to fall for phishing attacks than those who are obedient and disorganized.

b) Trust

Trust can be defined as *a truster's subjective estimation of the probability that the trustee B displays a behaviour X preferred by the truster* (Bauer & Freitag, 2013). This definition highlights two important parameters; the trustee B and the behaviour X. Two other important parameters that were discussed by scholars are *personalized* and *generalized* trust. Personalized trust, often named, particularized trust, refers to people we know from everyday interaction such as friends. Generalized trust refers to people whom we do not know such as strangers (Freitag & Buer 2013; Freitag & Traunmuller, 2009).

Trust can also be defined as a general propensity and is thus primarily a personal innate predisposition. In this view, trust is not exclusively dependent on the perceived qualities of external factors, but depends largely on the trusters' innate propensity to trust (Sztompka, 1998; Uslaner, 2002). In this regard, trust is therefore a stable predisposition that does not change appreciably over time and is closely related to personality traits.

In this sense, we expect to see two possible situations of how personality traits may affect an individual's trust judgements. First, according to certain personality traits, one may *generally* judge the trustworthiness of others in a more positive or a more negative way regardless of the trustee. Second, based on an individual's personality traits, a person may judge *whom* to trust. An example of this is judging strangers in daily interactions, trusting email messages and SMS messages, swapping SIM cards between mobile users and sharing passwords between many individuals.

There is evidence from previous literature about the relationship between trust and personality traits. For example, Dinesen, Nørgaard and Klemmensen (2014) show that all personality traits influence generalized trust. Conversely, a number of studies have found a relation between generalized trust and only the personality trait of agreeableness (Mondak & Halperin 2008; Anderson 2010; Dohmen, Falk, Huffman, & Sunde 2008). It was also found that agreeableness and extraversion are linked to generalized trust (Hiraishi, Yamagata, Shikishima, & Ando, 2008).

Oskarsson, Dawes, Johannesson, and Magnusson (2012) ascertain that generalized trust is correlated to extraversion, personal control and intelligence. Lastly, Uslaner (2002) calls attention to the relation between general trust and optimism.

Based on the Big Five taxonomy, trust is a subcategory of the personality trait agreeableness. Agreeableness is a personality dimension that describes a collection of traits that assess individuals' compassion, cooperation and trust. An individual who is not agreeable may be suspicious, impatient and assertive. In contrast, agreeable individuals are altruistic, trusting and sympathetic. The Agreeableness trait covers six main features: trust, straightforwardness, altruism, compliance, modesty and tender-mindedness.

McCrea and Costa (2003, 50) define agreeable individuals as those who *"are trusting, believing the best of others and are rarely suspecting hidden intents"*. Moreover, agreeableness, more than any other trait describes an individual behaviour in interactions with others (Mondak, 2010).

We found this consistent with the results of our study which confirm and explain the behaviour of our participants of low trust in others, who used special code for their communication via mobile with their friends and were less likely to fall for phishing attacks than other individuals who have stated they may give away their mobile PIN number by phone to a customer support representative.

Accordingly, we suggest that the individual differences proposed by our grounded theory (reported in section 3.3.1) as a key role player in shaping users' security strategies and situational decisions, can be mapped into A*greeableness* and *Conscientiousness* personality traits.

B) Users' history and security knowledge as Moderating Variables between personality traits and Security attitude

There is evidence from the literature that experiences influence individuals' trust. A sizable body of research suggests that human's trust is basically grounded in experiences of trustworthiness in social interaction (Garbarino & Johnson, 1999; Coleman, 1990). Drawing on past experiences of an individual, it is possible to infer their future behaviour (Coleman 1990).

The way that personality traits can interact with experiences to shape an individual's trust was discussed by Bauer and Freitag (2013). They suggest that personality traits have an indirect effect on trust judgments. They believe this indirect relation is mediated and moderated by other external factors. For example, Mondak (2010) suggests that personality influence education and institutional trust. Bauer and Freitag (2013) believe that this suggests that distant factors such as *personality* influence our experiences which are more proximate causes of our propensity to trust.

In this regard, a vast amount of research has linked personality traits to education (Paxton 2007; Robinson & Jackson 2001; Uslaner 2002). It was suggested that increased education expands people's horizons and tends to make them more open minded and thus more willing to accept others, which promotes trust (Bauer & Freitag). Education supplies us with knowledge and information, which form the basis of daily interaction.

A number of studies (Jaccard & Jacoby 2010; Huckfeldt 1983) support our conclusion. They suggest that contextual factors can moderate the way personality affects attitude and behaviour and that contextual factors can structure people's actions and interactions. Bauer and Freitag (2013) also believe that the socio-economic structure of a given context also moderates the relationship between personality and trust.

Linking previous literature to our results in the context of security practices, this indicates that new situations and events can trigger disturbing memories, leading the person to believe that danger will occur again if they continued on performing the same bad security practices, and this belief would lead them to take a defending action by becoming more cautious and embrace better security practices. Consequently, the perceived usefulness of their new healthy behaviour will turn into confirmed usefulness.

This suggests that previous security experiences can act as a moderating variable that can affect individuals' future security behaviour. Of course there is no direct connection between past experiences and future attitude. Here we highlight the importance of the intervening variable of *'Learning'*. What happened with our participants was that an internal state of learning intervened between past security experiences; 'independent variable' and future security attitude; 'dependent variable'. It was this state that caused the behaviour to improve, not the past security experiences.

Accordingly, our grounded theory was reframed as follows:

"Human security attitude, represented in both situational decisions and frequent security strategies, can be attributed to Agreeableness and Conscientiousness personality traits. This general behaviour is moderated by individuals' past security experiences and their level of security-related awareness".

Implication:

The development of the proposed grounded theory calls for conducting further studies to test the produced hypotheses and the introduced variables. Yet, an important step of validating the theory is needed before conducting further studies. This face validity investigation is reported in the next section.

3.8 A Follow-up Face Validity Study of the Effects of Personality on Security Behaviour

3.8.1 Introduction

The grounded theory study presented in sections 3.1-3.5, suggested that personality is the main determinant for human security behaviour, a relationship that is moderated by individuals' past security experiences and their level of security-related awareness.

3.8.2 Study Motivation

Face value studies are generally used to preliminarily confirm conceptual models. Also quantitative analysis is mainly used to test theories with hypothesis.

In the grounded theory we interpreted the themes without using a standard personality test. We also used only qualitative analysis. No quantitative analysis was used.

As we depend on the grounded theory to generate a set of hypotheses that the thesis will investigate via further three studies, it was central to our research to preliminary confirm our theory before starting the next study.

3.8.3 Study Objectives

The main objective of the study is to assess the validity of the grounded theory produced in the previous study. In specific, the study assesses the correlation between personality traits and individuals' security behaviour. This was broken down into the following objectives:

-Investigating the possible effects of personality on individuals' vulnerability to mobile phishing attacks.

-Investigating the possible effects of personality on individuals' security strategies in regards to their mobile phones.

3.8.4 Study Structure

A follow-up standard personality questionnaire was filled by the participants. Then the correlation between the participants' personality traits and their scores in phishing responses questions and security strategies were measured.

Therefore, mainly, the data for this study was obtained from two sources:

a) Participants' responses to questions of the grounded theory study.

b) Participants' personality scores.

a) Participants' responses to the interviews:

Only scenarios and questions that investigated participants' mobile security behaviour was pulled from the interviews of the grounded theory. They were 4 scenarios and 4 questions. Below we discuss the participants' responses for each.

i) Participants response to scenarios:

Four phishing scenarios were selected. Two of them represented Vishing attacks, one represented email phishing and one represented a SMishing attack. For each scenario, the Participants were asked to indicate the extent to which they would trust a communication method asking them to reveal confidential information. The scenarios included the following; phone call from their mobile operator, phone call from their bank, mobile text message from their mobile operator and an email message from their bank. These scenarios are listed below.

- You received a phone call from your mobile operator customer support asking you about your password; would you cooperate and tell them about it?

-You received a phone call from your bank support asking you about your bank account information; would you cooperate and tell them about it?

-You received an Email, the sender header says 'HSBC', how certain will you be that your bank has sent you an email?

-You received an SMS, the sender header says 'HSBC', how certain will you be that your bank has sent you a text?

ii) Participants response to security strategies questions:

Five mobile security practices questions were selected. All of them were in relation to participants' mobile phones. These included the following questions:

-Do you have password for your mobile phone (PIN)?

-Do you allow mobile SIM swap with others' mobile handsets?

-Do you lend your mobile phone to others?

-Do you have back-up for your mobile data?

b) Participants' personality scores

The personality traits of the participants were assessed using a standard personality questionnaire. Every participant had five scores each for every personality trait.

3.8.5 Sample

The participants of this study were the same participants involved in the grounded theory. They were 15 mobile users. Yet, due to travel arrangements of the participants, only 11 could be reached to participate in this study.

3.8.6 Instrument

Psychological Instrument

The psychological domain used in this study to describe human personality was *the Five Factor Model* (FFM) that consists of five broad personality traits. This covers Agreeableness, Conscientiousness, Extraversion, Openness and Neuroticism. The psychological instruments used to measure the FFM personality traits, in this study, was the *international Personality Item Pool* (IPIP). The IPIP questionnaire is a standard questionnaire. It stands for International Personality Item Pool. It was created by Lewis Goldberg (IPIP, 2013). The questionnaire is composed of 120 self-descriptive sentences on a five-point scale, ranging from "strongly disagree" to "strongly agree". The personality test can be accessed here: http://ipip.ori.org

The rational for choosing FFM and IPIP in specific was discussed in chapter 1.

3.8.7 Quantitative Analysis

Table 13 below shows the percentage of participants performing a practice that is not considered a sound security practice.

Note: security behaviour was regarded to be sound based on general agreement in security manuals. Example includes AOL online safety manual (AOL, 2004).

Table 13:The Study's Eleven Participants' Response to Security Scenarios and Questions

Security Practice	Number of Participants who do	Percentage of Participants who do
Respond to a phishing call pretending to be from the mobile operator	5	45.5%
Respond to a phishing call pretending to be from the participant's bank	3	27.3%
Trust an email pretending to be from the participant's bank	4	36.4%
Trust an SMS pretending to be from the participant's bank	4	36.4%
Swap mobile SIM card with others	8	72.7%
Not have PIN for their mobile phones	8	72.7%
Lend own mobile phones to others	6	54.5%
Not have back up for Mobile data	8	72.7%

Table 13 Table 14 below shows the participants' security actions. This data is based on the interviewees' answers to the questions and scenarios in section 3.5.1 the dots here refers to risky security behaviour.

Table 14: Participants' Risky Security Practices

Participants	Reply to Phishing Call (claimed to be from Operator)	Reply to Phishing Call (claimed to be from Bank)	Trust Phishing Email	Trust Phishing SMS	Swap Battery With work colleagues	Have PIN for mobile device	Lend Mobile Device to friends	No Backup
P1								
P2		•	•	•	•	•	•	•
P3	•	•	•			•		•
P4	•				•	•		•
P5	•				•	•	•	•
P6					•	•	•	•
P7	•	•		•	•			
P8	•		•	•	•	•	•	•
P9				•	•	•	•	•
P10			•		•	•	•	
P11								•

The results represented in **Table 14** were then compared with the participants' personality traits. This is explained in the next section.

Statistical Analysis

The relationship between the participants' personality traits and the risky actions performed by them has been examined using the Spearman correlation test. The personality traits investigated are the Big Five personality traits Agreeableness, Conscientiousness, Openness, Extraversion, and Neuroticism. The actions investigated are the risky security actions illustrated in **Table 14** above.

Only three personality traits showed correlation with the participants' risky security behaviour. These are: Agreeableness, Conscientiousness, and Extraversion. The risky behaviour correlated is trusting SMS banking phishing message.

Below, these relationships are explained.

a) Personality Trait Agreeableness

The analysis shows positive correlation between the personality trait *Agreeableness* and the risky action 'trusting falling SMS banking phishing message'. This suggests that individuals who score high in Agreeableness are more likely to fall for phishing (Correlation Coefficient = .660 with significance 0.27). This result is in line with the grounded theory results which proposed that phishing vulnerability can be attributed to '*Trust*'; a subdomain under Agreeableness. The correlation is shown in **Table 15** below.

Table 15: Agreeableness Correlations

Correlations

			Agreeableness	SMS_bank_Response
Spearman's rho	Agreeableness	Correlation Coefficient	1.000	.660*
		Sig. (2-tailed)	.	.027
		N	11	11
	SMS_bank_Response	Correlation Coefficient	.660*	1.000
		Sig. (2-tailed)	.027	.
		N	11	11

*. Correlation is significant at the 0.05 level (2-tailed).

b) Personality Trait Conscientiousness

The Analysis shows negative correlation between the personality trait *Conscientiousness* and the risky action 'trusting falling SMS banking phishing message'. This suggests that individuals who score high in *Conscientiousness* are less likely to fall for phishing (Correlation Coefficient = -.660 with significance 0.051). This is in line with the grounded theory results that proposed that '*Self-Control*'; a sub-domain of *Conscientiousness* personality trait, is closely associated to phishing vulnerability. The correlation is shown in **Table 16** below.

Table 16: Conscientiousness Correlations

Correlations

			Con	SMS_bank_Response
Spearman's rho	Con	Correlation Coefficient	1.000	-.600
		Sig. (2-tailed)	.	.051
		N	11	11
	SMS_bank_Response	Correlation Coefficient	-.600	1.000
		Sig. (2-tailed)	.051	.
		N	11	11

*. Correlation is significant at the 0.05 level (2-tailed).

c) Personality Trait Extraversion

The analysis shows negative correlation between the personality trait *Extraversion* and the risky action 'trusting falling SMS banking phishing message'. This suggests that individuals who score high in *Extraversion* are less likely to fall for phishing (Correlation Coefficient = -.603 with significance 0.049). The correlation is shown in **Table 17** below.

Table 17: Extraversion Correlation

			Extra	SMS_bank_Response
Spearman's rho	Extra	Correlation Coefficient	1.000	-.603*
		Sig. (2-tailed)	.	.049
		N	11	11
	SMS_bank_Response	Correlation Coefficient	-.603*	1.000
		Sig. (2-tailed)	.049	.
		N	11	11

Face Validity Summary of Results:

Agreeableness positively correlated with mobile SMS phishing vulnerability.

Conscientiousness negatively correlated with mobile SMS phishing vulnerability.

Extraversion negatively correlated with mobile SMS phishing vulnerability.

Face Validity Results Interpretation:

The results added statistical validity of the grounded theory results that proposed correlation between personality traits and security attitude. However, although the grounded theory suggested the personality trait *Agreeableness* is responsible for phishing susceptibility and the personality trait *Conscientiousness* is responsible for maintaining sound security strategies such as those in relation to anti-virus software, passwords and data backup, the face validity results suggest otherwise. The face validity results indicated that it is not only *Agreeableness* that may affect phishing vulnerability. But also, *Conscientiousness* personality trait was significantly correlated with phishing susceptibility. One explanation for this may be the facet 'paying attention to details', which is a sub-domain of the personality trait conscientiousness. The face validity also suggested another personality trait, *Extraversion,* as being responsible for phishing susceptibility. One explanation for this is that extrovert individuals are more socially engaging persons and so are more likely to be aware of spread phishing scams.

Accordingly, in light of the face validity results, the grounded theory can be framed as below:

The success of phishing attempts is accounted for by the victims' personality traits, specifically Agreeableness, Conscientiousness and Extraversion. This general behaviour is moderated by individuals' knowledge and upsetting past security experience.

Note: we focused on upsetting security experience, as security positive security experiences by nature are less likely to be identified by the users (West 2008, jakobsson 2007). West (2008) explains that the users are more likely to feel the loss resulting from security incidents than the gain. Jakobsson (2007) states that the reward of security is that nothing happens at all.

3.9 Chapter Summary

The chapter investigated people's perception about mobile security and the drivers for their security behaviour by means of a series of interviews performed sequentially in multiple stages.

The author agrees and refutes several theories before concluding that human security attitude is strongly influenced by their *agreeableness*, *conscientiousness* and *extraversion* personality traits. The developed theory suggested that this general behaviour is moderated by individuals' knowledge and upsetting past experiences. We test this theory via conducting three studies reported in the following three chapters.

4 Chapter 4: Phishing IQ Test

This chapter reports the findings of a phishing quasi-experiment. The experiment serves two purposes. First, it investigates IT-literate individuals' ability to correctly distinguish between phishing and legitimate mobile text messages. Second, it provides context for the design of the field experiments reported in chapter 5 and 6.

4.1 Introduction

The previous study reported in chapter 3 proposed a theory for phishing vulnerability. The theory suggests that "The success of phishing attempts is accounted for by the victims' personality traits, specifically Agreeableness, Conscientiousness and Extraversion. This general behaviour is moderated by individuals' knowledge and upsetting past security experience". The hypotheses generated by this theory are tested throughout the thesis.

Investigating individuals' phishing vulnerability is ideally done by measuring their response to a real (or a simulated) phishing attack (Jakobsson, 2007). The thesis reports two studies of this sort (field experiments). These are reported in chapter 5 and chapter 6.

However, most field experiments usually investigate individuals' phishing vulnerability by measuring their response to only one phishing stimulus (a phishing message or a phishing email). Accordingly, the design or the selection of this message should be done very carefully. Most importantly, this message should be thought to be *believable* by the users. In the quasi-experiment reported in this chapter, we investigate which mobile phishing messages are *believable* via showing conducting a phishing IQ test study. Phishing IQ is total scores derived from a phishing test designed to assess individuals' ability to detect phishing messages (Dhamija et al., 2006, Jakobsson, 2007, Sonic Wall 2016).

4.2 Aims

This section discusses the purpose of the study. The study aims to:
a) serve for the design of the coming two field experiments reported in chapter 5 and 6.
b) help us understand the psychological aspects of mobile SMS phishing via a lab experiment context.
c) investigate the first hypothesis (individuals' personality affect their phishing vulnerability).

4.3 Research Methodology

4.3.1 Method

The research method used in this study is phishing IQ tests. Phishing IQ-tests measures the ability of individuals to detect phishing messages. The test usually takes the form of screen shots of websites and/or emails that are shown to the users to classify to either phishing or legitimate ones. Phishing IQ-tests are widely available to help individuals assess their susceptibility to phishing attacks. Examples of these are Sonic Wall (2013) and Mail Frontier (2013). This type of phishing study can be effective in a number of aspects. These aspects are discussed below:

a) 'Believable' Vs 'Believed':

Phishing IQ tests can provide insights to what phishing messages are "believable" in contrast to which messages are "believed" which can be investigated via phishing experiments (Jakobsson, 2007). That is because IQ tests can help us understand what text messages would typical mobile users react to and why by measuring users' reactions to a sequence of stimuli. This cannot be done via field experiments which normally test users' response to only one phishing message, or otherwise, a severe increase in the sample size will be needed (Jakobsson, 2007).

b) Educational Purposes:

Phishing IQ tests have been proposed as an approach to educate users and also to measure phishing education effectiveness (Downs, Holbrook, Cranor, & 2007). This is often done by performing the test twice: before and after training, to measure if an improvement would occur in regards to users' ability to detect phishing messages as a result of the training.

c) Users' Interpretation:

Finally, the nature of phishing IQ studies permits an opportunity for a prolonged interview with every participant, through which they can explain reasons for their interpretations for each stimulus. This opportunity is not always available for phishing experiments, where the participants are normally not introduced to the true nature of the experiment (Finn and Jakobsson 2007)

4.3.2 Participants

Participants were all graduate students in Computer Science department, University of York. The study recruited 36 students, of whom 8 were women and 28 were men. The age of the participants ranged from 23 to 45 years old, with the most common age group being between 23 and 30. All participants were UK mobile users for at least 1 year at the start of the study.

4.3.3 Design

The study is examining the relationship between personality traits and IT-literate individuals' ability to detect phishing. The independent variable is the personality traits.

The study followed the 'closed-lab' quasi-experiment approach. The experiment incorporated a phishing IQ test where 12 mobile messages were shown to the participants. Half of which were authentic texts while the other half were captured phishing messages. Participants were asked to make a distinction between phishing messages and genuine ones. The study followed within-subject design, where every participant sees every message. The study took the form of a roleplay exercise. Roleplay is a well- established exercise in phishing IQ experiments. (Downs et al. 2007, Sheng et al., 2010, Mayhorn et al., 2015). In roleplay exercises, the participants do not behave as themselves but rather as an imaginary person described by the researcher. While pretending to be this person, the participants check a number of messages and tries to identify phishing ones. This design is specifically beneficial in cases where the researcher is interested to measure the participants' response to spear phishing attacks.

4.3.4 Instruments

This section discusses the instruments used to measure:

a) The pseudo-independent variable (predicting variable): participants' personality traits.

b) The dependant variable: Phishing vulnerability

c) The effect of a) on b) (effect of the pseudo-independent variable on the dependant variable).

a) Psychological Instrument

This section discusses the psychological instrument used in the study to measure pseudo-independent variable: the participants' personality traits.

The psychological domain used in this study to describe human personality is *the Five Factor Model* (FFM). It consists of five broad personality traits: Agreeableness, Conscientiousness, Extraversion, Openness and Neuroticism. The psychological instrument used to measure the FFM personality traits, in this study, was the *international Personality Item Pool* (IPIP).

The rationale for choosing both FFM and IPIP is discussed in chapter 2.

b) Phishing IQ-test

This section discusses the instrument used in the study to measure the dependent variable: the participants' phishing vulnerability (their ability to detect phishing).

Respondents' ability to detect phishing was measured via a phishing IQ-test that was composed of 12 mobile messages. Half of the messages were phishing messages, and the other half were genuine ones. The messages were presented to the recruits in paper format. The phishing messages were collected from a pool created and archived by the author over a period of a year.

The selection of the genuine messages:

The genuine messages were collected from real mobile texts sent by authentic service providers such as mobile operators, gas companies or Universities to their clients over their mobile phones.

The selection of the phishing messages:

Normally in phishing lab studies, the stimuli are gathered from phishing archives available online such as (Anti-Phishing Working Group, 2014, Millersmiles, 2013; Scamdex, 2013; phishme, 2014). However, to the best of our knowledge, there are no 'mobile' phishing archives published. For that reason, the author built her own database of real mobile phishing messages via networking. A Facebook page has been created for this purpose. The messages were then analysed, validated, and archived by the author.

The purpose of the analysis was to make sure that the archived messages were all phishing messages not legitimate messages mistakenly reported as phishing attempts. Analysing the content of the collected messages is a data-driven process that involves coding the collected messages to either phishing messages (and hence including them in the archive) or legitimate messages (and hence discarding them). To achieve this, every message was divided into:

a) Physically-defined segments: In this step, the following was checked:

i) The 'sender ID' unit: The authenticity of the number sending the message was investigated to check whether the number truly represents the party or the service provider it claims to be.

ii) The 'message body' unit: The message body was checked by dividing the message content into linguistically-defined segments (discussed below).

b) Linguistically-defined segments: In this step, the following was checked:

i) Links: The message content was checked to find whether there are any links to a replica (false version of an authentic website of a well-known bank or trusted organization).

ii) Action required: The message content was checked to find whether it requires the user to call or text a premium rate number, or to provide any Personally identifiable information (PII).

Purpose of the validation:

Following the guidance of Potter and Levine (1999), the process of analysing the messages discussed above entails two types of validity:

a) validity of the coding scheme that guides the researcher in the analysis of the content (Potter and Levine, 1999).

b) validity of decisions made by the researcher in relation to codes or labels produced (Potter and Levine, 1999).

To ensure such validity, it is recommended that more than one researcher conduct this process, and an inter-coder reliability is conducted to measure the degree of agreement among coders. If only one researcher conducts the analysis, measures need to be put in place to provide confidence in the archiving results. Below we list the measures the author has followed to ensure confidence in the results.

Measures applied to increase the coder reliability:

The following measures have been put in place to increase the coder reliability:

a) Intra-coder reliability measures have been used: the researcher conducted a test-retest for the data at different times as recommended by Mackey and Gass (2005) and Norris and Ortega (2003) in studies that involve researchers acting as their own raters. In test-retest method of reliability, the same analysis is performed by same individuals at two points of time. The researcher used one month as time interval between the two tests. phishing messages were archived where the data analysis was performed at time x was consistent with analysis performed at time y.

b) The use of peer-checking: As recommended by Mackey and Gass (2005), the researcher supervisor checked the coding procedure, in terms of the analysis procedures of the proposed phishing messages, and the resulting archive.

Phishing IQ-Test Messages Profiles:

a) Phishing Messages Profiles:

The phishing messages that were used in the IQ-test were chosen carefully to cover different levels of complexity, including both easily-identified mobile texts (such as 419 scams) and more sophisticated messages (such as spear phishing). Below we discuss the development of the complexity levels of the phishing messages.

Phishing Messages Complexity Levels

Based on phishing activity trends reports produced by The Anti Phishing Working Group (APWG 2015, APWG 2014), the phishing messages covered different levels of sophistication. The phishing messages complexity ranged from low, medium and high complexity. The phishing messages classification produced by Abu-rous (2010), and, Hong (2012) were also used to guide our selection. Below, we explain the context used for every level.

Low level of Complexity:

The messages that represented low level of complexity belonged to the 419 scam type. In this type of scams, scammers promise their victims a large amount of money or a big prize, and in return they ask them to pay a front payment (Jakobsson 2010). This scam is often referred to as a 'Nigerian scam'. Winning a lottery or a big prize, inheritance, debt relief, and accidents claims were classified as 419 scams (Boone-Lutz, 2007, Ismail 2003, Krebs 2015).

Three messages of this sort were used in three different contexts. These are discussed below:

Stimulus 1 (The Pepsi Award):

This phishing message purported to be sent by the famous carbonated soft drink company Pepsi. The message starts off with the phrase 'Lucky Winner'. It offers one Million Pounds as a reward for the lucky winner and asks the message receiver to send an email to a provided Hotmail email address to claim the money.

Stimulus 2 (The Debt Relief):

This phishing message purported to be sent by the government. It claims that the government has issued a clearance order for those in debt. The message asked the recruits to text the sending number back.

Stimulus 3 (The Accident Compensation):

This second phishing message purported to be sent as a settlement for a person who has had an accident recently. The message stressed that it is a free message twice in the text. It offered 2950 pounds for the claimant and asked the recruits to text the sending number back.

Medium level of Complexity:

The messages that represented medium level of complexity were of banking nature.
Two messages of this sort was used._These are discussed below:

Stimulus 4 (The Bank Account)

This phishing message purported to be sent by a bank that claimed that the account of the participant has been closed due to unusual activity. The message asked the recruits to call a 0800 number.

Stimulus 5 (The ATM Suspension)

This phishing message purported to be sent by a bank that claimed that the ATM card of the message receiver needs reactivation. The message asks the recruits to call a 0800 number for the reactivation.

High Level of Complexity:

Recently, phishing messages became more sophisticated using spear phishing attacks (Anti-Phishing Working Group 2014, Anti-Phishing Working Group 2014, Krebs 2015, Abu-rous, 2010, Hong 2012). Spear phishing is also called context-aware phishing. They can be defined as an attack that targets specific group at specific time (Dunham, 2004). These attacks may address the victims by their names or they may appear to be sent by an individual or a business that the victim knows.

Stimulus 6 (The Friend missed call)

The last phishing message purported to be sent by a friend who claimed to have tried to call the recruit yet got no answer. He asked for the recruit to call him back on an international number and left his full name. Although the message did not address the participants with their name, it used names from the participants' departments that they are familiar with.

Table 18 below classifies the phishing messages according to level of complexity and summarizes the main features of the messages.

Table 18: Phishing Messages

SMS	Main Features	Level of Complexity
Pepsi	Lucky Winner of £1 Million Pepsi Award 2011 Email:markjose65@hotmail.com	Low
Government Debt Relief	Incentive to text back	
Accident Compensation	Incentive to text back a Claimed free number	
Bank Account	Closed Bank Account for unusual activity Sender: Unknown number Requiring a Call Back	Medium
ATM Card	ATM Reactivation Sender: Unknown number Requiring a Call Back	
Friend Missed Call	Using familiar Names International Number	High

b) Genuine Messages Profiles:

The Context of Stimulus 7 (The University Enrolment)

This message was sent by the participants' university (University of York). In reality, the University administration used to send this message every semester to the students' mobile phones to remind them to enrol to the University system. The message asks the students to enrol online and provides a University web link for that. The message also warns the students that a fee of 30 Pounds would be payable for late enrolment and specify a date for that.

The Context of Stimulus 8 (The Gas Company)

This message was sent by 'British Gas' Company asking its customers to send their meter reading either via short message service or via the company website.

The Context of Stimulus 9 (The Dentist)

This message was sent by a dentist surgery in York; Clock House Dental. The message was a reminder of the routine check-up. The message was sent using a sender ID 'Dentist @' and asked the client to phone a York landline number starts with York code (1904) to book an appointment.

The Context of Stimulus 10 (The NHS)

This message was sent by the National Health Service (NHS). The message reminded the students to fill in the patient survey of the University NHS surgery (Dr.Price and Partners). The message used a sender ID 'NHS-No Reply' and sent the online link for the survey.

The Context of Stimulus 11 (The Mobile Company ad.)

This message was sent by the mobile operator 'Talk Mobile'. The message offered good rate for mobile internet and guided the message receiver to the company online link for further information. The message sender ID used was 'Talkmobile'.

The Context of Stimulus 12 (The Mobile Service Suspension)

This message was sent by the mobile operator 'Mobile World'. The message starts off with the word 'urgent' and warns the customers of a mobile service suspension. The message advised the clients who desire to keep their number to visit the company website. The message provided an online link and a code to use online for that purpose.

Table 19: Genuine Messages

SMS	Main Features
Dentist	Routine dental check-up Requiring a Call Back
NHS	Patient Survey Sender: Known Link:www.dr.priceandpartners.co.uk Wenlock.terrace.nhs.net
TalkMobile	Mobile Internet Offer: 30p per day Link:www.talkmobile.co.uk
Mobileworld	Mobile Service Suspension Alert Link:talkmobile.co.uk Code: MW010
University of York	Enrolment Alert Link:www.york.ac.uk/enrol Warning of late fee of £30
Gas Reading	Gas Reading Alert Link: www.britishgas.co.uk/meterreads Notice period of 5 days.

c) Statistical Instrument:

The effect of the pseudo-independent variable (Personality traits) on the dependant variable (Phishing vulnerability) was measured using the statistical application SPSS. SPSS (Statistical Package for the Social Scientists) is a data management and statistical analysis tool. It is used for its versatile data processing capability (IBM, 2016).

4.3.5 Procedure

The participants were recruited via advertising by email to the department of Computer Science students. The respondents were offered an Amazon voucher of five pounds and a free personality report. The recruits filled the IPIP personality questionnaire in a paper form. This was followed by a phishing IQ-Test.

An introductory briefing was given to the participants about the nature of the study and the meaning of 'phishing'. It was defined as a fraudulent attempt to acquire money and confidential information from people by impersonating legitimate entities. Participants were asked to play the role of a mobile user who interacts with a number of service providers who send her texts and updates on her mobile. The mobile user's characteristics and the service providers they interact with were given to the participants at the beginning of the study (See Appendix B).

Participants were presented each message in a separate paper. Each message was composed of two parts; the message sender (some in a form of a number and some in a form of an ID) and the message content. Every message was followed by 3 questions. In the first question participants were asked to rate the authenticity of the message over a 7 point Likert scale ranging from Definitely Phishing to Definitely Genuine. In the second question, participants were asked to explain the reason for their rating. The third question is a behavioural response question that asked the participants what their reaction would be towards the message. Options included; texting back, calling back, ignore or other to be specified by the participants.

After that, the participants were thanked and their personality reports were sent to them by mail.

4.4 Results

In this section we discuss the participants' responses to the messages. Then we explain how we measured the participants' phishing vulnerability, and the effect of personality on this vulnerability.

4.3.1 Participants' Responses to Messages

In this section we give a summary of the participants' responses to both phishing and genuine messages. Each participant expressed suspicion in at least two and in at most eleven of the twelve messages. The participant with the least number of suspected messages has detected only the *accident* and the *Pepsi* award messages. The participant with the highest number of suspected messages has rated all the legitimate advertisement messages as phishing attempts.

a) The phishing messages

The most phishing message detected was the *Pepsi award* message as none of the participants thought it was a legitimate message. The least phishing message detected with *the friend* message. This message was also the most to cause confusion to the participants. 28% of them could not decide whether it was a genuine or a phishing message. Table 20 summarizes the number of participants per message according to how they rate the message (a phish, a genuine or undecided).

Table 20: Suspicion in the Phishing Messages

Stimulus No.	Message Context	No. of Participants who rate it as a Phish	No. of Participants who rate it as a Genuine	No. of Participants who said 'I do not know'	Percentage Expressing Suspicion
1	The Debt	33	2	1	92%
2	The Accident	34	-	2	94%
3	The Friend call	19	7	10	53%
4	Pepsi Award	36	-	-	100%
5	The Bank account	24	3	9	67%
6	The ATM deactivation	25	6	5	69%

Below, we briefly review the phishing messages and generally discuss the recruits' behavioural responses to each.

Participants' behavioural response to Stimulus 1 (The Debt Relief)

All the participants except three successfully detected this message and rated it as a phishing message. The three participants stated that they would not text or call back to investigate. But, they thought such offer may exist in reality.

Participants' behavioural response to Stimulus 2 (The Accident Compensation)

None of the participants fell for this message. Only 2 were confused and said they are unable to make a decision.

Participants' behavioural response to Stimulus 3 (The Friend missed call)

This message in specific was the least detected by the participants. 25% of the participants said they will either call or text the sender back. It was also noticed that 71% of the participants who fell for this message scored low in both Extraversion and Assertiveness. This is consistent with the quantitative results, and will be discussed in details in the discussion section.

Participants' behavioural response to Stimulus 4 (The Pepsi Award)

There has been no difference in the participants' responses in regards to this message. All the participants were able to detect it was a phishing message.

Participants' behavioural response to Stimulus 5 (The Bank Account)

Only three participants fell for this message. They all scored low in Extraversion, which is again consistent with the quantitative results.

needs reactivation. The message asks the recruits to call a 0800 number for the reactivation.

Participants' behavioural response to Stimulus 6 (The ATM Suspension)

This message was the second most message (after stimulus 4, the friend missed call message) that deceived that participants. It was also noticed that this message got doubled the number (of participants) who fell for stimulus 5 (the bank message) despite that they both are of banking financial nature. For this, we got responses like *"This message is more convincing than the bank one"* and *"I'll respond immediately"*.

b) The Genuine messages

All the genuine messages were suspected by at least one participant (see **Table 21**). The most suspected message was the *Mobile service suspension* message (stimulus 12) the least suspected message was the *Dentist* message (stimulus 9).

Table 21: Suspicion in the Genuine Messages

Stimulus No.	Message Context	No. of Participants who rate it as a Phish	No. of Participants who rate it as a Genuine	No. of Participants who said 'I do not know'	Percentage Expressing Suspicion
7	The University	4	30	2	11%
8	The Gas Company	5	27	10	14%
9	The Dentist	3	31	2	8%
10	NHS	8	27	1	22%
11	The Mobile ad.	6	22	8	17%
12	The Mobile service suspension	19	9	8	53%

Below, we briefly discuss the recruits' behavioural responses to each.

Participants' behavioural response to Stimulus 7 (The University Enrolment)

Although this message is sent every semester to the students' mobile phones, 11% of the participants rated it as a phishing attempt. Some students said that they have to check their email first and to contact the

University administration for assurance. Others said "*Currently, the University contact me through mail or email, they have not used mobile messages for billing issues"*. They all scored low in Extraversion.

Participants' behavioural response to Stimulus 8 (The Gas Company)

13% of the participants rated it as a phishing attempt. We got responses like: "According to the role play, I'm a customer of British Gas. Yet, still, I would not use the number provided in the message". "I'll wait for the company to send someone to take the reading. I'll not contact them". "British Gas always estimate alternate bills and I'm sure they would NOT make things convenient for their customers", "This link is probably to download malware onto my computer". All these participants scored low in Extraversion.

Participants' behavioural response to Stimulus 9 (The Dentist)

Only 3 participants rated this message as a phishing attempt. No significant relation to the participants' personality was found.

Participants' behavioural response to Stimulus 10 (The NHS)

Although, almost all the University students are registered on NHS via the surgery mentioned in the message (that is located on the University campus), 22% of the students have rated its message as a phishing attempt. This survey has been sent regularly to the University students. 88% of these participants who rated the message as 'a phish' scored low to average on Extraversion.

Participants' behavioural response to Stimulus 11 (The Mobile Company ad.)

16.7% of the participants doubted the credibility of this message. The rationale they provided included the very cheap price offered and them not hearing about this company before. We got responses like: *"Price unrealistic", "never heard of them", and "Arbitrary company with no credentials"*.

Participants' behavioural response to Stimulus 12 (The Mobile Service Suspension)

This message was the most genuine message to be rated as a phish by the recruits. 53% of them suspected the authenticity of the message. The reasons they gave included; the brand name as well as the communication method. Also, the urgency of the message sent a false alarm to the participants that it is a phishing attempt. We got responses like: "I've never heard of a UK operator called mobile world", "No legitimate trust behind the URL", "Urgent messages tend to be spam", "Just trying to force users to a URL to install an exploit".

4.5 Quantitative Analysis

In section reports an investigation of the relationship between the pseudo-independent variable (Personality traits) and the dependant variable (phishing vulnerability) using statistical methods. We start by discussing data preparation of the variables measured then we examine the quantitative relationship between the variables.

4.5.1 Data Preparation

As the process of data measurement is central to quantitative research, we explain in this section how data were prepared for the analysis in terms of how they were scored in respect to each variable.

a) Measuring the Pseudo-Independent Variable Personality Traits:

As explained in section 4.2.5, participants' personality traits were measured using the standard personality tool IPIP. The results of the personality tool assign every participant a score (percentile) for every personality trait. These personality traits scores will be compared against the dependent variable (phishing vulnerability) as explained in the following section.

b) Measuring Participants' Phishing Vulnerability

In this section, we discuss how we measured the participant's vulnerability to phishing (i.e. their ability to detect phishing). The process of detecting which messages are phishing messages and which are genuine ones can be regarded as a binary detection problem (Wickens, 2002). The four possible outcomes are summarized in Table 22 where True Positive is when a participant correctly detects a text message as a phishing one. True Negative is when a participant correctly detects a text message as a genuine one. Hence, False negative would be when a participant mistakenly detects a phishing text as a genuine message. This means the participants have fallen for the phish. Finally, False Positive is when participant mistakenly identifies a legitimate text message as a phishing one.

Table 22: Binary Detection Table of Phishing

		Participants think the message is:	
Actually the message is		Genuine	Phishing
	Genuine	True Negative	False Positive
	Phishing	False Negative	True Positive

Table 23 below shows the mean number of the texts correctly detected in each category. The participants were more accurate in detecting phishing messages (mean = 4.75) than genuine ones (mean= 4.06).

Table 23: Binary Detection mean and Standard Deviation

		Participants think the message is:		
		Genuine	Phishing	Undecided

Actually the message is:	Genuine	Mean= 4.055556
		SD=1.286
			Mean=1.25
			DE=1.251
				Mean=0.75
				SD=0.685344

	Phishing	Mean=0.50
		SD=0.775
			Mean=4.75
			SD= 1.105
				Mean=0.694444
				SD=0.850696

To interpret the binary results of the binary detection, two measures were calculated: Accuracy and precision. Below we provide an explanation of both terms, and how we used them to measure users' ability to detect phishing.

According to ISO (1994) 'Accuracy' refers to how close a measured value is to the actual (true) value, while, 'Precision' refers to how close the measured values are to each other. As Figure 13 shows, individuals that are high in precision but low in accuracy, will have their score close to each other, but not necessarily at the right direction that they should aim at.

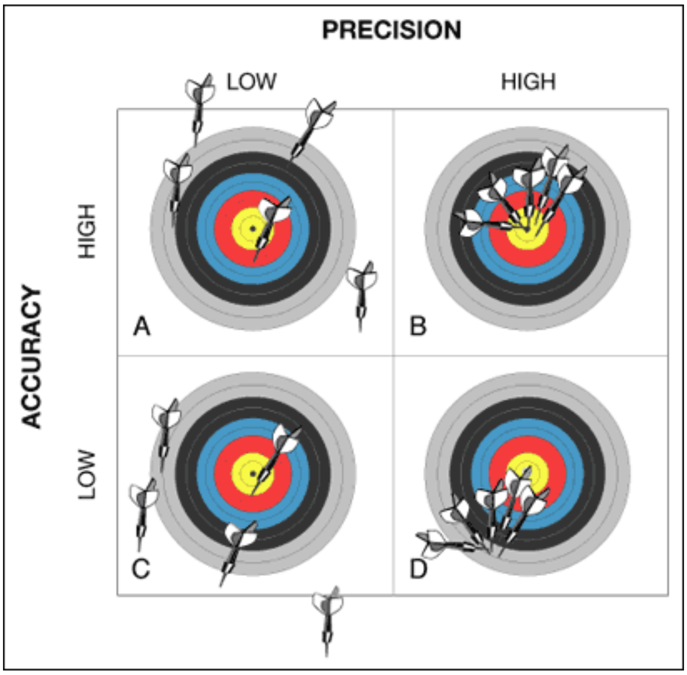


Figure 13: Illustration of precision and accuracy (Mapp & Ono, 2006)

For our study, Accuracy refers to the percentage of correct answers out of the total answers. Precision refers to the percentage of correct positives of all the positive responses, where positive refers to detecting message as a phishing (as explained in table 13). Below is how each was calculated.

Accuracy= (Number of True Positives + Number of True Negatives) / (Number of all possibilities)
Precision= (Number of True positives / Number of all positives (True and False)

4.5.2 Measuring the Effect of Personality on the Participants' phishing vulnerability

In this section we discuss how we measured the effect of personality on participants' accuracy and precision. First, we discuss how we chose that statistical approach for modelling the relationship between the variables. Then, we report our interpretation of the statistical results.

a) Choosing the statistical approach:

A linear regression analysis was conducted to investigate the relation between the participants' personality traits and their accuracy and precision scores. Linear regression predicts on one variable from one or more independent variables. As we have multiple personality traits on one side to compare against two dependent variables (accuracy and precision) on the other side, multiple regression was suited for our analysis. Multiple regression helps answering the following questions: do the predicting variables (personality traits) predict which of the two categories on the dependent variable, the person falls into? Question 2: are all the independent variables or only part of them predicting the participants' response? Question 3 what is the relative importance of the independent variables, as it answers the question which of these independent variables is most useful in predicting phishing response?

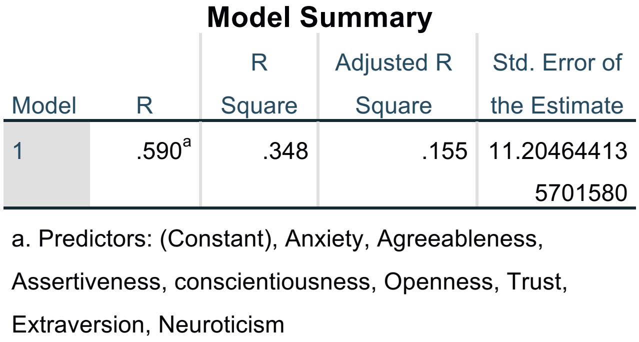
b) Statistical Analysis

To investigate the relationship between the participants' personality traits and their accuracy and precision scores, the software package SPSS and an alpha level of 0.05 were used. The method used for multiple regression is 'Entry'. The rationale behind using such method is that it does not require the data to be normally distributed in contrast to 'stepwise' method that may lead to results biases if the data is not normally distributed (Chatfield, 1995; Whittingham, Stephens, Brandbury & Freckleton, 2006).

i) The Effect of Personality Traits on Accuracy

The analysis shows correlation between the participants' personality traits and their accuracy in detecting phishing messages. 15.5 % of the total variability in the participants' accuracy is explained by their personality traits, as reported by the Model Summary below in **Table 24**, where the adjusted R square = (.155).

Table 24: Accuracy Model Summary



Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.590[a]	.348	.155	11.204644135701580

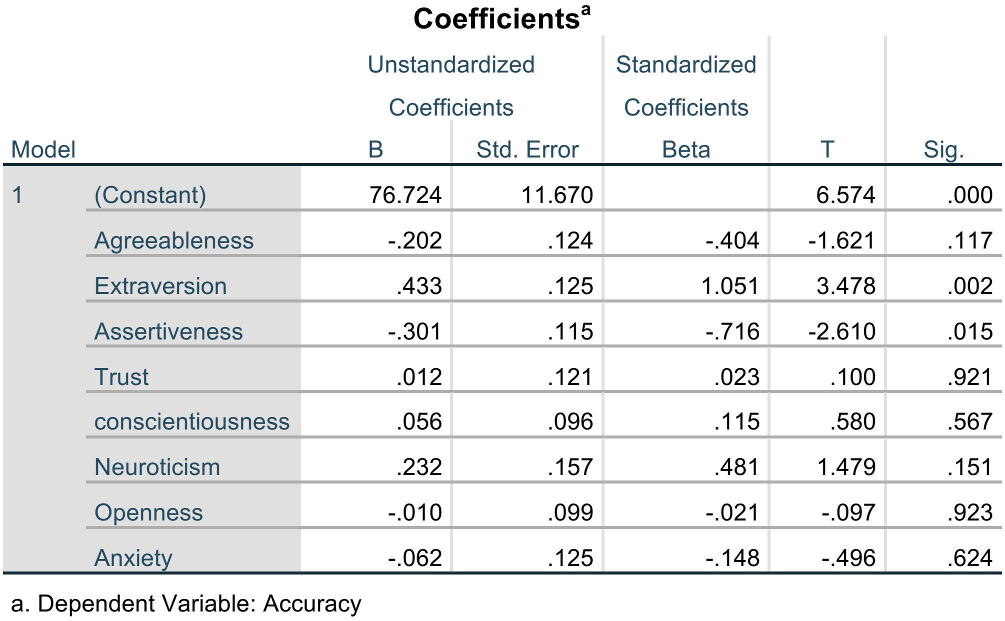
a. Predictors: (Constant), Anxiety, Agreeableness, Assertiveness, conscientiousness, Openness, Trust, Extraversion, Neuroticism

In regards to which personality traits proved to be significant, and which did not, the analysis shows that Extraversion personality trait significantly predicts the participants' phishing detection accuracy (Beta= 1.05, p< .05). This suggests that participants who score high in Extraversion are more likely to accurately detect phishing messages.

The analysis also shows that Assertiveness personality trait significantly predicts the participants' phishing detection accuracy (Beta= -.716, p< .05). This suggests that participants who score high in Assertiveness are less likely to accurately detect phishing messages.

These results are summarised in Table 25 below.

Table 25: Accuracy Coefficients



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	T	Sig.
1	(Constant)	76.724	11.670		6.574	.000
	Agreeableness	-.202	.124	-.404	-1.621	.117
	Extraversion	.433	.125	1.051	3.478	.002
	Assertiveness	-.301	.115	-.716	-2.610	.015
	Trust	.012	.121	.023	.100	.921
	conscientiousness	.056	.096	.115	.580	.567
	Neuroticism	.232	.157	.481	1.479	.151
	Openness	-.010	.099	-.021	-.097	.923
	Anxiety	-.062	.125	-.148	-.496	.624

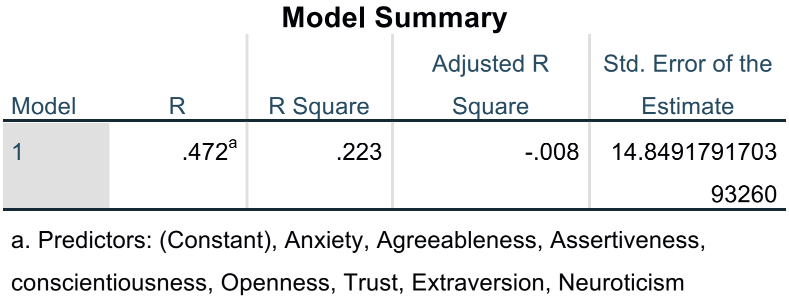
a. Dependent Variable: Accuracy

ii) The Effect of Personality Traits on Precision

The analysis shows correlation between the participants' personality traits and their precision in detecting phishing messages. 0.8 % of the total variability in the participants' precision is explained by their personality traits, as reported by the Model Summary below in

Table 26, where the adjusted R square = (-.008). The negative adjusted R square can occur when the test investigates high number of variables over small sample size. This also means that the independent variables explanation of the dependent variables is very low.

Table 26: Model Summary



Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.472[a]	.223	-.008	14.849179170393260

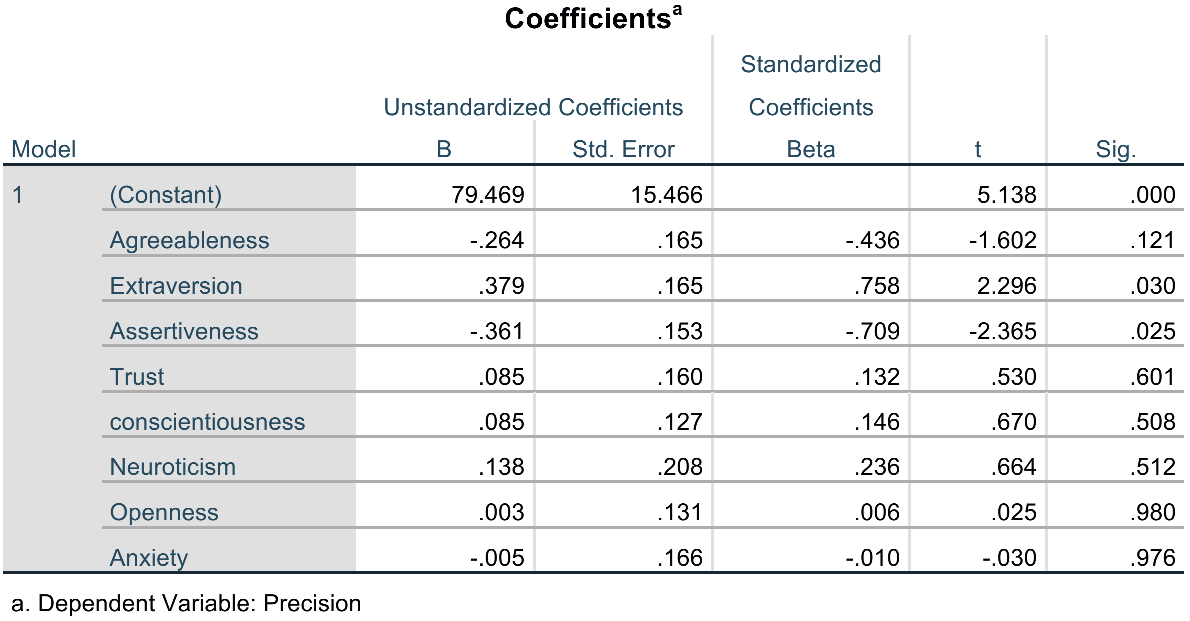
a. Predictors: (Constant), Anxiety, Agreeableness, Assertiveness, conscientiousness, Openness, Trust, Extraversion, Neuroticism

The analysis shows that Extraversion personality trait significantly predicts the participants' phishing detection precision (*Beta*= *.758*, *p*< *.05*). This suggests that participants who score high in Extraversion are more likely to precisely detect phishing messages.

The analysis also shows that Assertiveness personality trait significantly predicts the participants' phishing detection precision (*Beta*= -*.709*, *p*< *.05*). This suggests that participants who score high in Assertiveness are less likely to precisely detect phishing messages.

These results are summarised in **Table 27** below.

Table 27 : Precision Coefficients



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	79.469	15.466		5.138	.000
	Agreeableness	-.264	.165	-.436	-1.602	.121
	Extraversion	.379	.165	.758	2.296	.030
	Assertiveness	-.361	.153	-.709	-2.365	.025
	Trust	.085	.160	.132	.530	.601
	conscientiousness	.085	.127	.146	.670	.508
	Neuroticism	.138	.208	.236	.664	.512
	Openness	.003	.131	.006	.025	.980
	Anxiety	-.005	.166	-.010	-.030	.976

a. Dependent Variable: Precision

Interpretation of the results

The results indicate that two personality traits significantly correlate with individuals' accuracy and precision in detecting phishing messages. These are Extraversion and Assertiveness personality traits. The individuals who score high in Extroversion are more likely to able to detect phishing messages. The individuals who score high in Assertiveness are less likely they to be able to detect phishing messages.

The positive effect of Extraversion personality trait on the participants' accuracy and precision in detecting phishing messages can be explained by the fact that extroverts are more socially engaging individuals and hence are more likely to be aware of phishing scams that are widely spread than introverts who are withdrawn in nature (Adali & Golbeck, 2014). This is consistent with the results of Halevi et al. (2013), Korzaan & Boswell (2008) and Pattinson et al. (2012) whose research concluded that extroverts are less likely to fall for phishing.

The negative effect of Assertiveness personality trait on the participants' accuracy and precision in detecting phishing messages can be explained by the fact that assertive people are more quick in making decisions (Peterson, 2007; John & Soto, 2008). This may lead to making decisions without showing careful thought, which may lead the individual to mistakenly trust phishing messages. To the best of our knowledge, the present research is the first to discuss the relationship between the personality trait Assertiveness and phishing vulnerability. However, the effect of assertiveness in making speedy decision was investigated by a number of scholars in different sectors, such as the business sector (Wally & Baum, 1994), and the education sector (Wehmeyer, Agran & Hughes, 1998).

4.6 Qualitative Analysis

Having the personality trait *Extraversion* been indicated as a personality trait that may affect individuals' ability to detect phishing by the quantitative analysis reported in section 4.4, the author sought to explore other psychological aspects involved in mobile SMS phishing interaction (via a lab experiment context). For this purpose, a qualitative approach was adopted for this section of the study.

4.6.1 Method

The qualitative analysis was submitted to thematic analysis (Boyatzis, 1998). Thematic Analysis is a method for identifying, analyzing and reporting underlying themes within data (Braun & Clarke, 2006). Because it helps clarifying different aspects of the research topic, a number of researchers characterize thematic analysis not as a method but instead as a tool to use over different methods (Boyatzis1998, Ryan & Bernard 2003, Braun & Clarke, 2006). It is widely used in qualitative research as it introduces order, structure and rich interpretation to qualitative data (Marshall & Rossman 2006, Braun & Clarke, 2006). Boyatzis (1998) offered a definition of a theme, which is the product produced by thematic analysis, as "a pattern in the information that, at minimum, describes and organizes the possible observation and at maximum, interprets aspects of the phenomenon" (p. 161). It is also defined as "an abstract entity that brings meaning and identity to a current experience" (DeSantis & Ugarriza, 2000).

Thematic analysis was suited for our analysis, as we are looking for patterns in the data that explain and justify users' behaviour in terms of phishing detection. It was also recommended for analysing discourse, as it helps analysing data sets and data items. This will be suitable for analysing the participants' data into two datasets: victims and detectors and them analysing every response (data item) within each data set.

4.6.2 Thematic Analysis

The thematic analysis was employed by following the guidelines suggested by Braun and Clarke (2006). Accordingly, our thematic analysis went through the following six phases:

-Familiarizing with the data
-Generating initial codes
-Searching for themes.
-Reviewing themes.
-Defining and naming themes
-Producing the data analysis report.

Below, we explain how we applied these steps below.

We will use the term as 'data corpus' to refer to all the data collected from the participants in the study how they identified the phishing and genuine messages, and what action they plan to take: ignore, call back, text back, etc.). We will use the term 'data set' to refer all the data collected from the corpus for a particular analysis. We choose here two data sets based on the source of the data: 'victimisation' or 'detection' for every message. We will use the term 'data item' to refer to the individual pieces of data, i.e. the components of the data set.

a) Familiarizing with the data

We aimed to get familiar with the breadth and depth of the data. As recommended by (Braun and Clarke (2006), we achieved this immersion with the data by reading the data in an effective way (by looking for patterns and meanings). The process we followed in repeated reading is by reading the entire dataset before we start the coding process reading through the answers of each participant. Our reading process was informed by the type of analysis we aimed to achieve. So prior to the reading process, a decision was made in regards to the type of thematic analysis we aim to achieve. Basically, there are two approaches for thematic analysis: inductive or theoretical 'deductive' (Braun and Clarke, 2006). In the inductive approach, the themes identified may bear little relationship to the specific questions asked in the data collection process. In the theoretical approach, the analysis is mainly driven by the researcher's theoretical interest. That's why this approach is referred to as 'top down' approach. The analysis of the data collected by the participants will follow this theoretical approach, as it permits more detailed analysis on certain aspects of the data, that mainly answers the proposed research questions we are interested in: why and how the participants either detect or fall for the phishing messages they have been shown. Accordingly, the way we read the data was driven by this approach, and hence, while reading the data, we were interested in the way the participants have dealt with each message, what factors in the messages have affected the way they identified phishing messages and what strategies they followed to make their decision. Also the time used via transcribing the data from the notes into more comprehensive documentation helped develop thorough understanding of the data, as repeated issues were noticed and ideas were marked to help for the coding phase.

b) Generating initial codes

After generating a list of relevant issues and ideas in phase 1, in phase 2 we aim to produce initial codes from these ideas. Codes refer to the most basic elements of the raw data that can be assessed in a meaningful way regarding the phenomenon (Boyatzis 1998). Below we explain the process we followed in generating our codes.

Our coding of the data was 'theory-driven', as we approached the data with specific questions in mind representing 'how', 'what' and why' questions: how the participants identified the messages? What were their strategies to interact with the messages, and why they chose to make their decisions the way they did?

Coding was done manually by using 'post-it' notes to identify any interesting aspects in the participants' data that may form potential patterns. Then these data extracts were copied to a computer file along with some surrounding relevant data, as recommended by Bryman (2001) to make sure context is not lost. This was repeated systematically through the two data sets with full attention paid to each individual data item.

Below is a sample of codes applied to a data extract from 'detectors' dataset. Table 28 Below shows an example of initial codes.

Table 28: Example of Initial codes

Data extract	Coded for:
"Government does not send SMS, they send official letters" "Text messages are not an official way"	-Expecting letters -Suspicion of using texting as a communication method.

c) Searching for themes

After all the data have been coded in phase 2, in phase 3, an interpretative analysis of the data took place looking for broader levels of patterns (themes). This process involved:

- Sorting the codes produced in phase 2 into potential themes.
- Combine relevant codes to form a joint theme.
- Form different levels of themes.

This process has been performed for our two datasets (victimization and detection). A thematic map was used to help find relationships between codes, themes, and different levels of themes. This produced candidate themes and sub-themes. We did not discard any significant themes at this stage, even themes that did not belong under any main theme, were mapped as well temporarily till the next phase for possible refinement. Initial thematic mind-maps of the datasets that represent victimization and detection themes are shown in **Figure 14**, and **Figure 15** below.

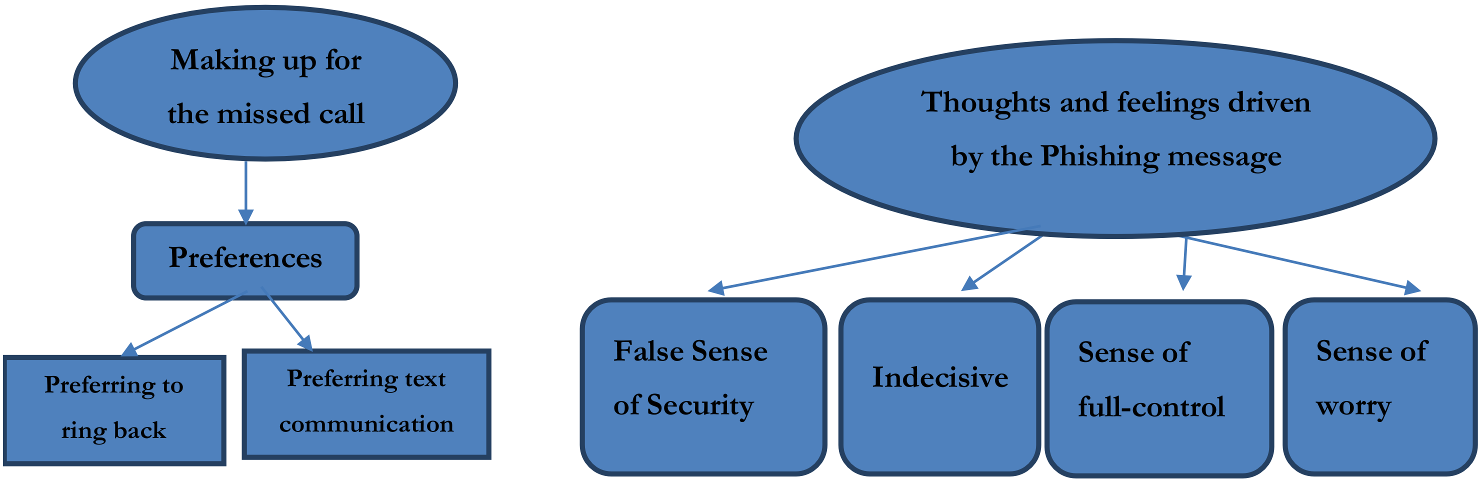

Making up for the missed call
Preferences
Preferring to ring back
Preferring text communication
Thoughts and feelings driven by the Phishing message
False Sense of Security
Indecisive
Sense of full-control
Sense of worry

Figure 14: Initial Thematic Mapping (Victimisation Dataset)

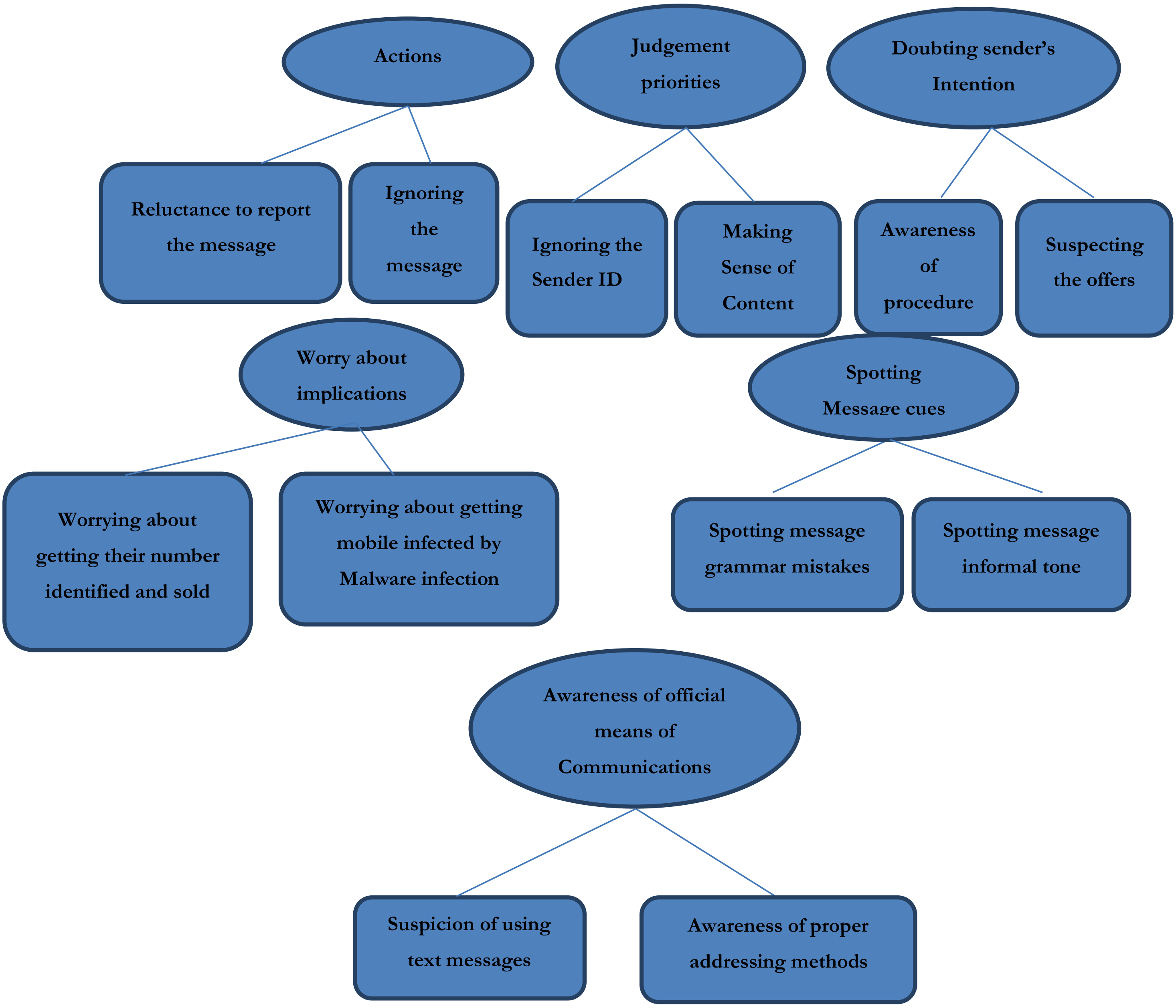

Actions
Reluctance to report the message
Ignoring the message
Judgement priorities
Ignoring the Sender ID
Making Sense of Content
Doubting sender's Intention
Awareness of procedure
Suspecting the offers
Worry about implications
Worrying about getting their number identified and sold
Worrying about getting mobile infected by Malware infection
Spotting Message cues
Spotting message grammar mistakes
Spotting message informal tone
Awareness of official means of Communications
Suspicion of using text messages
Awareness of proper addressing methods

Figure 15: Initial Thematic Mapping (Detection dataset)

d) Reviewing themes

This phase is responsible for the refinements of the candidate themes generated in phase 3. This refinement was made via two levels of reviewing the themes. In this first level, we read and reviewed all the coded data extracts to check if they form a coherent pattern. In the second phase, we revisited the relation between the themes and the datasets (victimization and detection). Accordingly, changes were made to the thematic map. For example, the theme 'receiving mixed signals' was placed under a new theme 'deception' in the victimization dataset, and the theme 'doubting sender's intentions' and 'suspecting the offers' were merged together under a new theme in the detection data set. The process was repeated till no more refinement is adding any substantial changes.

e) Defining and naming themes

In this phase, we identified the essence of every theme to make sure the name reflects what each theme is about. This was done by going back to the collated data extracts for every theme, and make sure that the themes make a narrative that represent both datasets. For example, for the detection dataset, the main themes covered 'why' the participants doubted the phishing messages, 'how' they were able to detect them, and 'what' actions they plan to take for each message. Examples of these themes included: 'judging the relevance of the message content before its authenticity', 'suspicion of the communication channel used', and 'awareness and concern about the implications'. For the victimization dataset, themes covered what' instilled the participants' trust in the messages, 'what caused the participants to be duped' and 'the effect of persistence communications by the attacker'.

f) Producing the data analysis Report

In this section, we report the main themes that showed prevalence in the data analysis for both datasets 'detection' and 'victimization'. In each of the subsections below, we identify a significant theme. A more general interpretation is provided in the discussion section. In reporting the thematic analysis, we rely heavily on quotations from the participants to 'provide sufficient evidence of the themes within the data', as recommended by Braun and Clarke (2006, p.23).

The established categories used for the thematic analysis involved two major domains. The first was the 'Themes leading to detection', which included themes discovered via discussing phishing messages being detected by one or more of the participants. The second was the 'Themes leading to victimization', which included themes discovered via discussing the phishing messages that succeeded in deceiving one or more of the participants

4.6.3 Major themes leading to detection:

For the detection category, the thematic analysis revealed 16 thematic elements mapped into 6 cognitive processes. Table 29 below presents the major themes and sub-themes for the first category (Detection).

Table 29: The Themes Leading to Detection

Theme	Subcategory
1.Impossibility	a. Un-attainability of offer. b. Impracticality of the process. c. Doubting the senders' intentions. d. Hopelessness
2.Judging Relevance before authenticity	No Subcategory (content, addressing)
3.Suspicion of the Communication Channel	a. Suspicion of the use of mobile text messages. b. Suspicion of the absence of sender ID.
4.Awareness and concern about Implications	a. Concern about further communication. b. Concern about malware download. c. Awareness of common attacks.
5. Considering the media as reference.	No Subcategory
6. Rational thinking/spotting phishing cues in the message	a. Questioning the means by which their mobile numbers were obtained. b. Questioning the reason for which their mobile numbers were obtained. c. Questioning the oddity of the sender number. d. Evaluating the prize offered. e. Spotting unofficial email addresses. f. Presentation

1- Impossibility – Offer, process, Intentions, Hope

Phishing messages that have put forward generous offers, such as debt clearance and big prize awarding, were regarded by the participants as implausible. Some participants stated that these offers are unfeasible.

"Complete debt write-off is impossible"

"The message does not make any sense, so it must be ignored"

"It is too good to be true", "unbelievable"

The participants stated that it is very unlikely for legitimate institutions to offer debt forgiveness.

"I doubt the government would come up with such a deal"

"No government ever wiped off its citizens' debt"

The participants also discussed the easiness of the process claimed and the lack of specific course of actions required. They found it impractical.

"Wiping off debts without official procedures is not convincing at all"

Doubting the intentions of the sender was considered by the participants for evaluating the messages.

"No one would offer that without wanting something in return"

"Definitely phishing, why would anyone dole out 1 Million pounds without even buying a lottery ticket?"

In regards to messages that offered prizes, the participants showed hopelessness.

"Nothing in the word is free"

"I am not lucky enough"

Many of these quotations reflect on the last step in making decision (discussed in chapter 2), when an individual refers to his assumptions and own abilities.

2- Judging Relevance before Authenticity- Content, Addressing

Participants were more likely to mistrust the messages that were irrelevant to them either for being out of their concern, for certain security settings they have arranged with their financial institutions, or for certain life style they are accustomed to.

"I do not have any debt",

"I didn't have any accident"

"I don't allow mobile banking messages"

It is also worth mentioning that some participants stated that one of the reasons they ignored some phishing messages was that they did not address them by their name.

3- Suspicion of Communication Channel- Texting, Sender ID

The participants' decision was affected by the communication channel via which they received the message. They expected the government, in specific, to communicate with the public by letters of correspondence rather than by mobile text messages.

"Government does not send SMS, they send official letters"

"Text message is not an official way, the government should have other official ways to inform me"

The same applies for banks.

"Banks do not normally send text regarding account management, more formal methods, like letters or messages to the internet banking inbox"

Several text messages were dismissed based on their sender, especially, the bank messages and mobile operator messages.

"Normal number not HSBC", "Normal number not O2"

"Unknown number"

Some participants applied this rule to all messages even if sent from individuals.

"I ignore numbers I do not know"

"I do not trust unknown numbers"

4- Awareness and Concern about Implications- Further communication, Malware, Common Attacks. Participants were worried in regards to the implications of their responses to the messages. Some were concerned that their reply may encourage the sender to keep annoying them in the future. Others were afraid that their reply may encourage the sender to sell their number for potential attacks.

"I'll ignore, because no matter what text I send, the scammers will record my number as 'active' and continue sending messages", "Possibly sent to random numbers. So, I'll ignore to avoid further attention", "If I replied, they would know my number is 'real' and would sell it".

The participants could relate some of the phishing messages to common real attacks. They referred to messages that aim at defrauding the victims for monetary gain and those offered compensation for claimed accidents.

"This is a classic 419 scam"

"I know loads of people who receive these messages despite having no accidents"

5- Considering the media as Reference

The participants regarded some of the offers as lacking proper publicity. The fact that these offers have not been made public elsewhere, made the participants doubt the legitimacy of the message. They wondered why the claimed offers are kept covert rather than getting advertised in more official manner. For example, they have expected the government would seek praises from the public if an actual decision has been made to clear debts.

"Government does not wipe out debts without a lot of press", "If it were true, it would be announced through the media, not through text to me!", "If there was any such scheme, it must have been in the news"

6- Spotting Phishing cues

A common theme among detectors was their success in spotting some phishing cues in the messages. This included poor grammar, the exaggerated value of the prize, the use of unofficial email addresses, and the oddness of the sender number.

"The number to call looks fishy"
"The message does not mention anything about which bank account and why"
"The email address does not sound professional; it does not carry the signature of the organization organizing the lottery", "It's a personal email address", "Markjose56@hotmail=not Pepsi"

Presentation and style affected the participants' opinion of the messages. For example, poor grammar and shoddy style were detected.
"Sloppy Grammar!"
"Language has an informal tone"

Even the wording of some messages irritated the participants. In specific, they stated that the use of certain words such as 'Winner' and 'Free message' made them believe these are phishing messages.
"Why they said Free MSG! This creates doubts. That's why I consider it phishing"
"Winner?!! Everything about this message is dodgy"
"The word 'Free MSG' indicates something is tricky"

The participants also questioned the means and the reason for which their mobile numbers were obtained.
"Why would the government have my number?"

4.6.4 Major themes leading to victimisation:

For the victimisation category, the thematic analysis revealed that 5 thematic elements were indexed and mapped into 3 areas of cognitive processes. **Table 30** below presents the same data for the second category (victimization).

Table 30: The Themes Leading to Victimisation

Themes	**Subcategory**
1.Deception	a. Receiving Mixed Signals b. Lack of knowledge about some phishing techniques
2.Trust	a. Worrying about missing important communication. b. The use of common names.
3.Response to Persistent Communication	No subcategory

1- Deception – Mixed Signals, New phishing Techniques

A common theme among the participants who said they would respond to some of the phishing messages, was expressing being duped by some messages. They felt that some of the messages gave them mixed signals. An example is the message that claimed to warn them of a bank account deactivation and asked them to call back an unknown number. They felt the absence of the name of the bank is fishy. However, they were confused because no confidential information was asked. This gave them a false sense of security. They decided to respond at the end.

"Giving a number to call in the message raises alarm bells, but giving complete control also removes the doubts"

"Tricky! It does not specify which account has been closed. So it could be poorly-expressed legitimate message or a clever phishing attempt"

Some participants were reluctant to call an unknown number. Yet, they decided to alternatively, text back. They stated that texting is safe. Apparently, they mistakenly thought that they would pay for a premium number only if they called, not texted. In their responses to message 4 that pretended to be from a friend, they said: ***"So, I'll text back. This sounds the logical approach as a sinister motive might be behind making me call and charge me unwittingly"***

Others were not aware of premium rate numbers at all. Although, the number provided in some of the messages was international, they decided to follow the phisher request and ring back.

"I'll call and ask", "If the message is not genuine, then I can find out on calling the number"

In regards to the bank message, we got same responses: ***"I'll call back to find out how true the text is by asking them to provide me more details such as my phone number, then after I know from which bank they are calling, I'll go directly to my bank"***

2-Trust

The participants revealed there were some trust indicators in the messages. One of which is the employment of common names that could be easily recognized. An example of this is the fourth stimulus that purported to be from a person who was trying to communicate the victims and asked them to call back. The use of familiar names such as 'Paul' and 'Clark' gave an authenticity to the message. Many participants did not even notice that the sending number was international.

Some recruits actually believed the message so that they were treating the purported friend name as the sender of the message.

"I'll call Mr.Paul Clark"

Some went further and said they already knew the people who tried to contact them: ***"I recognize the names; I'll call back"***

Some participants were willing to call or text back the message sender even though they did not recognize the names because they were keen not to miss a call that might be important. For the same stimulus (message 4), we got the following responses:

"I am not expecting any call from J.Paige or Paul Clark & I don't know any of those. But it might be genuine, I'll call back to find out what are they calling for"

"Not sure about the number and the name, I'll text him back, I think it might be important to me to check the person name and the reason of the call"

For the stimulus of financial nature (messages 7 and 8), some participants seemed convinced of the message content: ***"I'll call back, I have to be sure that this is true, and that I did not do any unusual activity",***

"My ATM card is with me and in these occasions they will call me not text. I'll send them a text to ask for the reason to deactivate the ATM card"

3- Response to Persistent Communication

The persistence of the attacker was one of the reasons the participants have suggested that may encourage them to respond to him. They stated that they are more likely to interact with the sender of the message if it was followed by another message, otherwise, they would ignore it.

"As long as this is the first time, I'll ignore it", "Only if they call again", "I'll wait for them to call again"

It was also noticed that the recruits seemed looking for clues from the attacker to urge them to respond.

"If I found a missed call, then it may be genuine, otherwise it's definitely not"

4- Mobile Users' Strategies:

The study also indicated a number of strategies that mobile users use interacting with the messages. To the best of our knowledge, this is the first research that reports mobile users' strategies in response to phishing attacks. We list them below.

-Google it

Many participants stated they would individually verify the phone numbers proposed in the messages by goggling it via the internet to make sure they are the correct numbers.

-Use own contacts

Very few said they would call the phone numbers they already have, either for their banks or other service providers such as their mobile operators, gas or electricity company. This applied as well for websites.

-Ignore it

Most of the participants chose to ignore the messages that were either not related to them or messaged they had doubts are phish. Some of them stated they ignored the messages to save their time. *"no time to waste on these"*, they said. Other reason was despair that an action could be made against the attacker, *"I'll ignore, bcz, there is no use of reporting it to my operator", "Even if they manage to block this msg from now on (which I doubt), Attackers will just come up with other phishing messages."*, they said. Feeling that the attackers have many ways to attack, was another reason for despair, *"I may consider contacting my operator to block the number, but I'm fairly sure the phisher could simply switch to another number"*, they said. Others simply felt it is sensible enough to ignore such texts, *"There is no point of replying to a phishing message"*, they commented. Some recruits chose to ignore the messages as a rational response to a communication they did not even ask for, *" I donot know how the company got my mobile number, and, it seems wrong that I tell them to 'stop' given that I never asked them to send me adverts in the first place"*, frustratingly they said.

-Waiting Policy

Some recruits chose not to respond to messages they were not sure are legitimate, but instead wait for the phisher to take the next step either by calling or texting them again.

-Respond

In responding to the stimuli, the participants chose either to call back or text back the number sending the messages.

4.7 Discussion

The first objective of the study was to serve for the design of the coming two field experiments reported in chapter 5 and 6 by providing the context for these experiments. Hence, we will start by discussing the participants' view of the context of the messages shown to them.

Factors that lead to trust: The participants' decisions were consistent with the recent phishing trends which showed a decline in certain types of phishing messages which used to deceive lots of online users in the past (Anti-phishing Working Group, 2014). These include messages that offer the users a large amount of money or a big prize. 100% of our participants were able to successfully detect messages of this sort (i.e. award message), and expressed that such messages are standard forms of phishing.

Instead, messages that were least detected by the participants, were those which used 809 scams, specially those purported to be sent by a friend, and those of financial nature. 809 scams are mobile phishing messages that trick the mobile users to call or text a premium-rate number. The participants who were deceived by such messages expressed that they were unaware of these sorts of attack, and that they were under the impression that it is safe to text or call back. This is similar to what Jakobsson concluded that people are more vulnerable to less common attacks (2007). Also, the use of common names in the message highly affect its response rate. The participants were worried that someone they know was trying to reach them, and that this purported missed call may have been trying to communicate valuable information, specially that the message did not ask 'ostensibly' for any confidential personal or banking details. Similarly, the banking messages which asked the users to call a certain phone number, were able to confuse the participants to a great extent. Nearly one third of the participants were not able to detect such messages. Noticeably, these messages used 'fear' to attract the users to respond. Examples include messages that warn the users of their bank account closure, email account deactivation, or ATM card invalidity. This technique is in line with behaviour science research that states that fear can be effective in making individuals pay attention. They explain that in cases where moderate levels of fear are used and a solution is provided, users are more likely to respond (Pfleeger and Caputo 2012, Petty and Cacioppo, 1984). The use of a discomfort feeling to attract people and affect the way they behave has been also discussed in the theory of cognitive dissonance. The theory explains that cognitive dissonance, which is a feeling of discomfort that results from holding two conflicting thoughts at the same time, is central to many forms of persuasion (Pfleeger and Caputo 2012, Harmon-Jones, 2002). The participants explicitly stated that such messages caused confusion as they did not ask for any private details, which can create trust. Yet, the message did not mention the name of the bank of which it warns the users that their account is subject to closure. Not mentioning which bank made the users doubt the legitimacy of the message. Nearly half of the users who felt confused responded to the message at the end.

The second objective of the study was to help us understand the psychological aspects of mobile SMS phishing via a lab experiment context. In this regard, one of the interesting findings of the study is that the participants judge the message via its content relevance before checking its authenticity. In particular, any message that offered money prize was identified as phishing. This is in line with the findings of a lab study performed by Tsow and Jakobsson (2007). They noticed that the users identify any message that asks for passwords as phishing. Jakobsson (2007) view this as a problem because users can be attracted to a phishing website by an information only email. This is very similar to our results in regards to 809 scams that earn users' trust by not asking for any confidential data or offering any monetary awards, but rather asked the user to ring a certain phone number. Judging relevance before authenticity can cause problems for companies that use mobile SMS for advertising purposes, or service providers who are publicizing customers' offers. Similarly, our participants mistakenly identified a message from their University as a phishing message, when it sent a reminder for fees payment.

Finally, the study investigates the first hypothesis (individuals' personality affect their phishing vulnerability). The results indicate that the personality trait *Extraversion* positively affects people's accuracy in detecting phishing attacks. Extrovert individuals are more likely to accurately distinguish between phishing and legitimate messages. This finding is counter-intuitive as one may assume that extrovert individuals, being sociable and open to new relations (Adali & Golbeck, 2014), would be more likely to trust others and hence fall for phishing messages and believe they are legitimate ones. The accuracy of extroverts can be explained by their tendency to enjoy human interaction and being around people which made them more knowledgeable about phishing attacks trends, and hence are able to identify them. Our results were consistent with other research in the field such as the work of Halevi et al. (2013), Korzaan & Boswell (2008) and Pattinson et al. (2012).

The results also indicate that the personality trait *Assertiveness* negatively affect people's accuracy in detecting phishing attacks. The more assertive the person is the less likely that they will be able to detect phishing. This result can be explained that assertive people who may rush into making decisions quickly may miss noticing phishing cues, especially for new types of phishing attacks such as 809 scams.

4.8 Threats to Validity

a) The conclusions of this study were reached in the context of a closed- lab test where the participants knew that they were being evaluated on their abilities to detect phishing attempts; therefore, they describe the abilities of the subjects rather than the habits of the subjects. This means that some of these observations may not hold in a real-life setting (jakobsson). A Phishing IQ-test, in this regard, introduces a preconceived notion, as subjects know their ability to detect phishing is being tested. Accordingly, "the knowledge of the existence of the study biases the likely outcome of the study" (Jakobsson & Finn, 2007). Therefore, its results cannot be linked to real life situations. In other words, they cannot be generalized to the real world as they are not a true representative of it.

b) As IQ-tests are performed in a closed-lab environment, they lack 'context' surrounding real life attacks. A number of researchers believe the artificial context of these studies may skew the tests' results (Anandpara, Dingman, Jakobsson, Liu, & Roinestad, 2007; Robila & Ragucci, 2006; Emigh, 2005; Jakobsson, Finn, & Johnson, 2008).

c) The sample used in the study included only Computer Science graduates. The reason is that we wanted to investigate how IT-literate individuals will communicate with phishing, given their relatively awareness of some security trends. However, this is threat to the external validity, affecting our ability to generalize the results of the study to the broader population. But as all the participants of the three studies reported in chapter 4, 5, and 6 were IT-literates, this was important as some studies were serving for each other (output of study 4, was used to design study 5 and study 6), as explained earlier.

We aim for future work to choose a sample that is more heterogeneous.

d) The sample size used was relatively small. This led to weak statistical power of the results. Using bigger sample size is recommended for future research.

4.9 Filling the Gaps of the Study

a) The study did not create highly sophisticated spear-phishing message to test users' ability to detect phishing attacks. The least detected phishing message achieved 19% response rate. This gap is addressed in the design of study 3 and study 4 reported in chapter 5 and 6 respectively. This was done by reflecting on the results of the current study and the participants' reactions with the messages. For example, as the 809 scam and the banking messages were both the least detected by the participants. The design of study 3 was based on 809 scam in banking context with the use of spear-phishing by addressing the participants with their last names. Whereas study 3 did not ask the participants for any personal data, study 4 asked the participants for their date of birth and first line of their address. More about the design of these studies is reported in the following chapters.

b) The study investigated only the first hypothesis H1 that investigates the effect of personality on phishing vulnerability). This was addressed as Study 3 and study 4 investigated all the three hypotheses:
H1: Personality traits affect individuals' phishing vulnerability
H2: Previous phishing knowledge affect individuals' phishing vulnerability
H3: Upsetting previous security incidents affect individuals' phishing vulnerability

4.10 Conclusion and Summary

The lab study results have indicated the personality trait *Extraversion* is correlated with the participants' ability to detect phishing messages. In specific, extrovert individuals were more likely to accurately detect phishing messages. This is consistent with the grounded theory hypothesis that proposed *Extraversion* as affecting phishing vulnerability. However, the lab study results did not prove a correlation either between the other two traits proposed by the grounded theory (*Agreeableness* and *Conscientiousness*).

The study highlighted some SMS phishing scams that are more likely to deceive mobile users such as 809 scams and financial messages. 809 scams specially those pretended to be sent by a friend were the least detected by the users. This supports Jakobsson (2011) that mobile phones are mostly associated with social interactions which add the risk of phishing. on the other hand, prizes and award messages were easily detected by the participants.

Users falsely detected some legitimate messages, even these sent by their own institutions such as their university or health centre. This is consistent with research that IQ tests measure users' fear and that they prefer 'better safe than sorrow' (Jakobsson, 2007). This highlights one of IQ-tests limitations and raises questions about generalizing their results.

5 Chapter 5: Study Three: An Experiment with 809 Scam Simulation

This chapter reports the findings of a simulated phishing experiment. The experiment investigates the effect of personality on IT-literate individuals' phishing vulnerability.

5.1 Introduction

In the previous study, a mix of legitimate and phishing mobile messages were presented to a sample of postgraduate Computer Science students in a context that is referred to as phishing IQ tests. The aim was to identify the personality traits responsible for detecting phishing messages. Although, phishing IQ tests provide a satisfying way to test individuals' ability to correctly identify phishing, as well as being a powerful tool in phishing education, their inherent artificial nature as controlled lab studies biases the outcome results (Jakobsson 2007, Vishwanath et al. 2011, Halvie 2013). In study 3, reported in this chapter, we carry out an 'in-the-wild' experiment, which is believed to avoid the lab studies biases by enabling the participants to behave in a more naturalistic manner. The reason is that these experiments are based on simulating a real life situation. The researcher simulates a real phishing attack and observes participants' behaviour towards it. To avoid the biased conclusions that may result if the participants know they are participating in a phishing experiment, the researcher needs to deceive the participants as to the real purpose of the study. Using deception in research means that researchers deliberately withhold some of the research procedures, mainly its purpose, from the participants.

This experiment is very important for the research in the thesis as it provides high ecological validity than correlational research (such as our first study reported in chapter 3) and lab experiments (such as our second study reported in chapter 4) (jagatic 2007, Jakobsson & Finn 2007, Oh & Obi, 2012). Ecological validity refers to "whether an effect has been demonstrated to occur under conditions that are typical for the population at large" (Brewer, 2000 p:12). High ecological validity of a certain study means that the settings of the study approximate to high degree those of the real world. Two closely related aspects: representativeness and generalizability contribute to the ecological validity of a certain study (Kvavilashvili & Ellis, 2004). Representativeness, refers to "the extent to which a phenomenon can be investigated in a form and in a context that corresponds to its occurrence in everyday life" (Kvavilashvili & Ellis, 2004, p:14). Generalizability, refers to "the degree to which the results of a particular study (or set of studies) are able to explain (other) similar processes or tasks in everyday life" (Kvavilashvili & Ellis, 2004, p.14).

Aiming to acquire representative and generalizable results, many phishing researchers have become recently more engaged in this sort of experiment (Oh & Obi, 2012). Examples include studies of Jagatic et al. (2007), Jakobsson (2007), Wright et al. (2010), Mohebzada et al. (2012), Halvie (2013). The most well-known study of this sort is the phishing field experiment performed by Jagatic, Jakobsson, Johnson, and Menczer (2007). The study was published in 2007, but the experiment was conducted in 2005. The authors describe their project as the first phishing experiment to provide a baseline success rate for phishing attacks, and that it was the first study to achieve this goal. To the best of our knowledge, our study reported in this chapter is the first field experiment to investigate human factors in mobile phishing. We aim that the study provides us with a more authentic estimate of phishing vulnerability than Phishing lab-studies based research.

As the findings of study 2 reported that 809 scams were the least detected by mobile users, we chose this type of phishing attack as the basis for our phishing experiment (study 3). In 809 scams, mobile users are tricked into dialling or texting a premium rate number. Consequently, Study 3 aims to assess the hypothesis proposed by study 1 in the context suggested by study 2. The findings of study 1 suggested that *the success of phishing attempts is accounted for by the victims' individual differences, specifically, their personality traits, moderated by their knowledge and upsetting past security experience.*

We summarize these goals in the following section.

5.2 Aims

This section discusses the purpose of the study. The study aims to:

a) improve our understanding of the psychological aspects of mobile SMS phishing via a field experiment context.

b) investigate the first hypothesis (individuals' personality affect their phishing vulnerability).

c) investigate the second hypothesis (individuals' upsetting past phishing experience affect their phishing vulnerability).

d) investigate the third hypothesis (individuals' knowledge affects their phishing vulnerability).

5.3 Research Methodology

Although phishing experiments have become favoured by phishing researchers recently (Oh & Obi, 2012) for the reasons explained in section 5.1, conducting this type of real-time experiments is extremely challenging. For instance, reaching a sample of phishing victims in external environments is often difficult. Also, the success rate of such experiments is often low (Vishwanath et al., 2011). Furthermore, although methods, materials and settings adapted in real-time experiments approximate the real-world that is being examined, which makes them acknowledged as the most ecologically valid, they are more ethically complicated than self-report studies or lab experiments.

These ethical complications arise from the involvement of deception in such studies. Deception is an indispensable element in real-time phishing experiments (Soghoian 2008, vishwanth et al. 2011, & Jakobsson 2007). It allows for more direct observation of natural behavior than self-reports or intentions (Downs et al. 2014). In order to run a simulated phishing attack, researchers need to deceive the participants as to the real purpose of the study. Yet, if the welfare of the participants was not dealt with as a priority, running phishing experiments without informing the participants that they have been phished, may involve harm to the public or sabotaging the public trust in researchers.

Nonetheless, although phishing experiments do involve deception, conducting simulated phishing experiments is an acceptable phishing research approach (Jakobsson 2007, Halvie 2013, Soghoian 2011, & Downs et al. 2014). Previous validation of real-time phishing experiments suggests that if a researcher can ensure the security of any personal information released by the participant neither a laboratory phishing study nor a naturalistic phishing experiment should adversely affect the welfare of the subject (Jakobsson &Finn, 2007).

Whether or not to debrief the subjects after the study fulfils its purpose is still a controversial issue among phishing researchers. Its advocates advise for debriefing the participants to the true nature of the experiment by the end of the study. They urge researchers to use it as 'risk-minimization strategy' (Israel, 2014). Yet, other experts in the field such as Peter Finn and Markus Jakobsson are in favour of keeping the purpose of the experiment withheld from the participants (Jakobsson & Finn, 2007). They even fear that the debriefing process may adversely affect the welfare of the participants. Moreover, they argue that, in real-time phishing experiments, the only source of risk of harm is a result of debriefing subjects as they might become upset or anxious when they discover via debriefing that they have been deceived (Jakobsson & Myres 2006, Jakobsson and Finn 2007, Jakobsson et al. 2008).

In study 3, we sought several ways of conducting experimental designs without running these risks. First, essentially, we followed the guidelines provided by professional bodies regulating ethics of research such as:
The British Psychological Society (BCS)
The American Psychological Association (APA)
Belmont report
Code of federal regulations

Second, Legal aspects were discussed in advance with *York Law Clinic*, York law School, University of York. The director of clinical programs confirmed that the study complies with:
-The Human Rights Act 1998
-The Fraud Act 2006
-The data Protection Legislation
-The Telecommunications Legislation

Third, the researcher has attended a two day Mental Health First Aid course. The course taught skills for providing initial help to people experiencing anxiety and panic attacks. She has also contacted:
-University of York Counselling Service
-University of York Training and Careers Team
-University of York Skills and Development coordinator in biology
-These contacts provided advice of handling anxiety. Moreover, University of York health and wellbeing service recommended anxiety and panic handling workbooks.

Fourth, the experimental design of study 3 was pilot-tested before engaging the targeted participants.

5.3.1 Study Design

The study examined the relationship between personality traits and people's vulnerability to phishing attacks. The pseudo-independent variable was Personality traits, with five levels: Agreeableness, Conscientiousness, Openness, Extraversion, and Neuroticism. The dependent variable is phishing vulnerability. Each subject participated in only one condition (exposure to simulated phishing attack) and provided 35 scores hierarchically arranged (5 scores estimate the individual's level on each of the five broad personality domains and 6 scores on the sub-domains that comprise each domain).

Note: one of the main differences between experimental and correctional research is that in experiments we manipulate one variable to observe its effect on another (Filed & Hole 2008). The variable we manipulate is referred to as the independent variable (IV), which is the variable that we propose as the cause of the effect we try to measure. In our study, we propose that personality is one cause of phishing vulnerability, and hence, it should be referred to as the independent variable. However, personality by nature cannot be manipulated (Rais & Judd 2000, Revelle 2007), and according to the handbook of research methods in personality psychology, personality belongs to what is referred to as 'subject variables' or 'personal variables' (PV), which reflect stable characteristics of the participants that are not subject to manipulation (Robins, Fraley, & Krueger, 2009). Other terms used to refer to subject variables is 'pseudo-independent variables'. Examples of other personal variables are intelligence and gender which cannot be changed by an experiment. Accordingly, we will not refer to personality as 'independent variable'. Instead, we will refer to it as 'pseudo-independent variable' or 'the predicting variable'. We follow the recommendation of Robinson, Shaver and Wrightsman (2013) to use the 'median-split' approach to be able to deal with personality traits special nature. This is explained in the data preparation section of the study.

5.3.2 Study Settings

A private company in Cairo, Egypt, Compu-Pharaohs for IT Services (CPS) authorized us to carry out a simulated phishing scenario via its employees' mobile phones. The aim is to improve their employees' resilience towards spear phishing. CPS is an IT professional service company that has been established 2006. Legally, CPS is a S.A.E company With a Capital of 10,000,000 L.E. The company is a Microsoft Gold Certified Partner (Compupharaohs, 2014).

The company administration wanted to raise its employees' awareness of the strategies and sophisticated tactics of phishing and collaborated with the author to measure their susceptibility to mobile phishing. The participants were told that they were taking part in a study to assess their personality. They were asked to give the author their mobile number in order for her to contact them to receive their personality results at a later meeting.

5.3.3 Sampling

82 employees were recruited for the study. Around 95% were aged between 21 and 40 years and 5% were over 40 years. Around 70% were male and 30% were female.

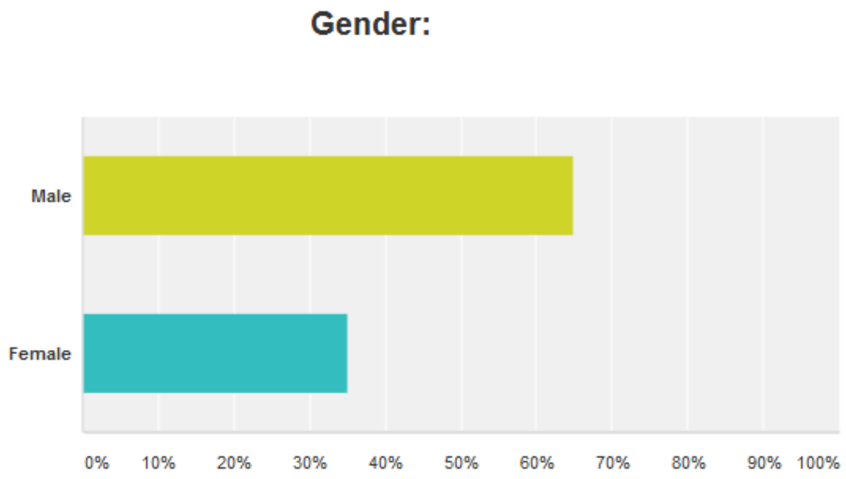


Figure 16: Gender Figures before exclusion

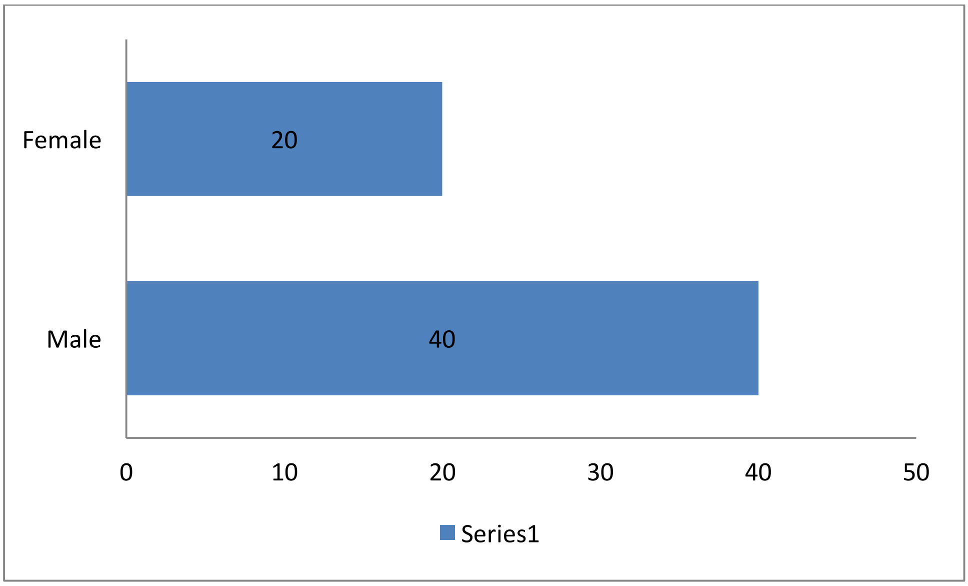


Figure 17: Gender Figures after exclusion

Exclusion Criteria

Employees were excluded from the study if they provided incomplete data via the questionnaire. This included participants who failed to complete the personality questionnaire fully and those who did not provide their mobile phone number.

Employees were excluded from the study if there was a possibility that they might reveal the true nature of the study to other participants. For example, only one partner (chosen randomly) of a married couple participated. 22 employees were excluded overall. (one for being married to another employee in the company, and 21 were excluded for providing incomplete questionnaire). Accordingly, the number of effective participants became 60 instead of 82. To avoid interaction between these employees, the message was sent on a weekend (explained in more details in the study procedures section).

5.3.4 Study Procedures

The study procedures were broken into three distinct phases:

Step1- Data Collection

Step2- Simulated phishing

Step 3- Debriefing

Step1- Data Collection

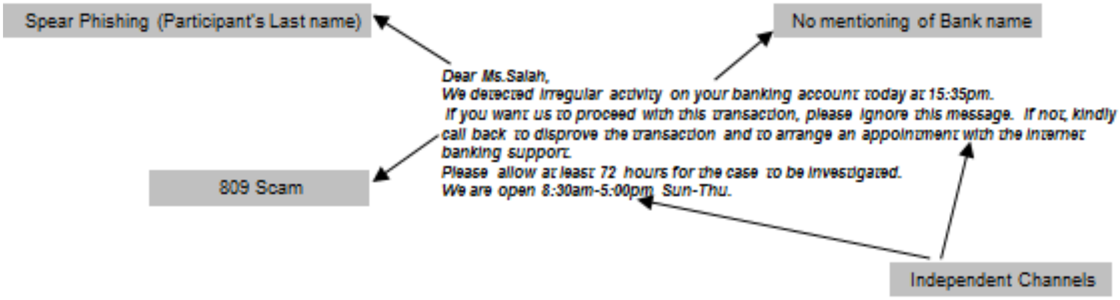
In the first phase of the experiment the participants were given a link to an online questionnaire and were asked to fill it in within 10 days. The questionnaire was hosted on Survey Monkey, an online survey tool. Each participant completed the questionnaire individually. It consisted of two sections:

Section 1: Personal data. This section asked the participants for their age, gender, email and mobile phone.

Section 2: Personality Questionnaire. In this section the user filled the short version of IPIP-NEO personality traits test.

Step2- Simulated phishing

In this phase of the study, the mobile numbers provided to us by the participants via the questionnaire were used. The author sent a simulated phishing message (See figure below) to each of these participants' mobile phones, a few weeks later. **Figure 18** below shows the structure if the phishing message sent to the participants.



Dear Ms.Salah,
We detected irregular activity on your banking account today at 15:35pm.
If you want us to proceed with this transaction, please ignore this message. If not, kindly call back to disprove the transaction and to arrange an appointment with the internet banking support.
Please allow at least 72 hours for the case to be investigated.
We are open 8:30am-5:00pm Sun-Thu.

Spear Phishing (Participant's Last name)
No mentioning of Bank name
809 Scam
Independent Channels

Figure 18: 809 Scam Phishing Message

The message pretended to be from a bank and used a fraudulent number that looks like premium rate numbers. It asked the participants to ring back to confirm an irregular internet banking activity. Following Jakobsson's suggestion (Jakobsson, 2007) that independent channels create trust, our stimulus implied to the participants that they can arrange a meeting with the bank administration, if they desire. Hence, we included the bank opening hours at the bottom of the message. The purpose of such an addition is to strengthen the respondents' trust in the phishing message.

As the participants belong to the same organization, there was a possibility that they may discuss with each other the phishing message sent, an act that is known as 'the conformity effect'. This effect can influence the results of our study if the participants' behaviour towards the message was based on the attitude of others. To avoid that, the date of sending the message has to be chosen to be a day off from work (a weekend). So, the day needs to be either Friday or Saturday. But at the same time, we want to give a chance to the participants who (either detect or doubt the message) may wish to contact their bank to check the authenticity of the message. Accordingly, Saturday was selected as the banks call-centres operate on this day. So, although the participants will not be able to visit the bank on Saturday, they would be to contact the call-centre by phone, if they wish to investigate the message further.

5.3.5 Instruments

This section discusses the psychological and technical instruments used in the study.

a) Psychological Instrument

The psychological domain used in this study to describe human personality was *the Five Factor Model* (FFM) that consists of five broad personality traits. The psychological instruments used to measure the FFM personality traits, in this study, was the *international Personality Item Pool* (IPIP).

The rational for choosing FFM and IPIP in specific was reported in chapter 2.

IPIP Personality Questionnaire Preparation

Data Entry from IPIP to Survey Monkey

The personality questionnaire was available online at a personality pool that provides immediate personality measurement. However, as delivering back the personality results to the participants was our cover up/ excuse to contact the participants again and hence get their mobile numbers, we preferred to let the participants access the questionnaire via Survey Monkey instead.

Translation

As the participants' mother tongue was Arabic, the personality traits items have been translated from English to Arabic to enable the participants to fully understand each item. Accordingly, the author used a translation that was approved and recommended by Goldberg, the founder of IPIP. Consequently, both the English and Arabic translation was entered manually to Survey Monkey Questionnaire (See Appendix C).

Data Entry from Survey Monkey to IPIP

The final step included feeding the IPIP with the personality answers of the participants. In return IPIP provided the participants' personality measures according to the Big Five Factor Model.

b)Technical Instrument: SIM card

A new SIM card has been used for the experiment. In order for the number to look similar to premium rate numbers, a special number with a high price was purchased from Vodafone Telecommunications. The premium rate number digit form used was 10XXX as this form has been abused by premium rate numbers providers recently (Federal Communications Commission, 2013).

5.3.6 Ethical Procedures

-The researcher's mobile was kept in a locked filing cabinet in a locked room at the department of Computer Science, University of York.

-The SIM card was dedicated to the study so the researcher's personal number is not revealed.

-The SIM card was discarded once the study was complete in order to protect the participants' mobile numbers.

-The mobile operator was contacted well in advance of the experiment and were notified that the SIM Card would be sending hundreds of text messages over a short period of time. This step was important as many mobile operators prohibit this action and may block the line.

-In the process of analyzing the personality questionnaire data, all participants' names were omitted and replaced by anonymous names. Such as; X, Tinker bell, etc. Accordingly the participants' personality reports did not include their names. All participants' personality questionnaires and reports were kept in a locked secure cabinet in the researcher's office accessible only to the researcher.

Participants' Welfare: Some protective procedures were planned for taking care of the wellbeing of the participants. Although, the personality test used does not measure participants' ability on any task, we had to recognize that the personality results may cause anxiety or stress to some participants with mental health problems. Accordingly, the following steps were undertaken:

-The first page of the personality test results given to the participants says explicitly: "Please keep in mind that 'low, 'average' and 'high' scores on a personality test are neither absolutely good nor bad".

The researcher assured the participants that this personality test is just a model and is not always 100% accurate. Accordingly the researcher has prepared a sheet about 'Issues of Personality Assessments' as evidence to the participant that there is always a probability of error and that the test results need to be taken with degree of scepticism. (See Appendix D).

-The researcher has contacted the Skills Development Co-ordinator in the Biology Department. She used to run many personality assessments for students in University of York. She assured us that these types of anxiety caused by personality tests are very rare and that they have never faced any anxiety or stress situation resulting from any of the personality tests she administered before.

5.4 Participants' Response

55% (33 of 60) of the participants responded to the simulated phishing message. The profile of the behaviour classifies the individuals. Participants who responded either by a text message or by a phone call were classified as 'victim'. Individuals who ignored the phishing message were classified as detectors.

5.5 Quantitative Analysis

This section reports an investigation of the relationship between the pseudo-independent variable (Personality traits) and the dependant variable (phishing vulnerability) using statistical methods. The data collected was between-subjects. Between-subjects is an experimental design where there is only one design (one phishing message) where every participant (sometimes referred to as subject) contributes only once in the experiment. Chi-Squared tests were performed to assess if the observed frequencies differ from those that would be expected by chance. This statistical test was used to examine the association between our two main variables; Personality Trait and Phishing Response. The section starts by discussing data preparation of the variables measured then we examine the quantitative relationship between the variables.

5.5.1 Data Preparation

As the process of data measurement is central to quantitative research, we explain in this section how data were prepared for the analysis in terms of how they were scored in respect to each variable.

a) Measuring the Pseudo-Independent Variable Personality Traits:

The same procedures that were used in study 3 (reported in chapter 4) to measure the participants' personality traits were applied here. As explained in the instruments section, participants' personality traits were measured using the standard personality tool IPIP. The results of the personality tool assign every participant a score (percentile) for every personality trait. In order to be able to measure the relationship between personality and phishing vulnerability, we needed to transform these personality scores into two groups (the first group exhibits high level of personality and the second group exhibits low levels of personality) per each personality trait. For that we used 'median-split' method.

Median-split is a method used to transform continuous variables into categorical ones. We applied it to our data by calculating the median score of the participants per each personality trait and then we regarded every value below the median as 'low' and every value above the median as 'high'. Accordingly, for every personality trait, we had two categories. The first category groups the participants who scored high, and the second category groups the participants who scored low in this personality trait. These are then compared against the dependent variable (phishing vulnerability) as explained in the following section.

b) Measuring Participants' Phishing Vulnerability

Phishing vulnerability was measured by the participants' response to the phishing message. So, the profile of behaviour classifies the participants into either 'detective' who did not contact the attacker, but may call third party, and 'victims' who contacted the attacker (either by call or text).

Guide for the Quantitative Results:

The statistical results produce frequency table for every personality trait. This table indicates the number of participants who belong to the category 'victims', and those who belong to the category 'detectors' based on their response to the phishing message. The table indicates whether these participants scored high or low in the investigated personality trait, according to which group they belong to (above or below the median in the median-split method explained earlier).

Accordingly, most of the tables will have:

2 columns: indicating high or low level of personality traits score.

2 rows: indicating the participants profile of behaviour (victim or detector) based on either response or no response to the phishing message.

In some cases, where there are some participants whose score in a certain personality trait equal to the median, the table will have 3 columns (indicating high, low and median score).

(a)Personality Trait Agreeableness Score:

The mean Agreeableness's score of the participants was 62 (SD=24.036). According to Goldberg's IPIP manual (IPIP, 2016), this means that our participants' level on this trait was estimated to be higher than 62% of persons of same age and gender. According to Prof.John Johnson interpretation of the personality traits levels, this indicates average level of Agreeableness indicating some concern with others' needs, but, generally, unwillingness to sacrifice themselves for others (Johnson, 2016).

This result also shows high standard deviation (SD=24.036). This indicates a wide spread of the data. This can be explained by either a large amount of variation of the personality trait 'Agreeableness' in the group, or by outliers' effect (having extremely low, or extremely high personality trait scores of some participants). However, given that the personality traits are normally distributed, then this indicates that our data meet the assumption of the personality traits model. This big standard deviation can explain why no significant results occurred, especially that we are not using big sample size.

The frequency table of responses shown in Table 31 is based on the median split of Agreeableness. A chi-squared test based on the same split shows no significant differences in response rates (chi-squared(1) = 0.619, p = 0.435, i.e. the probability of obtaining the chi-quared value (1 degree of freedom) of 0.619 or greater is 0.435).

Table 31: Agreeableness Frequency Table (Median Split)

	Low	high
No Response	11	15
Response	19	15

(b)Personality Trait Conscientiousness Score:

The mean Conscientiousness's score of the participants was 59.79 (SD=28.286). This indicates average level of Conscientiousness among the participants. This means participants were reasonably reliable, organized, and self-controlled.

The frequency table of responses shown in Table 32 is based on the median split on Conscientiousness. A chi-squared test based on the median split shows no significant differences in response rates (chi-squared(1) = 0, p = 1).

Table 32: Conscientiousness Frequency Table (Median Split)

	Low	High
No Response	14	12
Response	16	18

(c) Personality Trait Extraversion Score:

On average the participants scored 50.03 (SD=24.986) on Extraversion indicating they are neither a subdued loner nor a jovial chatterbox. This also implies they enjoy time with others but also time alone.

The frequency table of responses is shown in Table 33 based on the median split on Extraversion. A chi-squared test based on the same split shows no significant differences in response rates (chi-squared(1) = 0.619, p = 0.435).

Table 33: Extraversion Frequency Table (Median Split)

	Low	0	high
No Response	15	1	10
Response	14	3	17

(d)Personality Trait Neuroticism Score:

The mean Neuroticism's score of the participants was 49.73 (SD=26.866). This score shows an average level on Neuroticism. Hence, it suggests a level of emotional reactivity that is typical of the general population. Stressful and frustrating situations are somewhat upsetting to the participants, but they are generally able to get over these feelings and cope with these situations.

The frequency table of responses is shown in Table 34 based on the median split on Neuroticism. A chi-squared test based on the same split shows no significant differences in response rates (chi-squared(1) = 0.2205, p = 0.6386).

Table 34: Neuroticism Frequency Table (Median Split)

	Low	high
No Response	13	13
Response	17	17

In regards to the personality sub-domains measured for every participant, below we display the most particularly relevant and closely related traits to phishing susceptibility. These include: Trust, Anxiety, Assertiveness, vulnerability, Dutifulness and Cautiousness facets.

Here is a brief justification of the rationale behind choosing these sub-domains in specific:

Trust: Trust is a facet under the big domain Agreeableness. A person with high trust assumes that most people are fair, honest, and have good intentions. Persons who score low in trust see others as selfish, devious, and potentially dangerous.

Anxiety: Anxiety is a facet under the big domain Neuroticism. The "fight-or-flight" system of the brain of anxious individuals is too easily and too often engaged. Therefore, people who are high in anxiety often feel like something dangerous is about to happen. They may be afraid of specific situations or be just generally fearful. They feel tense, jittery, and nervous. Persons scoring low in Anxiety are generally calm and fearless.

Assertiveness: Assertiveness is a facet under the big domain Extraversion. High scorers on Assertiveness like to speak out, take charge, and direct the activities of others. They tend to be leaders in groups. Low scorers tend not to talk much and let others control the activities of groups.

Vulnerability: Vulnerability is a facet under the big domain Neuroticism. High scorers on Vulnerability experience panic, confusion, and helplessness when under pressure or stress. Low scorers feel more poised, confident, and clear-thinking when stressed.

Dutifulness: Dutifulness is a facet under the big domain Conscientiousness. This scale reflects the strength of a person's sense of duty and obligation. Those who score high on this scale have a strong sense of moral obligation. Low scorers find contracts, rules, and regulations overly confining. They are likely to be seen as unreliable or even irresponsible.

Cautiousness: Cautiousness Dutifulness is a facet of the big domain Conscientiousness. It describes the disposition to think through possibilities before acting. High scorers on the Cautiousness scale take their time when making decisions. Low scorers often say or do first thing that comes to mind without deliberating alternatives and the probable consequences of those alternatives.

Personality Sub-Domains Investigation:

We examined the relationship between each of these sub-domains and phishing vulnerability. Below are the scores for each.

(e)Personality Trait Sub-Domain Trust:

The frequency table of responses is shown in Table 35. It is based on the median split on Trust. A chi-squared test based on the same split shows no significant differences in response rates (chi-squared(1) = 5.3938, p = 0.06742).

Table 35: Trust Frequency Table (Median Split)

	Low	0	High
No Response	10	0	16
Response	19	3	12

Depending on the Median split results, these results indicate that the Trust sub-domain is approaching significance in relation to peoples' vulnerability to phishing attacks. The more trusting a person is, the less vulnerable they are to phishing. This result is counter-intuitive, and we hope that the qualitative results explain it. Hence, this point is discussed further in the discussion section, after investigating the qualitative results.

(e)Personality Trait Sub-Domain Anxiety:

The frequency table of responses is shown in Table 36 based on the median split on Anxiety. A chi-squared test based on the same split shows no significant differences in response rates (chi-squared(1) = 1.2004, p = 0.5487).

Table 36: Anxiety Frequency Table (Median Split)

	Low	0	high
No Response	13	4	9
Response	15	3	16

(f)Personality Trait Sub-Domain Assertiveness:

The frequency table of responses is shown in Table 37 based on the median split on Assertiveness. A chi-squared test based on the same split shows significant differences in response rates (chi-squared(1) = 6.6365, p = 0.03622).

Table 37: Assertiveness Frequency Table (Median Split)

	Low	0	high
No Response	17	2	7
Response	11	7	16

(g)Personality Trait Sub-Domain Vulnerability:

The frequency table of responses is shown in Table 38 based on the median split on Vulnerability. A chi-squared test based on the same split shows no significant differences in response rates (chi-squared(1) = 0.1311, p = 0.9366).

Table 38: Vulnerability Frequency Table (Median Split)

	Low	Score=Median	high
No Response	12	2	12
Response	15	2	17

(h)Personality Trait Sub-Domain Dutifulness:

The frequency table of responses is shown in Table 39 based on the median split on Dutifulness. A chi-squared test based on the same split shows no significant differences in response rates (chi-squared(1) = 0.0679, p = 0.7945).

Table 39: Dutifulness Frequency Table (Median Split)

	Low	high
No Response	12	14
Response	18	16

(i)Personality Trait Sub-Domain Cautiousness:

The frequency table of responses is shown in Table 40 based on the median split on Cautiousness. A chi-squared test based on the same split shows no significant differences in response rates (chi-squared(1) = 0.6218, p = 0.7328).

Table 40: Cautiousness Frequency Table (Median Split)

	Low	0	high
No Response	12	3	11
Response	17	2	15

5.5.2 Quantitative Analysis Discussion

As the analysis reported in the previous section indicates, participants' personality traits were compared against their response to the phishing message. Depending on Chi-square Median split, only two personality traits have been highlighted by the quantitative analysis. These are Assertiveness and Trust. Depending on Chi-square tertile split, the personality trait Extraversion showed significant correlation with phishing vulnerability.

In this section, each is discussed.

a) The effect of Assertiveness:

Assertiveness is a sub-domain under Extraversion personality trait. The results showed that individuals' Assertiveness correlated significantly with phishing vulnerability. Participants with high scores in Assertiveness had a tendency to fall for the phishing attack. Although this was not what we expected based on previous research on phishing-personality relationship (lack of connection between assertiveness and phishing vulnerability in the literature), this result is unsurprising, given the previous research on Assertiveness. Assertiveness is correlated with being **outgoing with strangers** as well as having uniquely strong correlations with self-confidence. Assertiveness has been strongly linked to **leadership**. It was described as preference for exerting control in a group setting. Assertive individuals were described as, often, leading the groups they belong to and as being relied on to **make decisions** (Deyoung, Quilty, & Peterson, 2007; Soto & John, 2008).

It is worth mentioning that Assertiveness is a subdomain of the Extraversion personality trait

No previous research has investigated the subdomains of the big five (maybe that's why no positive or negative correlation has been reported in literature in regards to Assertiveness).

We aim that the qualitative study (reported in the next section) can describe how these qualities of assertiveness (including leadership, decision making and being outgoing with strangers) manifest themselves in the mobile user-phisher interaction.

b) The effect of Trust

The results showed approaching significance of the effect of the personality trait Trust on phishing vulnerability. People who scored low in trust were more likely to fall for the phish.

This result is quite unexpected given previous literature that relates high scores on Trust to phishing vulnerability. Accordingly, we will delay discussing this effect until after the qualitative analysis that we hope can provide an explanation for such an odd effect.

c) The effect of Extraversion:

No effect of extraversion has been proved statistically significant using a median split approach. However, performing a tertile split analysis of the data, the personality trait extraversion showed approaching significance.

Although the tertile split procedure permits us to be more confident that the selected categories of mobile users actually represent different types (thereby strengthening the study's internal validity), the procedure eliminates from the analysis a large number of mobile users whose extraversion is "average" (thereby weakening the result's external validity). Thus, while our focus on the extreme groups in our sample may provide a clearer test of the hypothesis, this approach limits the generalizability of our findings.

To recap, the quantitative results suggested a positive correlation between Extraversion and phishing vulnerability, where individuals who scored high on Extraversion where more likely to fall for the phish. A possible explanation of this effect of Extraversion trait on phishing susceptibility, is that extrovert individuals have a greater preference for engaging in social interaction than introverts. Extraverted behavior is believed to be more closely related to the distinct, higher-order trait of impulsivity (Guilford and Zimmerman 1949); a possible explanation of why our extroverted participants were more likely to respond to the phishing and contact the phisher. Again, this assumption needs to be examined via the interviews reported in the qualitative study presented next section.

5.6 Qualitative Analysis

Having indicating a number of personality traits that may affect individuals' susceptibility to phishing, the author sought to explore how these factors work. For this purpose, a qualitative approach was adopted for this section of the study. During the debriefing process, a formal request for an interview was made from the same MSISDN number that initiated the phishing message. 54 participants took part in the follow-up interview, five did not responded and one refused to participate. The hypothesis proposed by the grounded theory reported in chapter 3 was the basis for the interviews.

The interviews were semi-structured, yet a pre-defined structure was preserved as a guide through the interview procedures (See Appendix E). The interviews lasted 10-15 minutes. Data was recorded as notes as the interview proceeded and then more comprehensive documentation was transcribed from the notes. To insure anonymity of the participants, each transcript was given a code to be used for quotations so only their initials are shown, no names. That was followed by a coding process.

5.6.1 Method

The qualitative analysis was submitted to thematic analysis (Boyatzis, 1998). The rationale of using thematic analysis approach was discussed in chapter 4.

5.6.2 Thematic Analysis

The thematic analysis was employed by following the guidelines suggested by Braun and Clarke (2006). Accordingly, our thematic analysis went through the following six phases:
1-Familiarizing with the data
2-Generating initial codes
3-Searching for themes.
4-Reviewing themes.
5-Defining and naming themes
6-Producing the data analysis report.
Below, we explain how we applied these steps.

The term 'data corpus' is used to refer to all the interview data collected from the participants in the study We will use the term 'data set' to refer all the data collected from the corpus for a particular analysis. We chose here two data sets based on the source of the data: 'victims or 'detectors' for every message. We will use the term 'data item' to refer to the individual pieces of data, i.e. the components of the data set.

a) Familiarizing with the data

We aimed to get familiarise ourselves with the data by reading it in an effective way (by looking for patterns and meanings). We followed the process of repeated reading of the entire dataset before we start the coding process. Our reading process was informed by the type of analysis we aimed to achieve. Similar to our approach in the second study (reported in chapter 4), we will use the theoretical approach for data analysis, as it permits more detailed analysis on certain aspects of the data, that mainly answers the proposed research questions we are interested in: why and how the participants either detect or fall for the phishing messages they have been shown.

b) Generating initial codes

We built on our list of relevant issues and ideas generated in phase one, to produce initial codes from these ideas. Codes refer to the most basic elements of the raw data that can be assessed in a meaningful way regarding the phenomenon (Boyatzis 1998). Below we explain the process we followed in generating our codes.

Our coding of the data was 'theory-driven', as we approached the data with specific questions in mind representing 'how', 'what' and why' questions: how the participants identified the messages? What were their strategies to interact with the messages, and why they chose to make their decisions the way they did?

Coding was done manually by using highlighter pens on the individual transcripts to identify any interesting aspects in the data that may form potential patterns. Then these data extracts were copied to a computer file along with some surrounding relevant data, as recommended by Bryman (2001) to make sure context is not lost. This was repeated systematically through the two data sets with full attention paid to each individual data item.

Table 41 Below is a sample of codes applied to a data extract from 'victims' dataset.

Table 41: Sample Extract of Victims Dataset

Data extract	Coded for:
"The message addressed me by name" "The format looked professional"	-Message cues. -The official look creates trust.

c) Searching for themes

In this phase, we were interested in performing interpretative analysis of the data that was coded in phase 2. We aimed to conduct this process on our two datasets: 'victims' and 'detectors'. Interestingly, we found a number of patterns that may look like they belong to the 'detectors' dataset, but, they were extracted from the victims' codes. For example, most of the victims analysed the components of the phishing message carefully, including certain expectations of the look of an official message, of a certain communication method (use of phone call not text), and of the use of sender ID that contains their bank title. These participants noticed the lack of these factors in our phishing message. Still, they fell for the message and communicated the message sender. Accordingly, the themes that represent these participants were grouped as a new theme, 'Detector-Victim'.

The process was repeated and the section below discusses the results of the analysis.

5.7 Data Analysis Results

In this section, we report some of the main themes that showed prevalence in the data analysis and that relate to the issue of phishing vulnerability. In each of the subsections below, we identify a significant theme. A more general interpretation is provided in the discussion section. In reporting the thematic analysis, we rely heavily on quotations from the participants.

The established categories used for the thematic analysis involved two major domains. The first was the 'victims', which included those participants who communicated with the phisher either via a phone call or texting. The second was the 'detectors', which included participants who either ignored the phishing message or communicated with a third party. A third domain, 'detector-victims', emerged. This includes participants who identified the message as a phishing attempt, however, they followed the phisher instructions by dialling the premium rate number sent.

For the victims, the thematic analysis revealed that 12 thematic elements were indexed and mapped into 6 areas of cognitive processes. For the detectors, the thematic analysis revealed 8 thematic elements mapped into 4 cognitive processes. For the detector-victims, the thematic analysis revealed 7 thematic elements mapped into 2 cognitive processes.

Table 42, **Table 43**,**Table 44**, and, **Table 45** present the major themes for each of these categories.

5.7.1 Major Themes for the Victims' Domain:

In this section, we present the main concepts that emerged in the interviews of those participants who fell for the phish (responded to the phishing message). We refer to these hereafter as the "phishing victims". In each of the subsections below, we identify a significant pattern and provide some relevant quotations from the interviews. We provide more interpretations in the discussion section.

Table 42: The victims' themes

Theme	Subcategory
1- Stimuli creating trust	a. The official look of the message creates trust b. External stimuli parallelism creates trust c. The use of independent channels creates trust d. Personalization creates trust
2- Ignorance of 809 scams	a. No subcategories
3-Unrealistic optimism	a. Awareness of appropriate channels to contact. b. Obeying the message instructions by contacting the message sender.
4-Difficulty of communicating legitimate entities.	a. Banks customer service lines are busy. b. Banks hot lines put customers in long waiting queues.
5-Inability to recall any past phishing (or similar) incidents	a. No subcategories
6- Lack of Cyber Security awareness efforts from Service providers	a. Banks awareness b. Mobile operator awareness

1-Stimuli Creating Trust – Presentation, Personalization, External Stimuli

A common pattern among those who trusted the message was basically a content-related trigger. The participants referred to the official layout of the message. They also related their trust to the foot of the message where the phisher added the bank opening hours. This confirms Jakobsson suggestion that independent channels create trust (Jakobsson, 2007). Participants also described how addressing them by their names increased the trustworthiness of the message.

"The message was very convincing"

"The time of the message was persuasive"

"The message had a realistic format"

"The message addressed me by name"

By chance, our phishing message coincided with external stimulus in the life of some participants, as they were expecting communication from their financial institutions same day.

"I had a transaction credited to my account same day, otherwise, I'd have ignored the message"

"I am expecting my salary these days"

"I've just applied recently for a debit card and I was expecting the bank decision same day at 9:00am"

2- Ignorance of 809 Scams

This was a prevalent theme among all the participants of this domain (victims).

"I did not know about premium-rate numbers"

3- Unrealistic Optimism

Another theme within the victims' domain that is worth noting is Unrealistic Optimism. Although, some participants were aware of the appropriate channels to communicate with their banking institutions to investigate the message, they still contacted the phisher - some before contacting the legitimate financial institutions and some after. Both groups misjudged the action of 'obeying the phisher instructions' as safe and free from danger.

"I did not know that calling a number is risky"

4- Difficulty of Communicating with Legitimate Entities

Another theme within the victims' domain that is worth noting is their complaint of the difficulty they faced when they tried to communicate with their legitimate bank via the phone. As one participant explains:

"I had to call. The bank hotline was busy and they put me on hold for very long time"

5- Inability to recall previous phishing (or similar) incidents.

All the participants who belong to the victims' domain, were unable to recall if they had previously been victims of similar phishing incidents. Some were unsure.

"I do not think so"

"Not as far as I know"

In terms of awareness of phishing messages circulating in their environment, only one participant mentioned that he was aware of these sorts of messages, but without any direct interaction. It was also clear, that he was unable to differentiate between phishing and fraud attacks.

"Ya, I lived in Canada, so I am familiar with this sort of Fraud"

6- Lack of Cyber Security Awareness from Service Providers

The participants expressed the lack of cyber security awareness efforts offered by their service providers. Very few attempts to educate the users made by their banks, and nearly none by their mobile operators.

"My bank sent this sort of messages only once (when I joined the bank)"

"You may receive these messages if you change your credit card"

"My mobile operator never sent me anything in this regard"

5.7.2 Major Themes for the Detectors' Domain:

In this section, we present the main concepts that emerged in the interviews of those participants who detected the phish. We refer to these hereafter as the "phishing detectors". In each of the subsections below, we identify a significant pattern and provide some relevant quotations from the interviews. We provide more interpretations in the discussion section.

Table 43: The Detectors' Themes

Theme	Subcategory
1-Previous 'error in judgment' experiences of the detectors	a. Personal phishing or fraud experience b. Family member, or close friend phishing experience c. Not bringing up the topic unless raised by the researcher
2-Security awareness	a. Precise working experience of either the field of phishing or mobile phones b. Awareness information is available online. c. No mobile Phishing Awareness
3-Exposure to several phishing attempts	a. No Subcategory
4-Expectation of specific institutional factors	a. Expectation of official sender ID

1) Previous 'error in judgment' experiences of the detectors

33% of the participants who were recognized as phishing detectors had been victims of previous phishing and fraud scams.

"It was mobile transfer credit, and I fall for it" **Participant 20**

"Not me, but my best friend, but I was heavily involved with him in the whole process" **Participant 13**

"In Egypt, we take these matters easily, I do not any more" **Participant 13**

It is worth mentioning that none of the participants brought up their upsetting experience. However, they only mentioned it when they were explicitly asked if they were victims of similar incidents in the past.

"Yes (laughing embarrassedly). It was a phone call as well, one pretended to be from my mobile operator, I believed him. My operator said they sent warnings, but I do not remember receiving any" **Participant 59**

"Only once, I lost money from my bank account as a result, I felt very bad" **Participant 46**

"I am an IT specialist, so I know about these issues, I was victim only once" **Participant 05**

"(After hesitation), Yes, I have been a victim before. It was a fraud. I lost trust in people since then" **Participant 82**

2) Security Awareness

33% of the participants who were recognized as phishing detectors had working experience in the field of security. Some of these working experiences directly involved phishing such as E-commerce and Mobile phishing. Those participants emphasized that the main reason for their ability to detect the phishing message was their security background they gained via their jobs.

"I am aware of phishing because of my job; I work in the field of Information security, in E-commerce" **Participant 76**

"How do you expect me to fall for this (laughing), I work in security" **Participant 80**

Those who had working experience related to mobile phones, were more aware as to the purpose of the phishing. They used technical terms such as premium rate numbers that cost more than ordinary numbers and USSD codes that some mobile phishing messages contain and can transfer the victim's balance into the sender.

"I usually don't reply to such SMSs because it's very known. Although it addressed me by name, I knew it was phishing as I know names & numbers are always sold to companies and may be individuals as well. Due to my past experience and knowledge I knew that this was a phishing and would have never responded to it. I was also worried that the message may contain USSD code. I worked for Vodafone for many years; we deal with these issues a lot" **Participant 73**

"The message did not state which bank it was referring to. It was also sent from an unknown number. I was afraid the number may be a premium rate number and costs me a lot if I responded, I know this from my previous job, I used to work for a mobile company. I also receive lots of offers like: Call us to receive a big prize" **Participant 35**

In regards to other means of security awareness such as educational efforts made by service provides such as banks and mobile operators, only one participant attributed his behaviour to the awareness efforts of his bank. He emphasised the 'many' alerts they send him.

"My bank sends me alerts constantly, so I know about phishing. They warn us about strange numbers, like yours" **Participant 25**

The rest of the participants took time to recall whether their service providers have warned them about phishing attacks before.

"Usually, I don't get lot of announcements and alerts from my mobile operators or banks" **Participant 55**

"No awareness at all" **Participant 54**

"Nope! No awareness, oh! They put some warning signs on their website for e-banking, but not for phone scams, just update your info or donot give your info away" **Participant 36**

"None!" Participant 05

"Only my bank, just on their website in case of incident" **Participant 06**

"May be my bank, but not about mobile phishing", **Participant 10**

"My bank hsbc did awareness on its home page, and sends emails if there were any attempts" **Participant 20**

3) Exposure to several phishing attempts

During the interviews, a number of participants (28%) called attention to the fact that they receive many phishing scams on their phones.

"I did not worry at all when I got your message, I receive many messages, so I ignore what I do not know" **Participant 20**

"I receive loads of these messages both on mobile and email" **Participant 26**

"Usually, I got messages, emails, even calls like these, lots of spam, so I become experienced enough to know if it is fake or not" **Participant 55**

5.7.3 Major Themes for the Detectors-Victims Domain

During the interviews some of the victims stated that they were aware that the message was not authentic (sent from their bank), and that they thought it was either a phishing message or a message sent by one of their friends as a joke. However, these participants still contacted the sender of the message via a mobile phone call. Accordingly, we will refer to these participants as 'detector-victim'. The analysis showed the themes that led to their detection of the message as well as the themes related to why they became victims. Below, both themes are discussed.

a) Themes that led to detection

Table 44: Detector-Victims' Themes of Detection

Theme	Subcategory
1- Expectation of specific Institutional Factors	a. Expectation of default official message sender ID b. Expectation of default official message medium c. Expectation of default official message content such as proper addressing and bank account clues.

1- Expectation of Specific Institutional Factors- Source, Medium and Content of the Message

A common pattern noted among the detector-victim group of participants was their expectation of specific institutional factors used by financial institutions to authenticate themselves to their clients. These include both the *source* and the *medium* of the message. For example, the participants expected the financial institution's name to be presented in the sender ID. They also stated they presumed their bank would communicate them via email or phone calls rather than via texting. As some participants explained:

"Normally the text sent from the bank contains the bank name"
"The message was not convincing, there was no mentioning of the bank name"
"The sender was a number, I expected to find the bank name instead"
"My Bank usually calls, not, sends text"

This demonstrates uncertainty about the authenticity of the message triggered by suspiciousness about the *source* of the message and the *media* used for communication.

Repeatedly, participants described similar scepticism triggered by the *nature of the request* (calling back).

"The bank does not request a calling back, instead, it asks for calling the bank call centre!"
"No hot line was mentioned for me to dial"

In regards to the content-related cues that confirm the message authenticity, two participants noted the followings:

"I was expecting to see the phrase (the account ending with 7777)"
"I expected the message to state the last 4 digit of my credit card"

This is consistent with prior research that explains how users find the presence of the last few digits of their bank account, in a message, is more trustworthy (Jakobsson, 2007).

The way the message addressed the clients was also discussed by the participants.

"I expected Dear Customer instead of my name"

b) Themes that led to victimisation

Table 45: Detector-Victims' Themes of Victimisation

Theme	Subcategory
1- Intolerance of uncertainty	a. Seeking more information via confirmation behavior b. Reducing uncertainty via investigation behavior c. Reducing uncertainty via waiting Behavior d. Concern for Security

1- Intolerance of uncertainty

A common pattern noted was the participants' intolerance of uncertainty. Confirming, investigating or waiting behaviour was associated with responding to the phishing message. Often, the content of the quotations that fell under this theme was focused on contacting the phisher either after a waiting period of time to see how the phisher would react, contacting the phisher seeking more information regarding the phishing message, or confirming even after they were assured by their legitimate financial institutions that the message was a phishing attempt.

"I called my bank customer support first"
"I checked my account via internet banking before I rang you"
"I knew it was a scam, just wanted to test your IQ by ringing after working hours to see if you would pick up the line or not"
"I was sure it's a trick, I called to know who wants to trick me"

These participants showed their *concern for security* as they stated they had no intention to reveal any confidential information to the phisher if she had answered their phone call.

"I was not going to give away any confidential data over the phone"

This theme is consistent with and is justified by the participants' *ignorance of 809 scams.*

Investigating the counter-intuitive results of the 'Trust' personality trait:

As the statistical results showed that the participants who scored high in trust were more likely to detect the phishing message, which is counter intuitive, we are investigating this relation further in light of the qualitative results.

Table 46 below lists the participants who scored high in trust, and did not respond to the phishing message, along with certain features that may explain their behaviour.

Table 46: Detectors who scored high in trust

Participant	Features that may have led to detection
P06	Security job
P13	Highly involved with a friend previous error in judgment experience
P20	Previous error in judgment experience
P35	Mobile Telecommunications Job
P42	Credit card expired
P46	Previous error in judgment experience
P52	Just ignored the message, no awareness
P54	Takes things lightly, if it was important, the bank would call again
P59	Previous error in judgment experience
P73	Security job
P82	Previous error in judgment experience

As the table shows, 73% (8 out of 11) of the detectors who scored high in trust have been heavily involved with phishing experiences in the past, either via previous error in judgment experience or as part of their jobs responsibilities. This indicates that factors other than personality can guide people's security behaviour. Although these participants scored high in trust, they did not trust the phishing message, probably as a result of the learning they gained from the different life experiences explained above.

5.8 Discussion

1) First Objective: Understanding of the psychological aspects of mobile SMS phishing

The first objective of the study was to improve our understanding of the psychological aspects of mobile SMS phishing. In this regard, the study indicates the followings:

a) There is a wide range of decision making errors. Our participants did not simply fall into one of two categories: victims or detectors. Instead, we had participants who were able to detect the message, yet, still, followed the instructions of the attacker and called the premium-rate number they were provided with. Some of them stated that they were sure it was a joke, and they rang the number to find who sent the message. Some stated that they simply called the number seeking more information about the message. Some contacted their bank and were assured that this message is not legitimate, but, still called the attacker. Others called the number after waiting for a while, and some called at night. They said they wanted to test how clever the attacker is. Regardless of their intentions, calling a premium-rate number means that they would pay a price for their call, that is higher than the normal charge. This resulted in having participants who fell for the phish driven by several motives (i.e. catching the phisher, trusting the message, curiosity, gambling, ignorance of new phishing technique, etc.). Accordingly, the profile of the participants' behaviour classifies them into three categories: 'victims', 'detectors', or 'detector-victims'.

This wide range of decision-making errors means that merely labelling falling for phishing as simply 'an error' is shallow. The same applies for research that suggests that individuals who fall for phishing are simply either naïve or greedy. In this regard, we stress the need to classify different categories of errors that model phishing responses, and to better understand the way phishers provoke such errors.

b) The high quality of the phishing communication itself (in terms of its presentation, language used, use of external stimuli, personalization) is likely to stimulate the participants to believe in the authority of the phisher. Our participants who fell for the message stated that the message looked very realistic, and its language was very professional. They mentioned that adding footing to the message, encouraging them to book an appointment with the bank help desk, was one of the factors that made them believe the message was authentic. This confirms Jokobsson's suggestion that adding independent channel to the message creates trust (2007). The participants said they did not expect the attacker to encourage them to contact the bank, and hence they trusted the message, and contacted the attacker instead of contacting the bank.

c) Strong motives reduce rational thought. The financial motive used in the phishing message reduced the participants' rationality. In our study, we had participants who have more than one bank account, which possibly indicates big amount of savings. Accordingly, this strong motive influenced them to ignore the phishing alarms in the message. Consistent with this result, there is evidence that under conditions of high emotional influence, it is less likely that clues that reveal the real status of scam messages will be noticed (Langenderfer & Shimp, 2001; Fischer et al. 2008).

d) New phishing messages are likely to be extremely successful. Our participants who fell for the message said that the fact that the message did not ask them directly for either money, bank details, or systems password, made them believe, it was legitimate. Asking them to call back did not make them doubt the authenticity of the message, because they were unaware of the premium-rate numbers. They stated that they were under the impression that calling or texting is not harmful. Generally, most of our participants suffered a lack of awareness of 809 scams. So for them, this was a new type of phishing. This success of new phishing messages is supported by previous research in scams in general and phishing in particular (jakobsson, Fischer et al. 2008). Hence, for my participants, dialling a phone number to investigate perfectly made sense or as a recent scam literature refers to as: 'clouding of sensible decision-making' (Office of Fair Trading, 2009).

e) A counter-intuitive finding of study 3 is that phishing victims put ***more cognitive efforts*** into analysing the phishing message content than the detectors. The analysis indicated some interesting patterns in the victims' interviews. Some of them conducted careful mental analysis of the phishing message, that may have led them to detect it, but it did not. For example, some of the victims analysed the components of the message and stated they were able to spot certain cues that indicate the message is not authentic. For instance, they mentioned that the name of the bank was not mentioned at all, either in the message body, or in the message ID. They also stated that they expected the last four digits of their bank account to be included. They also, stated that communicating via mobile text is not the normal method they bank used in the past. This indicates that the participants put some cognitive effort in analysing the message. On the other hand, we have some participants who did not fall for the message, simply by ignoring it. They said "*I do not reply to such messages", "I just chose to ignore it"*.

This finding has series of implications:

a. This disproves previous research that claims that phishing victims are naïve (webroot 2013, Herzberg & Jbara 2008, Herzberg & Jbara 2004). This is also supported by our quantitative study results where those who scored high in Assertiveness were more likely to fall for the phish. Assertiveness has been correlated almost equally with **Intellect** (DeYoung et al., 2007), which contradicts with being naïve.

b. This disproves previous research that suggests that people fall for scams because they did not notice scam clues (Langenderfer & Shimp, 2001). Individuals may notice the inconsistent cues of phishing messages. Nevertheless, they make a decision error and fall for the phish. Our mobile users were able to detect clues in the phishing message that indicate that the message was not authentic (such as: the source, media and content of the message which did not match the default factors of their financial institutions, see section 5.5). Still and all, they fell for the phish and followed the phisher instructions. This is in accordance with fraud research where scams' victims recognized that there was something wrong with the message they received, yet, they decided to respond to the scam (Office of Fair Trade, 2012). This action was referred to as 'a long-odds gamble' (Fischer et al., 2008).

c. Integrating these qualitative results with the quantitative ones (reported in section 5.3) makes the picture clearer. It shows how the victims' reaction to the phishing message goes in line with the defining features of both ‘Assertiveness’ and ‘Extraversion’ personality traits of taking control, decision making, initiation and leadership. It explains how these qualities, in specific, made the victims intolerant for uncertainty. By responding to the message, they were, in fact trying to clear the inconsistency of the message cues (such as addressing the bank clients by their full name, yet, not mentioning bank name, etc.

e. Also this cognitive effort invested by the victims indicates that they were not impulsive in the way the interacted with the message, a question that the quantitative results have raised (given that the participants who were more likely to fell for the phish were extrovert and assertive). Although, being outgoing is one of the features of both assertive and extrovert individuals, and that extraverted behavior was linked in the literature to impulsivity (Guilford and Zimmerman 1949), the qualitative results reveal the cognitive exercise exerted by the victims to properly analyse the message. This suggests that their response was thoughtful and planned rather than impulsive.

2) Second Objective: Answering First Research Question (Effect of Previous Error in Judgment Experiences):

The study indicates a positive effect of previous error in judgement experiences on the individuals’ ability to detect phishing. This is consistent with the results of Study 1 (reported in chapter 3). Participants who suffered an upsetting experience in relation to phishing (or similar) interaction were less likely to fall for the phish. 33% of our detectors stated that they had experienced upsetting phishing experiences in the past. Some of the phishing messages they received purported to be from their bank, and some from their mobile operator. Some of them said that they lost trust in people after this bad incident. Some of these incidents were personal, where the participants themselves suffered the consequences, while some were suffered by one of their family members or a close friend. But in all cases mentioned in the interviews, the participants were able to recall all the details of the past incident, as they were heavily involved in the incidents helping their friends or family to track the hacker by reporting the event to the concerned service providers. This indicates that these rich past upsetting experiences affected the participants’ behaviour towards future phishing attempts, including ours.

This is in accordance with literature that performed studies on the effect of past personal experiences on individuals' perception of future events. In brief, those with previous personal experience of an event were more likely to believe they would have further experiences of that or similar type in the future. For those individuals, causal sequences are more likely to be constructed. As a result, that personal experience should make it easier for the individual to recall past occurrences of the event and to imagine situations in which the event could occur, leading to greater perceived probability of the event occurring again (Weinstein 1980, Tversky & Kahneman 1973). The phishing detectors in our study stated that it was their upsetting experience with phishing incidents that drove them to detect the message, in contrast to the victims who felt something was wrong with the message, yet they were too optimistic to think it was a phish. Weinstein (1980) explains that personal experiences of negative incidents, specifically, might decrease optimism about negative events by making images of the past events more available or by undercutting defensive denial.

More direct evidence is presented by (Pfleeger & Caputo 2012; Slovic 2000) in relating personal experience to events that involve risk. For that, Slovic (2000) describes the behaviour of those who depend on their experiential system in making decisions that involve risk, as being mediated by vibes from the past. Here the experiential system automatically searches its memory banks for related events, including their emotional accompaniments (Epstein, 1994). If the activated feelings are pleasant, they motivate actions anticipated to reproduce these feelings. If the feelings are unpleasant, they motivate actions anticipated to avoid such feelings.

Pfleeger and Caputo's (2012) evidence, relating specifically to phishing, is in accordance with our results. They believe that when individuals relate to their own real experiences, they can counter optimism bias that makes people underestimate risks or think they are immune to cyber-attacks. They gave spear phishing as an example.

In our study, when we compare the phishing experience of those who fell for the phishing to those who were able to detect it, we found that both groups knew about phishing, as they have stated, through their work in the field of information technology. They have heard about it via their service provider, or via their own surroundings in society. However, those who fell for our message had no direct connection with phishing incidents, they were unable to recall any memory in this regard. Some said they might have been victims before, but were unsure. On the other hand, those who were able to detect our message stated that not only have they experienced real phishing interaction, as being victims, but also they followed it up and contacted their service provider to trace the incident. Accordingly, previous personal phishing incidents were easier to remember because they are more sharply defined, whereas phishing stories were more difficult to characterize and therefore harder to recall. Our data hence confirm Slovic's (2000) suggestion that incidents differ in characteristics that may affect their memorability.

3) Third Objective: Answering Second Research Question (Effect of Personality):

The results indicate that Assertiveness and Extraversion are more likely to affect individuals' vulnerability to phishing. Both assertive and extrovert individuals were more likely to fall for phishing. The qualitative analysis suggests that the leadership, taking charge and outgoing qualities of these traits, especially in the context of a phishing message that hold many uncertainties and inconsistent cues, encouraged the mobile users to take initiative and communicate with the phisher and hence fall for the 809 scam.

The quantitative results also proposed a very surprising suggestion that individuals who scored low in 'Trust' were more likely to fall for the phishing message. Although this result seems odd and contradicts previous literature that linked low in trust to phishing detection not susceptibility, the qualitative results revealed that some participants were classified as detector-victims as they knew the message was a phishing attempt, but responded to the message aiming to catch the attacker. Also, the results indicated that the phishing message used succeeded in deceiving even cautious individuals (who are less likely to trust others) to follow the phisher instructions and call a premium rate number. This was mainly attributed to their ignorance of 809 scams. This confirms both our argument and Jakobsson's that new phishing techniques are more likely to succeed. This also indicates the limits of personality traits to fully account for phishing vulnerability without considering the content of the phishing message used.

Also, it is worth pointing out that this result of the personality trait 'trust' was not significant, as the p value was slightly higher than 0.05, as p= 0.07. Here psychology researchers suggested two ways of reporting these results:

a) reporting the result as approaching significant (Rice, 1989)

b) reporting the result as not-significant. Some researchers describe reporting results as approaching significance as 'statistically flawed' as it describes an aspect of the data that actually does not exist (Hankins, 2013). Opinion against reporting results as 'approaching significant' includes criticism to the authors as they set themselves the threshold of 0.05 for significance, yet failed to achieve that threshold value for p and hence described it in such a way as to make it seem more interesting (Hankins, 2013).

Accordingly, we choose to follow the second opinion and will not report the 'trust' personality trait as approaching significant.

4) Fourth Objective: Answering Third Research Question (Effect of Security Awareness):

The results revealed that general security background knowledge was not enough to help the mobile users to detect the phish. All our participants were IT specialists. However, 53% of them fell for the phishing message. Only those with a very specialized work experience (in cyber security or mobile communications) could detect the message based on their back grounds. Also the interviews showed the scarcity of the educating endeavours of the service providers such as banks and mobile operators, where banks were a little better in providing education to their customers. However, it was clear that banks policies differ in this regard and there is no consistency among banks in Egypt in providing similar type of phishing alerts to their clients. This is consistent with the Anti-Phishing Working group criticism to mobile service providers. They complain that mobile phones manufacturers and vendors want to sell their products, yet they provide little guidance other than basic start-up procedures. They stated that mobile devices sold come without instruction on how to stay safe other than a cursory "install only from trusted sources" (APWG, 2013). They also said: General advice on the dangers posed by phishing or "smishing" is available through the support or community sections of the operators' websites but advice specific to mobiles is hard to find. Our participants tend to trust mobile messages more than emails. Some of them even deleted the email we sent to them containing their amazon voucher to thank them for participating in our study. They said they thought it was a phishing attack. These same participants fell for our SMS message. This shows that there is a lack of awareness in regards to phishing on mobile phone, which requires more attention in training.

5.9 Proposed Actions

The results suggest that naturalistic phishing experiments can play an effective role in phishing education. The results showed that the hotlines of the service providers were busy and that the participants had to wait long time in a queue for their enquiry to be answered. This in fact facilitates the phishers job, as contacting him was way much easier than communicating with the legitimate service providers. We call for facilitating customer support and hot lines communication between customers and concerned parties such as banks and mobile operators. We encourage these service providers to consider the cost of reputational damage that may affect their organizations as a result of potential fraud attacks.

5.10 Threats to Validity

1-The Researcher effect: it is possible that some victims distort their responses by pretending that they did not get phished before either out of embarrassment or to make a certain social impression on the researcher. As reported by (Office of Fair Trade, 2012) some participants hid their responses to some scams from their own family members. Also Snyder (1986) reported that in the context of gambling swindles, victims did not want to admit they have been defrauded and avoided reporting swindles for fear of shame.

2- The interviews were not recorded, because they were conducted via international phone calls, as the participants were not located in the UK, which poses a threat to the reliability of the data. However, the researcher put every effort to make sure the data was reliable via repeating the question and making sure the participant fully understood it. She also repeated their answers to them before transcribing.

3-Experimental studies are subject to the effect of extraneous variables the researcher has no control over. These variables can bias the results and make it hard for other researchers to replicate the study.

6 Chapter 6: Second Mobile Naturalistic Phishing Experiment

In this chapter we report findings of our second naturalistic mobile phishing experiment. The experiment investigates human vulnerability to mobile text messages phishing.

6.1 Aims and Hypothesis

The previous chapters investigated a proposed explanation of phishing susceptibility grounded in the prior research presented in chapter 3 (Grounded Theory). It suggests that *the success of phishing attempts is accounted for by the victims' individual differences, specifically, their personality traits, moderated by their knowledge and upsetting past security experience.* This hypothesis was investigated in Chapter 4 (phishing Lab Study) and Chapter 5 (809 scam naturalistic phishing experiment).

In this chapter, we wish to support the results of our previous research studies using a new sample of mobile phone users. In contrast to study 3 (reported in chapter 5) which used an 809 scam (which measures users' vulnerability to call a premium-rate number) this study measures the participants' vulnerability to provide confidential information in response to a phishing text message.

6.2 Study Design

The study examines the relationship between personality traits and people's vulnerability to phishing attacks. The pseudo-independent variable was Personality traits. The dependent variable is phishing vulnerability.

Similar to the previous study reported in chapter 5, personality traits are referred to in this study as 'pseudo-independent variable' or 'the predicting variable'. More information about the rationale of such a decision is reported in chapter 5, section 5.3.1.

6.3 Study Settings

A governmental University in Cairo, Egypt, Helwan University, authorized us to carry out a simulated phishing scenario via its students' mobile phones. Helwan University comprises 20 departments and 50 research centres (Helwan University, 2014).

The university administration collaborated with the author to measure the students' susceptibility to mobile phishing. The participants were told that they were taking part in a study to assess their personality. They were asked to give the author their mobile number in order for her to contact them to receive their personality results at a later meeting.

6.4 Sampling

62 undergraduate and postgraduate students were recruited for the study. The sample included both male and female participants. The majority (60%) was male. The participants were aged between 21 and 40 years except 1 participant, who was 55 years old.

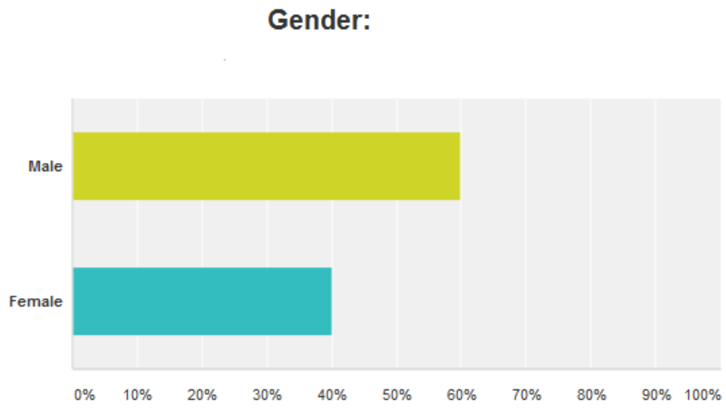


Figure 19: Gender Figures before Exclusion

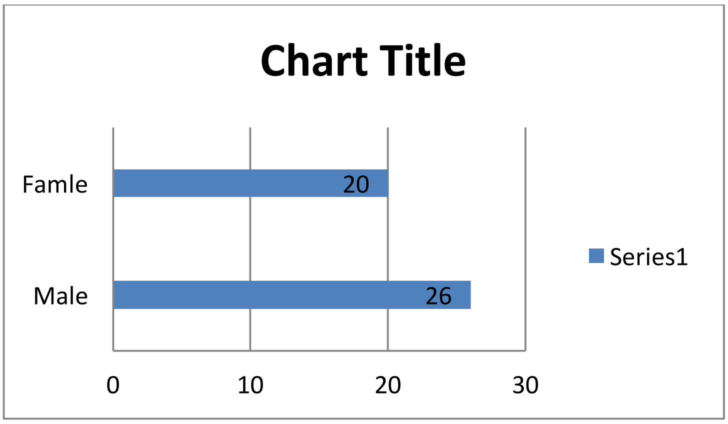


Figure 20: Gender Figures before Exclusion

Exclusion Criteria

Students were excluded from the study if they provided incomplete data via the questionnaire. This included participants who failed to complete the personality questionnaire fully and those who did not provide their mobile phone number. 16 students were excluded overall. Accordingly, the number of effective participants became 46 instead of 62.

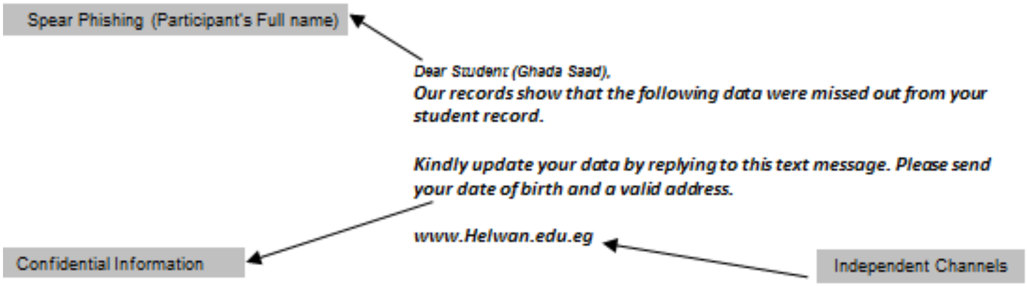
6.5 Study Procedures

The study procedures were broken into three distinct phases:
Step1- Data Collection
Step2- Simulated phishing
Step 3- Debriefing

Step1- Data Collection
In the first phase of the experiment the participants were given a link to an online questionnaire and were asked to fill it in within 10 days. The questionnaire was hosted on Survey Monkey, an online survey tool. Each participant completed the questionnaire individually. It consisted of two sections:

Section 1: Personal data. This section asked the participants for their age, gender, email and mobile phone.
Section 2: Personality Questionnaire. In this section the user filled the short version of IPIP-NEO personality traits test.

Step2- Simulated phishing
In this phase of the study, the mobile numbers provided to us by the participants via the questionnaire were used. The author sent a simulated phishing message (see Figure 21) to each of these participants' mobile phones, a few weeks later.



Dear Student (Ghada Saad),
Our records show that the following data were missed out from your student record.

Kindly update your data by replying to this text message. Please send your date of birth and a valid address.

www.Helwan.edu.eg

Figure 21:(Study 4) Phishing Message

The message pretended to be from the University and used a normal mobile number. It claimed that it was found that some data were missed from the student record (date of birth and home address) and asked the participants to text this data back. Following Jakobsson's suggestion (Jakobsson, 2007) that independent channels create trust, we included the University website at the foot of the message. The purpose of such an addition is to strengthen the respondents' trust in the phishing message.

The choice of the data required

Date of birth and home address were selected because they belong to the Personally Identifiable Information (PII) that can be used to identify a single person (UK Data Protection Act, 1998).

6.6 Instruments

This section discusses the psychological and technical instruments used in the study.

1- Psychological Instruments

The psychological instruments used in this study are the same as those reported in chapter 5, section 5.3.5.

2- Technical Instrument: SIM card

A new SIM card has been used and dedicated only for the experiment.

6.7 Ethical Procedures

The same ethical procedures applied in study three and reported in chapter 5 section 5.4 were applied. The only additional issue was the confidential data (Date of Birth and Address) sent to the researcher by the participants who fell for the message. In this regard, the University of York ethics committee has advised the researcher to keep the messages un-read till the participants' approval is granted in the debriefing process.

6.8 Analysis

For clarity, the analysis is presented in two sections. The first section is the quantitative analysis. The second section is the qualitative analysis. 19.5% (9 of 46) of the participants responded to the simulated phishing message by sending their data via a text message to the phisher mobile phone. These were considered to have demonstrated susceptibility to phishing. Individuals who ignored the phishing message or contacted the University were regarded as deception detectors (i.e. not susceptible to phishing).

6.9 Quantitative Analysis

The data collected was between-subjects. Between-subjects is an experimental design where there is only one design (one phishing message) where every participant contributes only once in the experiment. The frequency of which participants responded to the phishing message was recorded. Chi-Squared tests were performed to assess if the observed frequencies differ from those that would be expected by chance. The test was used to examine the association between our two main variables; Personality Trait and Phishing Response.

In order to analyse the measurements of each personality scale, the subjects have been placed in two different methods into identifying groups. For the first method, I used median split to create two groups for every personality trait: one representing the participants who scored 'low' in that trait, and the other representing the participants who scored 'high' in that trait. The median split is explained in more details in chapter 5, section 5.5.1. For the second method, tertile split was used to create 3 groups per every personality trait; low, high, and average. To strengthen the internal validity of the results, tertile split then eliminate the 'average' observations from the analysis to make sure that data truly represents high and low values.

No personality trait was found to be of statistical significance. The quantitative results and the contingency tables are attached in Appendix F.

6.10 Qualitative Study

Having established no personality trait that may affect individuals' susceptibility to phishing, the author sought to explore how other factors that may have influenced the participant response. For this purpose, a qualitative approach was adopted for this section of the study. During the debriefing process, a formal request for an interview was made from the same MSISDN number that initiated the phishing message. 25 participants took part in the follow-up interview, 15 did not respond, 4 did not remember receiving the phishing message and 2 were wrong numbers. The hypothesis proposed by the grounded theory reported in chapter 2 was the basis for the interviews.

The interviews were semi-structured, yet a pre-defined structure was preserved as a guide through the interview procedures. The interviews lasted 10-15 minutes. Data was recorded as notes as the interview proceeded and then more comprehensive documentation was transcribed from the notes. To ensure anonymity of the participants, each transcript was given a code to be used for quotations so only their initials are shown, no names. That was followed by a coding process.

Method

The qualitative analysis was submitted to thematic analysis (Boyatzis, 1998). This revealed the reported psychological processes that had led the participants to respond to the simulated phishing attempt the way they did.

6.11 Qualitative Analysis

In this section, we report some of the main themes that showed prevalence in the data analysis and that relate to the issue of phishing vulnerability. In each of the subsections below, we identify a significant theme. A more general interpretation is provided in the discussion section. In reporting the thematic analysis, we rely heavily on quotations from the participants.

The established categories used for the thematic analysis involved two major domains. The first was the 'victims', which included those participants who sent their data to the phisher via a text message. The second was the 'detectors', which included participants who either ignored the phishing message or communicated with a third party. 7 participants were categorized under the victims' category, while 18 fell under the detectors' category.

For the detectors, the thematic analysis revealed 15 thematic elements mapped into 8 areas of cognitive processes. For the victims, the thematic analysis revealed that 12 thematic elements were indexed and mapped into 5 areas of cognitive processes.

Table 47 presents the major themes and sub-themes for the first category (detectors). Table 50 presents the major themes and sub-themes for the second category (victims)

6.11.1 Major Themes for the detectors' Domain

Table 47: (Study 4) The Detectors' themes

Theme	Subcategory
1- Illogicality of the request	The acquisition of the requested data by the University
2-Expectation of institutional-specific factors	Expectation of usual University communication methods Expectation of usual University regulations
3- Expectation of both institutional and country use of technology	Expectation of certain level of technology employed in their University Expectation of certain level of technology employed in the country
4-Previous 'error in judgment' experiences of the detectors	Personal phishing or fraud experience Family member or close friend phishing experience Feeling easy to speak about past experiences
5-Exposure to several phone phishing attempts	No subcategory
6-Awareness of the thriving market of data	Caring for their data, as it's confidential. Caring for their data, as it's a business now.
7- Habitual reasons	Not trusting any one easily. High level of confidence of their decision. Past phishing experience.

1-Illogicality of the Request – Requesting information previously provided

A common theme among detectors was their confidence that they have already provided the University with the information requested by the phishing message (their birth date and address). In consequence, the students found it illogical for the University to ask for this data again.

"Every term, they have this information" **Participant 03**
"How come Uni does not have my data" **Participant 06**
"I felt suspicious because uni has my data", **Participant 13**
"I did not believe it, Uni already has this data. So it's not from uni", **Participant 12**

2-Expectation of specific Institutional Factors- Communication methods and regulations

A prevalent theme among detectors was their awareness and expectations of certain institutional factors. These included both the method of communication they expected their University to use and also the current regulations deployed by the University admin staff for updating students' records. In regards to the communication method, the students were astonished that their University communicated them via mobile.
"I did not expect Uni to contact me via mobile, that's not realistic", **Participant 10**
"That's the first time Uni contact us via mobile", **Participant 32**

The students also raised the issue that texting in specific was not expected.
"Even if they used mobile, I'd expect them to phone not to text", **Participant 11**

The students showed awareness of their University regulations.
"The University sends letters officially, or communicate face to face and even then, an official document should be signed and stamped", **Participant 21**
"I believe, if such data was missed, the University will ask me to attend in person not to just send them", **Participant 12**

It is worth mentioning that the students were not worried of any consequences that may result of them not sending the required information.

3-Expectation of both Institutional and Country use of Technology

The students showed certain expectations of the level of technological progression employed in their University in particular and their country in general. They doubted that their University administration would use texting as a tool of communication, since it is a governmental institution.

"UNI will not send any message, Uni deals with paper. (old system), it's just Not logical" **Participant 33**

"The uni is not so high-tech, to send such messages via mobile", **Participant 32**

"Abroad maybe, but in Egypt, no", **Participant 21**

It is worth noting that students in Egypt provide the University administration with their contact information (Home address, phone number, mobile number, etc.) as soon as they enrol to the university. The University then has the freedom to contact the students via any of these communication methods. This is supported by the comments of participant 19 who had checked with the university administration after receiving our phishing message. The administration mistakenly confirmed that the message is genuine and that it was sent by them. Also, the high response rate of the message (19%) proves that the message sent was expected by many students to be sent from the University.

4- Previous 'error in judgment' experiences of the detectors

61% (11 of 18) of the detectors had previous experience of error in judgment themselves, their family, or close friends as being victims of previous phishing and fraud scams.

"Once, someone sent me a link by email. I clicked it", **Participant 41**

"I received a message that promised me a prize, I visited their website, they asked me very personal questions, even political ones, when I used the number given to claim my prize, it was a fake number, I was really upset, and became more cautious since" **Participant 3**

"Also, two of my relatives, one was deceived by a message pretended to be from a bank and the other about network down, they gave their info and they both found money stolen from their bank accounts", **Participant 3**

"Some of my close friends fell for phishing and the hackers used their visa card details to buy things online", **Participant 56**

"It happened in front of my own eyes, to my brother, he got a message pretended to be from Vodafone, Since then I knew that anyone can fake an ID", **Participant 5**

"My best friend fell for similar message, they asked him for donations, he paid, but then discovered it was fake", **Participant 10**

5- Exposure to several phone phishing attempts

The students communicated the fact that they receive many phishing attempts via their mobiles, and landlines.

"I receive lots of messages on my mobile claiming that they have sent me mobile credit by mistake, I ignore them all the time", **Participant 33**

"I receive many messages of this sort, recent SMS I got said {congratulations! You have won a prize of 100 pounds credit, call to confirm}, others ask for address too, I ignore them", **Participant 11**

"I get phishing messages via mobile claiming they have sent me credit by mistake, I do not have extra credit, so I know it's fake,", **Participant 25**

"I guess the frequent messages I get on my mobile made me cautious", **Participant 14**

6- Cyber Security Awareness

The students were aware of the value of their data and how data has become a prosperous business nowadays.

"I thought someone has sold my data, and now it is misused", **Participant 5**
"HR companies buy and sell data, many of their jobs are even fake", **Participant 12**
"I work in digital Marketing, there is a big campaign fir this now", **Participant 46**

Caring for the confidentiality of their data was not the only reason students were keen not to text back their details. The feeling that data has become a flourishing business, made the students treat their data as an asset, which they believe they should not disclose free of charge.

"Data is a treasure, so I will never give my data for free, so, it was not for security reasons that I did not reply to your message", **Participant 46**

8- Habitual reasons

Some students explained that it is their nature/personality to think carefully before trusting anyone or divulge confidential information.

"Not anyone send me any message, I trust it", "Naturally, one should be always cautious", **Participant 10**

"Not any one claim to be uni, I believe him", **Participant 14**

"That's the culture I was raised by at home: not to trust anyone and not to give any data", **Participant 11**

"How can I share personal info", **Participant 21**

It was noticed that the students who referred to their nature of 'not trusting anyone easily' were all so confident of the decision they made (to ignore the message) to the extent that all of them (except one) did not even bother to check with the University administration.

"I do not trust everyone. Did not ask in admin office", **Participant 41**

It is also worth mentioning that all of the students who clearly stated they do not trust everyone, or believe every message, have previously interacted with phishing experiences either via close friends or family members. What needs investigation, in particular, is the position of Participant 41 and participant 25. Although, they have stated clearly they do not believe every message, they had been victims of phishing before. Participant 25 fell for 809 scams, he called an unknown number and was charged big amount of money as a result of that. Participant 41 was tricked by a phishing email to click a fake website and entre his password. This can either be explained that people say something while in reality they do something else, or that the bad experience they went through (interacting with phishing incidents) have really changed their security attitude.

Table 48: (Study 4) Previous Error-in-judgment incidents

Participant	Interaction with Phishing	Previous victim
Participant 10	Phishing Experience	Best friend
Participant 14	Phishing Experience	Mother
Participant 21	Phishing Experience	Best friend
Participant 25	Phishing Experience	Himself
Participant 41	Phishing Experience	Himself

Table 49: (Study 4) Participants with no Previous Phishing experience

Participant	Features
Participant 11	-No phishing error in judgement experience -Only exposure to many messages -Never been a victim

6.11.2 Major Themes for the Victims' Domain:

Table 50: (Study 4) The Victims' themes

Theme	Subcategory
1-Stimuli creating trust	Sense of Urgency & Importance of message. The official look of the message. The relevance of the request. External Stimuli.
2-Lack of cyber-security awareness	Lack of Knowledge about existence of Mobile phishing. Lack of Knowledge of phishing. C. Undermining the value of certain data. d. Content of the message
3-No exposure to phone phishing attempts	No subcategory
4- Insufficient educating endeavours from service providers	Receiving very rare awareness from concerned parties Regarding past phishing experiments as sort of awareness Regarding frequent phishing message as sort of awareness
5- The absence of error in Judgment experience	No subcategory

1) Stimuli Creating Trust – Urgency, Presentation, Relevance, External Stimuli
A very interesting theme among the victims was the sense of urgency and importance they perceive of the message although there was no mention in the message content of certain time frame by which they are required to send the claimed missing data.

"I instantly trusted the message and that it is from Uni, I felt the message was very important so that I had to respond quickly", **Participant 07**
"I sent it because I did not want to lose time", **Participant 47**

This can be explained as *obedience to authority figures* represented by the University administration.

The participants also referred to the official layout of the message.

"The message was formal", **Participant 47**
"I was really happy when I got the message, that our University is using that technology", **Participant 39**

They also stated that the request made sense as it was relevant to data which the University is interested in.
"Data was useful to my uni", **Participant 47**

By chance, our phishing message coincided with external stimulus in the university, which affected a number of students. At the time we sent the phishing message, there was some real chaos in the university administration office. Examples included delay in assigning students to courses, and a delay in issuing graduation certificates to final year students. When the students got our message which said some data were missing from their record, they were under the impression that these missing data was the cause of the actual chaos in the administration office. Accordingly, the students responded to our phishing message to push things forward.

What is really astonishing and proves the level of chaos in the administration and lack of communication between the University departments, is that when one of these students went to the admin office to enquire about our message, the admin assured him that they did text some students.

Note: We have included this participant in the victims' domain, as she has contacted the University after responding to the phishing message.

"There were some chaos in assigning subjects to students so your message made sense", **Participant 19**
"I went to the admin office after I have sent you the message, they confirmed they have sent the message but to year 3 not year 4!" **Participant 19**
"It was on the time of me getting my graduation certificate, so I trusted it. Because they were late to send me my certificate, I thought It is related", **Participant 27**

2) Lack of Cyber Security Awareness- phishing, mobile phishing
The participants had little knowledge about phishing in general and mobile phishing in particular.
"I know a little about phishing, mainly links download, or you won money", Participant 24
"I know about phishing but only in relation to bank tricks, so I do not leave much in my bank", Participant 38
"I have never heard about phishing", Participant 39

They did not know mobile phishing exists.

"I heard about phishing before, but via email only, not mobile", **Participant 7**

The victims undervalued the data requested by the phisher.

"The data was not critical so that I should worry", **Participant 47**
"I always reply if I got a message asking about address or date of birth", **Participant 38**

The content of the message itself was very important. Some participants stated that messages with financial nature are the only messages that worry them.
"When it is related to banks, that's clear, but because its uni, I did not think it's from a hacker", **Participant 24**

3) No exposure to phone phishing attempts
None of the victims mentioned receiving any sort of mobile messages, only email and Facebook were remarked.

"I have received an email before from a company promising a prize of 5 million dollars, it asked about my bank account", **Participant 7**
"Lot of messages: Facebook, email such as links to click or buttons to press", **Participant 19**

4) Insufficient Education Endeavours from Service Providers
All the participants stated that they have not received any training, awareness or updates from their mobile operator in regards to phishing. Two participants received security awareness from their banks. The first participant received security alerts in regards to general security practices which emphasized on use of passwords. The second participant was actually involved in a very unique experience, as his bank has invited him among some customers to a phishing training session at the bank premises one year before our experiment. The participant declared his dissatisfaction of the training.

"No awareness from my mobile operator. Only from my bank, it was only about passwords", **Participant 7**
"No security alerts from my mobile company", **Participant 19, Participant 24**
"My bank organized some training for the customers, one year before I got your message, I attended but was not interested, same boring traditional training", **Participant 38**
"No training at all", **Participant 39**

5) Absence of Previous Error in Judgment Experience

It was noticed that none of the victims has experienced a previous error in judgment experience of phishing or similar incidents.

"I was not a victim before" **Participant 19**
"I never fell for phishing", **Participant 24**

6.12 Discussion

The study indicated certain ***decision making errors***. These errors basically stemmed from trusting the message. This has coincided with lack of awareness of mobile phishing and undervaluing certain data (mainly, date of birth and address). The students who fell for the phish were under the impression that phishing only occurs via email or Facebook and will ask only either about financial information (such as debit or credit card details) or system information (such as user names and passwords).

***Individual's perception and interaction with the same educating endeavours differ* -** Although the students took the same module 'Computer Security' which introduced them to the concept of phishing, they differed in their judgment of the benefit of the module, its relevance to real life situations and level of details about phishing the modules has discussed. For example, when asked whether they were aware of phishing before, the students' answers ranged from knowing nothing to knowing very little. Same fluctuation in answers was noticed when the students were asked about how effective the phishing education they received via their module was. Most of the students felt the module lacked details and introduced phishing very lightly (hints, as they referred to it), with the exception of one student, who stated that since attending a lecture about phishing in the computer security module, he stated to be more cautious.

As much as this shows individuals' diversity of views, it raises an alarm about how ineffective current phishing education efforts are. Even the very rare phishing education endeavours made by service providers was regarded by the trainees as boring and non-beneficial (as described by the participant who has attended such training. Note: this participant fell for our phishing message).

This suggests that normal training (in forms of lecturing and message alerts) addresses peripheral learning routes rather than central ones and hence fail to empower the users with adequate knowledge about different security threats they may encounter in real life.

Phishing awareness was gained via different sources* -** It was expected that computer security curriculum and service providers' education efforts would be the first source of information for the students. However, other channels acted as the primary source of information for the students in regards to phishing. These include previous error in judgment experiences and frequent phishing messages circulating in the surroundings of the participants. This resulted in limiting the scope of phishing awareness to only financial-related or system-related messages as explained earlier. Consequently, when the students received our message that asked for neither the users' financials nor passwords, the students thought it was a legitimate message and fell for it. This also indicates and supports the conclusion of the previous study 3 that ***Creative new phishing messages are likely to be extremely successful.

Illiteracy of Mobile Phishing existence- Students were not aware of mobile phishing. Although they have received many messages about fake mobile credit, they stated that when they got our phishing message, they did not relate it with the sorts of messages they normally receive. This implies that they were under the impression that mobile phishing will only ask about mobile credit related issues.

Ignorance of Personally identifiable information- Many students were unaware of the value of some of their data such as their date of birth and home address. They stated they were not aware that such information is confidential and can be of use for impersonation purposes by hackers.

Chaos helps phishers - The disorder in the university registry services office increased the students' vulnerability to phishing. The students who witnessed problems associated with either issuing their graduation certificates or assigning them to modules, have interpreted the phishing message differently. They imagined that their response to the message was needed to help overcoming these admin problems. To our astonishment, when one of the students asked in the admin office about our phishing message, one of the employees in the admin office did confirm that the University had sent it! This reflects a lack of communication between the University's different departments, and how this can increase phishing susceptibility

Weak motives reduce phishing vulnerability - 19% of the students fell victim for the phishing message. Although, this is regarded as high phishing success rate (Luo, 2012), it is significantly lower than the success rate of study 3 reported in the previous chapter. One of the main differences between the two studies is the framing of the phishing message itself. In comparison to study 3, which adopted the 'financial loss framing, via warning the users from a possible paying for some online transactions they did not make, the current study barely used any motivation to encourage the students to respond. As the students mentioned, they were not worried of any consequences that may result of them not sending the required information. So, basically, no reward or penalty has been promised. These results are consistent with previous research that suggests that low motivation decreases scamming vulnerability (Langenderfer and Shimp 2001). Additionally, this message asked the participants to send some confidential data, in comparison to study 3 that asked the participants to call back.

Answering the First Research Question (Effect of Previous Error in Judgment Experiences:

Like, Study 1 and study 3, this study as well confirmed the effect of previous incidents of error in judgment on the individuals' susceptibility to phishing. Those who experienced previous phishing incidents, or alike, were less likely to fall for the phish. Moreover, many students stated that these upsetting phishing experience was also their only source of information in regards to phishing.

Answering the Second Research Question (Effect of Personality):

The results did not confirm any effect of the proposed personality traits on phishing vulnerability. This can be attributed to a number of reasons:

The type of the message itself- Although the phishing message sent to the students asked for confidential information, it did not adopt either loss or gain framing. Neither a reward nor a penalty was suggested for either responding to the message or ignoring it. According to decision making research, individuals' decisions are affected by 'risky-choice framing'. This refers to the interpretation of the same decision problem either as loss frame or gain frame. (Piñón and Gärling, 2004). According to recent research, there is a correlation between personality traits and framing effects and that these traits differ for gains and for losses (Lauriola & Levin, 2001a, 2001b; Levin et al., 2002).

Conformity effect- In a university of thousands of students, there is no guarantee that the students did not discuss the message together and possibly affected each other's decision.

Over-use of special participating groups- The sample included only the students who volunteered to participate in a study to test their personality. This by itself gives an indication of a quality of personality they may all share. Rosenthal and Rosnow found that participants recruited as volunteers are more sociable, intelligent, and are more likely to have a respect for science and scientists (Rosenthal & Rosnow, 1975)

Sample size- 46 students participated in the study, with the exclusion of 16 students who did not complete the personality questionnaire fully. This can be attributed to the length of the questionnaire (120 questions). This resulted in having a restricted number of participants. There is a possibility that a larger sample could have showed some significance of certain personality traits effect. Accordingly, we call for the conducting of more large-scale studies that have larger sample sizes and which, if possible, select the participants randomly.

Answering the Third Research Question (Effect of Security Awareness):

Although all the participants stated their dissatisfaction because of lack of proper awareness from concerned parties such as banks and mobile-operators, they varied in their levels of cyber security knowledge. It was noticed that those who were aware of the value of their data and of the thriving market of data nowadays were treating their data as 'assets' and were able to detect the phishing message. However, the students who were unknowledgeable in this regards fell for the phish. This indicates that education is a key in preventing users from phishing attacks.

6.13 Threats to Validity

1- The interviews were not recorded, because they were conducted via international phone calls, as the participants were not located in the UK, which poses a threat to the reliability of the data. However, the researcher put every effort to make sure the data was reliable via repeating the question and making sure the participant fully understood it, and she also repeated their answers to them before transcribing. For future studies recording is recommended.

2- Experimental studies are subject to the effect of extraneous variables the researcher has no control over. These variables can bias the results and make it hard for other researchers to replicate the study.

3- The sample included participants only from an Information Technology background. This affects our ability to generalize the results.

6.14 Proposed Actions

1- The results confirm the suggestion of study 3 for that naturalistic phishing experiments can play an effective role in phishing education.

2- The results revealed some pitfalls in computer security modules in Egypt that failed to empower students with enough knowledge on how to protect themselves from phishing threats and the like. However, we cannot be certain of this as we are unaware of the objectives of the curricula and whether the syllabus aimed at providing general or specialized knowledge about phishing

7 Chapter 7: Conclusion

7.1 Objectives of the Research

The present research started with the basic question of why a large number of individuals respond to phishing attacks. Why were millions of people unable to detect phishing messages? And so, online banking losses in the UK only have reached £30 million in the first half on 2014(FFA, 2014)? Why has SMS phishing grown 400 percent only in the first half of 2012 and more than 1 in 5 SMS spam in June 2013 were phishing attempts (GSMA, 2013)? And why do some individuals fall repeatedly for phishing despite losses incurred?

The thesis approach regards falling for phishing as a result of cognitive processes that guide individuals' decisions. We argue that the quality of a specific decision should be judged by its process not by its outcome. These processes are often based on cognitive and social heuristics which often lead to right decisions. But can sometimes lead to systematic deviation from logic which results in cognitive bias. On the basis of the present research, certain experiential factors as well as personality factors, that are more likely to guide the decision making process in judging phishing messages, are well supported. Our argument is supported by the results of four studies, specially the experimental studies, where the interviews of the participants, for example indicated that labelling falling for phishing as simply 'an error' is shallow, as there are wide range of decision errors, to the extent that we classified our users into three categories detectors, victims, and detector-victims. Note: the term 'falling for phishing' here refers to responding to the demands of the attacker (such as calling, texting, or sending confidential information).

Recognizing falling for phishing as an error in judgement brings an array of theoretical and practical resources that can be used to explain phishing vulnerability. This existing literature, reported in chapter 2, was inconclusive and contradictory, and hence did not help us generate the research hypotheses. Accordingly, we developed our own grounded theory reported in chapter 3 to produce the thesis hypotheses, especially that although the literature was diverse, it lacked research about SMS phishing (from human factor perspective). In that chapter, we have studied mobile users' perception of mobile security in general and mobile phishing in particular. As we argue that SMS phishing cannot be studied in isolation of the mobile context, which certainly affects potential victims' responses to phishing, we started by investigating how individuals perceive the security of their mobile phones widely, before focusing on SMS phishing solely. That study proposed a number of research questions that the thesis tackled via three further studies.

7.2 Contributions of the Thesis

We have conducted four studies in which we have used two research methodologies; self-report studies and experimental studies. We derive two main conclusions. First, in three of our four studies, we find evidence that individuals' history of error-in-judgement incidents positively affects their ability to detect phishing messages. Second, in three of our four studies, the Extraversion personality trait was correlated with phishing vulnerability. The Assertiveness personality trait, which is a sub-domain of Extraversion, was correlated negatively with phishing detection in two of our studies.

1) First conclusion (The effect of history of error in judgement)

The results indicate the effect of previous interaction with phishing scams on individuals' ability to detect future phishing messages. In particular, those who were previous-victims of phishing attacks or similar error-in- judgement incidents were more able to detect phishing messages. They were more likely to expect similar event to occur in the future and the similarity between two events (past and present) made it easier for them to recall their past personal experiences. On the other hand, individuals who have received phishing training or have been receiving phishing alert messages from their service providers were not less likely to fell for phishing.

2) Second conclusion (Effect of personality)

The results indicate that the personality trait Assertiveness significantly affect individuals' vulnerability to phishing. Assertiveness affected phishing susceptibility negatively in two of our four studies (reported in chapter 4 and 5). The more assertive a person is, the less likely that they will be able to detect phishing. This effect can be explained by the taking-charge, and speedy decision-making qualities of assertive people, who may rush into making a decision which may be wrong, especially in the case of new types of phishing attacks, such as 809 scams investigated in the present thesis.

The results also indicate that the personality trait Extraversion is more likely to affect individuals' vulnerability to phishing. Extraversion affected phishing susceptibility negatively in the two self-report studies (reported in chapter 3 and 4) and positively in the experimental study (reported in chapter 5). The inconsistency of our experimental results from those derived from our self-report studies (in regards to Extraversion) highlights the sensitivity of the results to the research methodology employed as well as the phishing message content. This conclusion was expected in light of previous research that suggested the importance of delving beyond individuals' assessment of their own attitudes and intentions via self-report constructs (Wilhelms & Reyna 2014; Jakobsson 2007). However, we could not use the experimental approach for all our studies as explained below.

Although experimental research is well-established in the field of Psychology, it is relatively new to the security discipline. Naturalistic phishing researchers face lots of challenges to get ethical approval for their research from their institutions' ethics committees (Oh & Obi 2012, Jakobsson & Finn 2007) because of the deception involved in these studies. We experienced these difficulties as well, one of our experiments was approved after 9 months.

The negative relation between Extraversion and phishing vulnerability suggested by the self-report studies can be explained by the fact that introverts are more withdrawn in nature, so they are less likely to be aware of common spread phishing messages that are known and familiar to those who are more extrovert. On the other hand, the positive relation between Extraversion and phishing vulnerability suggested by the experimental study can be explained by the outgoing, leadership and taking charge qualities of Extroversion as well as its subcategory Assertiveness (whose correlation to phishing vulnerability was highly significant).

We should not also overlook the sensitivity of the results to the type of phishing message used. Every phishing message triggers certain motives. In the literature the effect of extraversion was interpreted differently among several studies which reached same result, yet used different phishing messages. For example, we find studies explaining the reason why extroverts fall for phishing because extroverts are optimistic, so they do not expect risk. Other studies explain that extroverts prefer high benefit than low risk. In the field study presented in this thesis (chapter5), extroverts fall for the phishing message (i.e. responding by calling a premium-rate number) because they were intolerant of uncertainty.

Therefore, we call for investigating the effects of personality via use of different phishing messages with different frames (such as gain, loss, etc.) for each study. We recommend the experimental approach to be used because of its external validity, as it helps assessing true decisions rather than hypothetical ones.

Key finding:

None of the previous research studies that concluded that extraversion affects phishing vulnerability has suggested which facet under extraversion is responsible for such an effect. The present research, suggested that assertiveness is the facet (subcategory under extraversion) that correlated with the participants' phishing vulnerability. However, we stress again that this is sensitive to the phishing message used.

Unexpected results:

Neither Agreeableness nor Conscientiousness had an effect on individuals' vulnerability to phishing, opposed to what was suggested by our grounded theory and by a number of phishing literature studies that linked phishing vulnerability to levels to trust (note: Trust is a subcategory under Agreeableness trait).

However, this counter-intuitive conclusion was supported and explained by our results. Our experimental studies showed that phishing victims deploy greater cognitive efforts to analysing the phishing messages than the detectors. This proves that falling for phishing is not just a simple matter of trust, where individuals who tend to trust others (High in Agreeableness) are more likely to fall for phishing. But rather, the decision made is a result of certain cognitive processes that are, to an extent, influenced by the individual personality trait, but not fully justified by it. We distinct here between 'influenced by' and 'fully justified by', referring to the power of personality traits to act as a 'descriptive' rather than a 'predictive' factor of phishing vulnerability, for the following reason:

We argue that the studies that investigate personality and phishing will be more likely to be sensitive to the phishing message content. For example, the effect of the personality trait 'trust' can be used to assess phishing vulnerability to a message that asks for confidential details. But if the message is only asking the user to call or text, for example, then the effect of 'trust' will not be clear, because of the lack of risk perception involved.

This was also supported by the quantitative results that found trust correlated negatively with phishing vulnerability to 809 scams. This again supports our position in regarding personality as a *descriptive* rather than *predictive* of human phishing vulnerability.

3) Third Contribution

The thesis contributes the first 3 studies to investigate human responses to SMS phishing (both lab studies and experimental studies). All studies especially the two experimental studies underscore the high vulnerability of mobile users to fall for SMS phishing, as the response rates of both studies were 53% and 19%. These are considered high response rates in comparison to current phishing emails rates. According to a recent study (Luo, 2012) that investigated phishing emails success rates, 36% and 15% were regarded as high rates.

The thesis suggested a number of reasons for such high vulnerability:

a) The mobile users stated that they do not expect phishing via SMS, but rather via their emails. As reported in the results of our 809 scams, some participants who fell for the phishing message were highly alerted in regards to their email messages to the extent that they mistakenly detected our amazon voucher reward email message as a phishing attempt. Accordingly, some deleted it and others ignored it.

b) Phishing scams that deploy new techniques, especially those using strong motives, are more likely to be successful. In our first phishing experiment (reported in chapter 5), the use of 809 scams with a strong financial motive reduced rational thought and hence the participants responded to the phishing message.

c) The type of the data requested in the phishing message affects the message response. In the second phishing experiment (reported in chapter6) the students stated they were not aware that giving away date of birth and personal address is risky.

4) Fourth Contribution

The thesis draws attention to an effective phishing training method that is phishing naturalistic experiments that are based on simulating phishing attempts.

7.3 Other key findings

The findings showed that users were more expecting to detect phishing received via normal communication channels and with familiar phishing content. In this regard, the users did not expect to receive phishing via their mobile phones but via their e-mails. They also stated that they had expected phishing messages to be of a financial nature and not concerned with their date of birth or address.

The findings highlighted that messages of a social interaction nature are less likely to be detected by mobile users, especially those messages that ask the victims to text or call premium-rate numbers. The findings also pointed out that prizes and award messages are more likely to be detected by the users.

The findings presented different types of decision-making errors in regards to phishing. The interviews with the phishing victims revealed that simply labelling them as either naïve or greedy is shallow. In this regard, we stress the need to classify different categories of errors that model phishing responses, and to better understand the way phishers provoke such errors.

A counter-intuitive finding is that phishing victims put a lot of cognitive effort into analysing the phishing message content. That disproves previous research that claim that people fall for phishing because they did not notice phishing cues. On the other hand, some detectors simply ignored the phishing messages.

7.4 Implications for Practice:

How can our improved understanding of the human factors involved in SMS phishing help reduce its risks?

a) Implication for using Research for Training Purposes: The thesis suggests that interaction with phishing has been proven to contribute to protecting individuals from falling as victims. Accordingly, the present research calls for such interactions. The question is how to create such incidents of phishing interaction. For that, we suggest using naturalistic phishing experiments as an education tool. The interviews conducted with 79 participants showed they (all except one) welcome being phished for educational purposes and that they enjoyed the experience and felt it was more personally relevant to them than the previous security training they have received.

Implication: These results have crucial implications for the development of phishing awareness programs. They highlight the importance of conducting naturalistic experiments in tandem with educating mobile users of different types of phishing attacks, rather than separately, as has been the case to a large degree in phishing training to date (Jagatic et al. 2007; Alseadoon 2012).

In this regard, we are in the process of designing a framework for the use of naturalistic experiments as a phishing training tool.

b) Implication for Current Education Programs: The results indicate that phishing victims put more cognitive effort into analysing the phishing messages content than the detectors. This disproves previous research that suggests that people fall for phishing because they do not notice the scam cues.

Implication: Phishing Education programs that focus solely on training users on detecting phishing cues are likely to be less effective. Many of our participants were able to detect such cues. However, they still fell for the phishing message. This is in agreement with the results produced by the Office of Fair Trading (2009) which suggests that victims often act against their own better judgement.

Accordingly, phishing awareness raising programs should aim not only at educating people how to recognise phishing cues but also how to resist them. More focus on the implications and the potential losses of responding to phishing messages is needed. This is expected to encourage people receiving phishing attacks to search for reasons why they should not respond to the phishing message rather than searching for reasons why they should. Education efforts should also alarm people against performing any form of communication with the phisher.

c) Implications for Future Education Programs:

(i) The personality results can be used to direct education against phishing by using personality tests to craft better training.

(ii) Our results indicate that the messages that include loss are more likely to deceive users than those who involve gain. Examples are the results of our lab study, when users were less likely to fall for prize and monetary awards. Hence I encourage awareness programs to focus more on messages that involve loss than gain in training users against phishing.

d) Implication for Phishing Research: the cognitive effort exercised by the participants in analysing the messages suggests that their response was thoughtful and planned rather than impulsive. This suggests that phishing research that uses impulsivity measures to test the participants' phishing vulnerability is less likely to be reliable.

e) Implications for service providers: the results tell us that even computer specialists still need reminders about security attacks in general and phishing in particular. Although, all our participants had an IT background, a significant number of them still fell for the phishing messages.

f) Implications for Policy: Our experiments have achieved high rate of response: 53% in first experiment and 19% in second experiment. According to Luo et al. (2012) these are considered high rates. This calls for a change in mobile operators' policies to put restrictions on the number of messages sent by a subscriber, similar to the policy employed by Korea and China, explained in section 1.1.

g) Implications for Law: The experiments indicated that messages that do not ask for confidential information but simply ask the users to call or text back (809 scams) are more likely to deceive the mobile users. The European Union has introduced legislations aimed at both email and mobile messages and resulted in enforcing the 'opt-out' approach. Through this approach, companies who wish to use mobile messages for alerts or for advertisement purposes need to add an 'opt-out' note asking users to send an 'opt-out' message if they do not wish to receive such messages. Based on the high response rates of our 809 scam experiment, we argue that this law can be misused by attackers to encourage mobile users to text premium-rate numbers. Many technical consultants such as Jamie Cowper have questioned the effect of this law. We urge appropriate change.

7.5 Limitations and Threats to Validity

1- The main limitation of the studies is that cultural differences may have affected the results. The experimental studies were both conducted with Egyptian participants, while the lab studies were conducted with non-Egyptians. The culture of data privacy and confidentiality is new to the Egyptian society. There are barely any laws or regulations that organize it. Accordingly, individuals' data can easily be distributed via their service providers without any prior agreement. This atmosphere also has led to unawareness of the Egyptian participants of the value of some of their personal information such as date of birth and address.

2- Although, the psychological instrument used to measure the participants' personality, IPIP, was effective in understanding different aspects of the users' traits specially that it tests the big five sub-domains, which enabled us to link phishing vulnerability to the sub-domain assertiveness, it used a very long questionnaire. It is composed of 120 questions and this may have driven many of the participants away and leading to small samples. In this regard, the present research calls for the use of shorter instruments.

3- Although the lab study suffers from threats to ecological validity, given the artificial environment they were conducted in, they can easily be replicated by other researchers.

4- The experimental studies are subject to the effect of extraneous variables which the researcher has no control over. These variables can bias the results and make it hard for other researchers to replicate the study. However, these studies provide high ecological validity and are more generalizable than lab studies.

7.6 Future work:

1- As the thesis suggests using naturalistic phishing experiments as an effective phishing educational tool to improve users' strategies in combating phishing, and although, this sort of experiments has been introduced and applied recently to measure people's responses to simulated phishing attacks, the current practices available in the literature cannot be generalized to provide guidance and assistance on how to use these experiments for educational purposes. Accordingly, our aim is to provide a framework for using naturalistic experiments for educational purposes. The framework will be in accordance with a number of behavioural science theories that have been suggested to have implications on cyber security and on attitude change and will cover both the design of the phishing message as well as the ethics and etiquette of the debriefing process.

2- We plan to conduct a repeated-observation study to test the effectiveness of the proposed framework. The study will be basically a naturalistic experiment, which will be followed by another experiment with the same participants to test if the proposed framework has helped in protecting them against phishing attacks.

3- The thesis investigated phishing vulnerability among individuals who have been mobile users for at least one year. Further studies to investigate novice users' susceptibility to phishing can provide new insight to the field of phishing research.

7.7 Recommendations

1- We recommend that phishing experiments proposals get are evaluated by social sciences ethics committees, rather than by physical sciences ethics committee, given that the deceit-based experiments are well-established in the fields of Psychology and Social Sciences, but relatively new to the Computer Science discipline. So inviting members with social science or psychology background, who are more likely to be familiar with this type of research, or even forming a joint ethics committee of both social sciences and physical sciences member, can provide better judgement on the proposal as well as giving useful insight and advice to the researchers.

2- We recommend that experimental phishing researchers design the studies with special care to the ethical and legal issues involved. We discussed these issues and provided the steps we followed in chapter 5 and chapter 6. We also published two papers to provide a roadmap for researchers on how to design ethical and legal phishing experiments.

7.8 Closing Remarks

These results have important implications for the development of phishing awareness programs. They highlight the importance of conducting naturalistic experiments in tandem with educating mobile users of different types of phishing attacks, rather than separately, as has been the case to a large degree in phishing training to date. In addition, the inconsistency between our experimental results from those derived from our self-report studies, in regards to personality traits, highlights the sensitivity of the results to the research methodology employed as well as the phishing message content. Therefore, this apparent inconclusiveness warrants the need for further investigation of the relationship between phishing and personality. In this regard, the thesis challenges other research that simply relates certain traits of personality to phishing vulnerability depending on studies that measure one type of phishing stimulus.

8 Bibliography

Adali, S., & Golbeck, J. (2014). Predicting personality with social behavior: a comparative study. *Social Network Analysis and Mining*, *4*(1), 1-20.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

Alberto, P. and Troutman, A.C. (2003) *Applied behavioral Analysis for Teachers (6th ed)* Upper Saddler River, NJ: Merrill, Prentice Hall

Al-Hamar, M., Dawson, R., & Al-Hamar, J. (2011). The need for education on phishing: a survey comparison of the UK and Qatar. *Campus-Wide Information Systems*, *28*(5), 308-319.

Alseadoon, I., Chan, T., Foo, E., & Gonzales Nieto, J. (2012, January). Who is more susceptible to phishing emails?: a Saudi Arabian study. In ACIS 2012: Deakin University, Geelong, Victoria: *Proceedings of the 23rd Australasian Conference on Information Systems 2012* (pp. 1-11). ACIS.

Anandpara, V., Dingman, A., Jakobsson, M., Liu, D., & Roinestad, H. (2007). Phishing IQ tests measure fear, not ability. In *Financial Cryptography and Data Security* (pp. 362-366). Springer Berlin Heidelberg.

Anderson, M. R. (2010). Community psychology, political efficacy, and trust. *Political Psychology*, *31*(1), 59-84.

Anti-Phishing Working Group APWG (2015). Phishing Activity Trends Report, 4th Quarter 2014. Retrieved March 2015. available http://docs.apwg.org/reports/apwg_trends_report_q4_ 2014.pdf

Armin, J., Komarov, A., Parkour, M., Chiesa, R., Thompson, B., Rogofsky, W. (2013). Mobile Threats and the Underground Marketplace. Retrieved November 1, 2014, from http://docs.apwg.org/reports/mobile/apwg_mobile_fraud_report_april_2013.pdf

Ashford, W. (2014) Phishing Attacks Track Mobile Adoption, Research Shows. Retrieved from http://www.computerweekly.com/news/2240215873/Phishing

Bagley, P. L. (2007). Evaluation Apprehension: An Examination of Affect in the Audit Environment (Doctoral dissertation, University of Georgia). Retrieved from https://getd.libs.uga.edu/pdfs/bagley_penelope_l_200705_phd.pdf

Bandura, A. (1994). *Self-efficacy*. John Wiley & Sons, Inc..

Bauer, P. C., & Freitag, M. (2013). Personality and the Foundations of Social Trust. In *EPSA 2013 Annual General Conference Paper* (Vol. 103).

Bishop, G. F., Oldendick, R. W., Tuchfarber, A. J., & Bennett, S. E. (1980). Pseudo-opinions on public affairs. *Public Opinion Quarterly*, *44*(2), 198-209.

Blau, J. (2006, August 28). McAfee Warns of SMishing. Retrieved from
http://www.pcworld.com/article/126932/article.html

Bogdan, R. C., & Biklen, S. K. (2006). *Qualitative research for education: An introduction to theory and methods,* 5th Edition. Boston: Ally and Bacon.

Boodaei, M. (2011, January). *Mobile Users Three Times More Vulnerable to Phishing Attacks.* Trusteer. Retrieved from http://www.trusteer. com/blog/mobile-users-three-times-more-vulnerable-phishing-attacks

Borkenau, P., & Ostendorf, F. (1990). Comparing exploratory and confirmatory factor analysis: A study on the 5-factor model of personality. *Personality and Individual differences*, *11*(5), 515-524

Bortinik S. (2011, January). *Why Do Phishing Attacks Work Better On Mobile Phones*? Retrieved from http://www.welivesecurity.com/2011/01/20/why-do-phishing-attacks-work-better-on-mobile-phones/

Bott, E. (2010). Favourites and others: reflexivity and the shaping of subjectivities and data in qualitative research. *Qualitative research*, *10*(2), 159-173.

Bown J. (2015, January 9). Premium rate text trap: retired vicar billed £200 for gambling text he did not want [online]. Retrieved from http://www.telegraph.co.uk/finance/personalfinance/household-bills/11328500/Premium-rate-text-trap-retired-vicar-billed-200-for-gambling-texts-he-didnt-want.html

Boyatzis, R. E. (1998). Transforming qualitative information: Thematic analysis and code development. Sage: Cleveland.

Boyce, L. (2016). Bank customers targeted in new 'SMishing' scam: Warning After one customer lost £23,000 [Online]. Retrieved from http://www.thisismoney.co.uk/money/saving/article-3438512/Beware-smishing-scam-saw-one-Santander-customer-lose-23k.html

Bradley, T. (2014, May 7). Report: Phishing scams increasingly using mobile apps to bait victims. Retrieved from http://www.pcworld.com/article/2152042/kaspersky-report-phishing-scams-using-mobile-apps-to-bait-victims.html

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101.

Brostoff, S., & Sasse, M. A. (2001, September). Safe and sound: a safety-critical approach to security. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 41-50). ACM., 2002.

Buston, K., Parry-Jones, W., & Livingston, B. Wood.(1998). *Qualitative research. The British Journal of Psychiatry*, *172*(3), 197-199.

Butler, R. (2007). A framework of anti-phishing measures aimed at protecting the online consumer's identity. *The Electronic Library*, 25(5), 517-533

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication*, *52*(2), 167-182.

Charmaz, K. (2006) Constructing Grounded Theory: A Practical Guide through Qualitative Analysis. Thousand Oaks: Sage Publications.

Cairns, P. and Cox, A.L. *Research Methods for Human-Computer Interaction.* Cambridge University Press, New York, NY, USA, 2008.

Chatfield, C. (1995). *Problem solving: a statistician's guide*. CRC Press.

Chuchuen C. & Chanvarasuth P. (2010). The Relationships Between Phishing Techniques And The User Personality Model. *ICLT 2010 - 2nd International Conference on Logistics and Transport*, Queenstown NZ.

CIFAS (2013). Fraud Trends 2013 (21 January 2014), Retrieved from https://www.cifas.org.uk/twentythirteen_fraudtrends. (Accessed 11 March 2014).

Ciochetto, S. (1995). How Do You Measure “Awareness”? Experience with Lead-based Paint Survey. In *Proceedings of the Section on Survey Research Methods. Alexandria. VA: American Statistical Association* (p. 1163).

Coleman James, S. (1990). Foundations of social theory. *Cambridge MA (Belnkamp).*

Comer, R. J. (2004) *Abnormal Psychology (5th ed);* Worth Publishers, New York.

Compupharaohs (2006), Retrieved May 2012 from http://compupharaohs.com/

Congress (2009). *M-Spam Act of 2009.* Retrieved from https://www.congress.gov/bill/111th-congress/senate-bill/788

Costanzo, L. A., & MacKay, R. B. (Eds.). (2008). *Handbook of research on strategy and foresight.* Edward Elgar Publishing.

Cranor, L. F., Egelman, S., Hong, J. I., & Zhang, Y. (2007, December). Phinding Phish: An Evaluation of Anti-Phishing Toolbars. In NDSS.

CSO Online. (2015). *CSO's 2015 Mobile Security Survival Guide,* George V. Hulme.

Cukier, W. L., Nesselroth, E. J., & Cody, S. (2007, January). Genre, narrative and the" Nigerian Letter" in electronic mail. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (pp. 70-70). IEEE.

DeSantis, L., & Ugarriza, D. N. (2000). The concept of theme as used in qualitative nursing research. *Western Journal of Nursing Research*, *22*(3), 351-372.

DeYoung, C. G., Quilty, L. C., & Peterson, J. B. (2007). Between facets and domains: 10 aspects of the Big Five. *Journal of personality and social psychology*, *93*(5), 880.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590). ACM.

Dinesen, P. T., Nørgaard, A. S., & Klemmensen, R. (2014). The civic personality: Personality and democratic citizenship. Political Studies, 62(S1), 134-152.

Direct Marketing Association (2010). Mobile Messaging Effectiveness. Retrieved from http://dma.wearearch.com/sites/default/files/tookit_files/MobMessageEffectivenessSept10.pdf

Dittrich, D., Bailey, M., & Dietrich, S. (2009). *Towards community standards for ethical behavior in computer security research*. Technical Report 2009-01, Stevens Institute of Technology, Hoboken, NJ, USA.

Dohmen, T., Falk, A., Huffman, D., & Sunde, U. (2008). Representative trust and reciprocity: prevalence and determinants. *Economic Inquiry*, *46*(1), 84-90.

Dong, X., Clark, J. A., & Jacob, J. (2008, May). Modelling user-phishing interaction. In *Human System Interactions, 2008 Conference on* (pp. 627-632). IEEE.

Dourish, P., Grinter, R. E., De La Flor, J. D., & Joseph, M. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, *8*(6), 391-401.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006, July). Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security* (pp. 79-90). ACM.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007, October). Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 37-44). ACM.

Driscoll, c. (2012, March 21) Ignore that Text, You Didn't Win a Walmart Gift Card. Retrieve from http://www.bbb.org/blog/2012/03/ignore-that-text-you-didnt-win-a-walmart-gift-card/#sthash.BPgVq2BW.dp

Dunham, K. (2008). Mobile malware attacks and defense. Syngress Publishing.

Emigh, A. (2005). Online identity theft: Phishing technology, chokepoints and countermeasures. *ITTC Report on Online Identity Theft Technology and Countermeasures*.

Epstein, S. (1994). Integration of the cognitive and the psychodynamic unconscious. *American psychologist*, *49*(8), 709.

Eysenck, W. (2004). Research methods: Psychological enquiry.

Federal Communications Commission (2013). Retrieved November 12, 2014 from http://www.fcc.gov/

Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011, October). A survey of mobile malware in the wild. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices* (pp. 3-14). ACM.

Field, A. and Hole, G. (2003). How to design and report experiments. London: Sage Publications.

Finkelstein, S., Whitehead, J., & Campbell, A. (2013). *Think Again: Why Good Leaders Make Bad Decisions and How to Keep it From Happeining to You*. Harvard Business Press.

Fischer, P., Jonas, E., Frey, D., & Kastenmüller, A. (2008). Selective exposure and decision framing: The impact of gain and loss framing on confirmatory information search after decisions. *Journal of Experimental Social Psychology*, *44*(2), 312-320.

Freitag, M., & Traunmüller, R. (2009). Spheres of trust: An empirical analysis of the foundations of particularised and generalised trust. *European Journal of Political Research*, *48*(6), 782-803.

Gajek, S., & Sadeghi, A. R. (2008). A forensic framework for tracing phishers. In *The Future of Identity in the Information Society* (pp. 23-35). Springer US.

Garbarino, E., & Johnson, M. S. (1999). The different roles of satisfaction, trust, and commitment in customer relationships. *the Journal of Marketing*, 70-87.

Gartner. (2015). *How Digital Business Reshapes Mobile Security*. Dionisio Zumerle, Nathan Hill.

Gist, M. E., & Mitchell, T. R. (1992). Self-efficacy: A theoretical analysis of its determinants and malleability. *Academy of Management review*, *17*(2), 183-211.

Gist, M. E., Schwoerer, C., & Rosen, B. (1989). Effects of alternative training methods on self-efficacy and performance in computer software training. *Journal of applied psychology*, *74*(6), 884.

Glaser, B., & Strauss, A. (1967). The discovery of grounded theory. 1967. *Weidenfield & Nicolson, London*, 1-19.

Görling, S. (2006, October). The myth of user education. In Virus Bulletin Conference (Vol. 11, p. 13).

Gudkova, D. (2014). **Spam in Q1 2014,** Retrieved December, 2014, Year, from http://securelist.com/analysis/quarterly-spam-reports/59423/spam-in-q1-2014/

Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, Personality Traits and Facebook. *arXiv preprint arXiv:1301*.7643.

Harrell, M. C., & Bradley, M. A. (2009). *Data collection methods. Semi-structured interviews and focus groups*. RAND NATIONAL DEFENSE RESEARCH INST SANTA MONICA CA.

Helwan University (2012), Retrieved March, 1, 2012, from http://www.helwan.edu.eg/english/

Herz, R. (1997) 'Introduction: Reflexivity and Voice', in R. Hertz (ed.) *Reflexivity and Voice*. Thousand Oaks, CA: Sage.

Herzberg, A., & Gbara, A. (2004). *Trustbar: Protecting (even naive) web users from spoofing and phishing attacks*. Cryptology ePrint Archive, Report 2004/155. http://eprint. iacr. org/2004/155.

Hickey, A. (2006, September). SMS Phishing is Here. Retrieved from http://www.computerweekly.com/feature/SMS-phishing-is-here

Hiraishi, K., Yamagata, S., Shikishima, C., & Ando, J. (2008). Maintenance of genetic variation in personality through control of mental mechanisms: A test of trust, extraversion, and agreeableness. *Evolution and Human Behavior*, *29*(2), 79-85.

Informa Telecoms & Media report. Informa Telecoms and Media. Technical Report, London, 2009. Retrived from http://telecoms.com/tag/informa-telecoms-media/

Ingvar, D. H. (1984). "Memory of the future": an essay on the temporal organization of conscious awareness. *Human neurobiology*, *4*(3), 127-136.

Jaeger, R. G., & Halliday, T. R. (1998). On confirmatory versus exploratory research. *Herpetologica*, S64-S66.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94-100.-100, October 2007.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

Jakobsson, M. (2007). The human factor in phishing. *Privacy & Security of Consumer Information*, *7*, 1-19.

Jakobsson, M. (2010). Are Nigerian Scams From Nigeria?. Retrieved March 15, 2012, from http://www.securityweek.com/are-nigerian-scams-nigeria

Jakobsson, M. (2011). Why Mobile Security is not Like Traditional Security. Retrieved from https://pdfs.semanticscholar.org/b3c2/bf91010350315f84bff452b1df7c429ff576.pdf

Jakobsson, M., & Finn, P. Designing and conducting phishing experiments (2007). *IEEE Technology and Society Magazine, Special Issue on Usability and Security.*

Jakobsson, M., & Myers, S. (Eds.). (2006). Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons.

Jakobsson, M., Finn, P., & Johnson, N. (2008). Why and how to perform fraud experiments. *Security & Privacy, IEEE*, *6*(2), 66-68.

Jevans, D. A. (2015). *U.S. Patent Application No. 14/918,535.*

John, O. P., Naumann, L. P., & Soto, C. J. (2008). Paradigm shift to the integrative big five trait taxonomy. *Handbook of personality: Theory and research*, *3*, 114-158.

Jones, G. R., & George, J. M. (1998). The experience and evolution of trust: Implications for cooperation and teamwork. *Academy of management review*, *23*(3), 531-546.

Kahneman, D., Slovic, P., & Tversky, A. (1982). Judgment under uncertainty: Heuristics and biases.

Kanfer, R. (1990). Motivation and individual differences in learning: An integration of developmental, differential and cognitive perspectives. *Learning and Individual Differences*, *2*(2), 221-239.

Karthikeyan, K. (2009). An Empirical Study on Consumers' Perception Towards Korean Mobiles in Chennai City. *IUP Journal of Management Research*, *8*(12), 44.

Kaspersky (2012). *Kaspersky Security Bulletin 2012* [Online]. Retrieved from https://securelist.com/analysis/kaspersky-security-bulletin/36843/kaspersky-security-bulletin-spam-evolution-2012

Kaspersky (2014). *Kaspersky Security Bulletin 2014* [Online]. Retrieved from http://securelist.com/files/2014/12/Kaspersky-Security-Bulletin-2014-EN.pdf

Katsirikou, A., & Skiadas, C. H. (2012). *New Trends in Qualitative and Quantitative Methods in Libraries: Selected Papers Presented at the 2nd Qualitative and Quantitative Methods in Libraries: Proceedings of the International Conference on QQML2010, Chania, Crete, Greece, 25-28 May 2010*. World Scientific.

Kienpointner, M. (2006). How to present fallacious messages persuasively: The case of the "Nigeria Spam Letters. *considering pragma-dialectics*, 161-173.

Kirlappos, I., & Sasse, M. A. (2012). Security Education against Phishing: A Modest Proposal for a Major Rethink. *IEEE Security and Privacy Magazine*,10(2), 24-32.

Kotler, P., & Armstrong, G. (2006). *Principle of marketing* (11th ed.). Upper Saddle River,

NJ: Pearson.

Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems*, *48*(4), 15-24.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2), 7.

Lambert, C., Jomeen, J., & McSherry, W. (2010). Reflexivity: a review of the literature in the context of midwifery research. *British Journal of Midwifery*, *18*(5), 321.

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing*, *18*(7), 763-783.

Lee, S., & Klein, H. J. (2002). Relationships between conscientiousness, self-efficacy, self-deception, and learning over time. *Journal of Applied Psychology*, *87*(6), 1175.

Leyden, J. (2003, September 10). *UK- Anti-Spam Law Goes Live* [Online]. Retrieved from http://www.theregister.co.uk/2003/12/10/uk_antispam_law_goes_live/

Li, S., & Schmitz, R. (2009). A novel anti-phishing framework based on honeypots (pp. 1-13). IEEE.

Locke, E. A., & Latham, G. P. (1990). Work motivation and satisfaction: Light at the end of the tunnel. *Psychological science*, *1*(4), 240-246.

Liu, W., Deng, X., Huang, G., & Fu, A. Y. (2006). An antiphishing strategy based on visual similarity assessment. *Internet Computing, IEEE*, *10*(2), 58-65.

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28-38.

Love, S. (2005). Understanding mobile human-computer interaction. Butterworth-Heinemann.

Mackey, A., & Gass, S. M. (2005). *Second language research: Methodology and design*. Nahwah, NJ: Lawrence Erlbaum Associates.

Mann, R. (2006). Reflexivity and researching national identity. *Sociological Research Online*, *11*(4).

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. sage.

MillerSmiles.co.uk. 419 scams. http://419.millersmiles.co.uk/.

Minor, J. (2015, June 1). Mobile Threat Monday: Russian Game Play Market Only Sells Malware. Retrieved from http://uk.pcmag.com/software/42370/feature/mobile-threat-monday-russian-google-play-market-only-sells-m

Mobile, N. Q. (2012). Security Report,". *NQ Mobile's Security ab*. Retrieved from http://www.nq.com/2012_NQ_Mobile_Security_Report.pdf

Marshall, C., & Rossman, G. B. (2006). Designing Qualitative Research. Sage Publications*: California*.

Marshall, M. N. (1996). Sampling for qualitative research. *Family practice*, *13*(6), 522-526.

Martocchio, J. J., & Judge, T. A. (1997). Relationship between conscientiousness and learning in employee training: mediating influences of self-deception and self-efficacy. *Journal of Applied Psychology*, *82*(5), 764.

McAfee. (2015). *McAfee Labs Threat Report* [Online]. Retrieved from https://www.mcafee.com/uk/resources/reports/rp-quarterly-threats-aug-2015.pdf

McCrae, R. R., & Costa Jr, P. T. (1997). Personality trait structure as a human universal. *American psychologist*, *52*(5), 509.

McCrae, R. R., & Costa Jr, P. T. (1999). A five-factor theory of personality. *Handbook of personality: Theory and research*, *2*, 139-153.

Micro, T. (2013). Mobile security. Retrieved from http://media.cancom.de/attachments/d/4/d4f90e0f-5bd3-924c-84f6-0fc2e4e3740e.pdf

Mohebzada, J. G., El Zarka, A., BHojani, A. H., & Darwish, A. (2012, March). Phishing in a university community: Two large scale phishing experiments. InInnovations in Information Technology (IIT), 2012 International Conference: Abu Dhabi (pp. 249-254). IEEE.

Mondak, J. J. (2010). Personality and the foundations of political behavior. Cambridge University Press.

Mondak, J. J., & Halperin, K. D. (2008). A framework for the study of personality and political behaviour. *British Journal of Political Science*, *38*(02), 335-362.

Mondak, J. J., Hibbing, M. V., Canache, D., Seligson, M. A., & Anderson, M. R. (2010). Personality and civic engagement: An integrative framework for the study of trait effects on political behavior. *American Political Science Review*, *104*(01), 85-110.

Moody, G., Galletta, D., Walker, J., & Dunn, B. et al. (2011). Which Phish Get Caught? An Exploratory Study of Individual Susceptibility to Phishing. *Proceedings of the International Conference on Information Systems, ICIS 2011*, Shanghai, China.

Mulaik, S. A. (1987). A brief history of the philosophical foundations of exploratory factor analysis. *Multivariate Behavioral Research*, *22*(3), 267-305.

Muir, J. (2003). Decoding mobile device security. *ComputerWorld*, 14.

Musthaler, L. (2013, March). How to avoid becoming a victim of SMishing. *Network World*,. Retrieved from http://www.networkworld.com

Nielsen, J. (2012). Why you only need to test with 5 users, 2000. Jakob Nielsen's Alertbox. Retrieved from www. useit. com/alertbox/20000319. html.

Norris, J., & Ortega, L. (2003). Defining and measuring SLA. *The handbook of second language acquisition*, 716-761.

Ofcom. (2015). *Ofcom's 2015 Communications Market Report* [Data file]. Retrieved from https://www.ofcom.org.uk/research-and-data/cmr/cmr15

Office of Consumers and Business Affairs (2008). *The little Black Book of Scams*. Retrieved from http://www.consumeraffairs.nt.gov.au/ForConsumers/Scams/Documents/little_black_book_of_scams_comprehensive.pdf

Office of Fair Trading. (2009) *The psychology of scams: Provoking and committing errors of judgement.* Prepared for the Office of Fair Trading by the University of Exeter School of Psychology. Devon, UK

Oh, Y., & Obi, T. (2012). Evaluation of Field Phishing Study Setup Method. *International Journal of Information and Network Security*, *1*(4), 235.

Oskarsson, S., Dawes, C., Johannesson, M., & Magnusson, P. K. (2012). The genetic origins of the relationship between psychological traits and social trust. *Twin Research and Human Genetics*, *15*(01), 21-33.

Oxford Dictionaries on-line. http://oxforddictionaries.com/

Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks. *Little Rock: University of Arkansas.*

Peterson, R. L. (2007). Affect and financial decision-making: How neuroscience can inform market participants. *The Journal of Behavioral Finance*, *8*(2), 70-78.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others?. *Information Management & Computer Security*, 20(1), 18-28.

Paxton, P. (2007). Association memberships and generalized trust: A multilevel model across 31 countries. *Social Forces*, *86*(1), 47-76.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), 597-611.

Phishing Scams. Retrieved March 12, 2014, from http://www.onguardonline.gov

Phishme.com. Phishme Products and Services. http://phishme.com

Potter, W. J., & Levine-Donnerstein, D. (1999). Rethinking validity and reliability in content analysis.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7), 241-253.

Robila, S. A., & Ragucci, J. W. (2006, June). Don't be a phish: steps in user education. In *ACM SIGCSE Bulletin* (Vol. 38, No. 3, pp. 237-241). ACM.

Robinson, R. V., & Jackson, E. F. (2001). Is trust in others declining in America? An age–period–cohort analysis. Social Science Research, 30(1), 117-145.

Rosenthal, R., & Rosnow, R. L. (1975). The volunteer subject.

Rusch, J. J. (1999, June). The "social engineering" of Internet fraud. In Internet Society Annual Conference, http://www. isoc. org/isoc/conferences/inet/99/proceedings/3g/3g_2. htm.

Ryan, G. W., & Bernard, H. R. (2003). Techniques to identify themes. *Field methods*, *15*(1), 85-109.

Scamdex.com. Scam Email Archive. http:// www.Scamdex.com

Schierz, P. G., Schilke, O., & Wirtz, B. W. (2010). Understanding consumer acceptance of mobile payment services: An empirical analysis. *Electronic commerce research and applications*, *9*(3), 209-216.

Schiller, J. H. (Ed.). (2003). *Mobile communications*. Pearson Education.

Schuman, H., & Presser, S. (1996). Questions and answers in attitude surveys: Experiments on question form, wording, and context. Sage Publications.

Secure Mail Anti-Phishing. Retrieved from http://www.hsbc.com/1/2/online-security/phishing

Security Cartoon (2013). Retrieved February 2103, from http://Securitycartoon.com

Security For The Post-PC Era. Mobile Security (2013). Retrieved March 3, 2103, from http://www.Lookout.com

Sharp, H., Rogers, Y., & Preece, J. (2007). Interaction design: beyond human-computer interaction. 2002.

Shaughnessy, John J & Zechmeister, Eugene B., 1944- & Zechmeister, Jeanne S (2000). *Research methods in psychology* (5th ed). McGraw-Hill, Boston MA

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, July). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88-99). ACM.

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information*, *22*(2), 63-75.

Shields, P. M., & Rangarajan, N. (2013). *A playbook for research methods: Integrating conceptual frameworks and project management*. New Forums Press.

Shull, F.; Singer J.; Sjøberg, D.I.K. (Eds.). (2008). *Guide to advanced empirical software engineering* (Vol. 5). Germany: Springer.

Skinner, B. F. (1953). *Science and human behavior*. Simon and Schuster.

Slovic, P. E. (2000). *The perception of risk*. Earthscan Publications.

Soghoian, C. (2008, October). Legal risks for phishing researchers. In *eCrime Researchers Summit, 2008* (pp. 1-11). IEEE.

Srikwan, S., & Jakobsson, M. (2008). Using cartoons to teach internet security.Cryptologia, 32(2), 137-154.
Statista. (2016). *Smart Phone Usage in the UK 2015-2016* [Data file] Retrieved from
https://www.statista.com/statistics/387218/market-share-of-smartphone-devices-in-the-uk/

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 124-133. Retrieved from sciencedirect: http://www.sciencedirect.com/science/article/pii/S0167404804001841

Strauss, A., & Corbin, J. M. (1990). Basics of qualitative research: Grounded theory procedures and techniques. Sage Publications, Inc.

Stavroulakis, P., & Stamp, M. (Eds.). (2010). *Handbook of information and communication security*. Springer Science & Business Media.

Stebbins, R. A. (2001). *Exploratory research in the social sciences* (Vol. 48). Sage Publications.

Sudman, S., & Bradburn, N. M. (1982). Asking questions: a practical guide to questionnaire design. Retrieved from http://www.popline.org/node/633345

Symantec Internet Security Threat Report (2015). Retrieved from https://www.symantec.com/security-center/threat-report. Retrieved January 2016.

Sztompka, P. (1998). Trust, distrust and two paradoxes of democracy. *European Journal of Social Theory*, *1*(1), 19-32.

The State Council of China (2006). *Regulation Launch to cut junk mail* Retrieved from http://www.gov.cn/english/2006-02/22/content_206772.htm

Timpano, K. R., & Schmidt, N. B. (2013). The relationship between self-control deficits and hoarding: A multimethod investigation across three samples. *Journal of abnormal psychology*, *122*(1), 13.

Pajares, P., & Abendan, G. (2013). Why Phishing Goes Mobile [Online]. Retrieved from https://blog.trendmicro.com/trendlabs-security-intelligence/when-phishing-goes-mobile/

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive psychology*, *5*(2), 207-232.

University of Sydney (2016). Sydney Cyber Security Network. Retrieved from http://sydney.edu.au/arts/research/cybersecurity/

Uslaner, E. M. (2002). *The moral foundations of trust*. Cambridge University Press.

Utter, D. (2006, August). McAfee Says Watch out for SMishing. Retrieved from http://www.securitypronews.com/mcafee-says-watch-out-for-smishing-2006-08

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*,51(3), 576-586.

Wally, S., & Baum, J. R. (1994). Personal and structural determinants of the pace of strategic decision making. *Academy of Management journal*, *37*(4), 932-956.

Wang, W., & Benbasat, I. (2008). Analysis of trust formation in online recommendation agents. *Journal of Management Information Systems*, *24*(4), 249-273.

Wehmeyer, M. L., Agran, M., & Hughes, C. (1998). *Teaching self-determination to students with disabilities: Basic skills for successful transition*. Paul H. Brookes Publishing Co., PO Box 10624, Baltimore, MD 21285-0624.

Weirich, D., & Sasse, M. A. (2001, September). Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 137-143). ACM.

Wendy, L. (2007). NEO PI-R - A Guide to Interpretation and Feedback in a Work Context. Hogrefe Ltd, Oxford. Retrieved from https://www.unifr.ch/ztd/HTS/inftest/Web-Informationssystem/en/4en001/d590668ef5a34f17908121d3edf2d1dc/hb.htm

Whittingham, M. J., Stephens, P. A., Bradbury, R. B., & Freckleton, R. P. (2006). Why do we still use stepwise modelling in ecology and behaviour?. *Journal of animal ecology*, *75*(5), 1182-1189.

Wickens, T. D. (2002). Elementary Signal Detection Theory. Oxford University Press. *New York*.

Wilhelms, E. A., & Reyna, V. F. (Eds.). (2014). *Neuroeconomics and Decision Making*. Psychology Press.

Workman, M. (2008). Wisecrackers: A theory- grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science and Technology, 59(4), 662-674.

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where did they go right? Understanding the deception in phishing communications. *Group Decision and Negotiation*, 19(4), 391-416.

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006, April). Do security toolbars actually prevent phishing attacks?. *In Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 601-610). ACM.

Xu, Z., & Zhang, W. (2012). Victimized by Phishing: A Heuristic-Systematic Perspective. *Journal of Internet Banking and Commerce*, *17*(3).

Ye, Z. E., Smith, S., & Anthony, D. (2005). Trusted paths for browsers. *ACM Transactions on Information and System Security (TISSEC)*, 8(2), 153-186.

Ying, L., Dinglong, H., Haiyi, Z., & Rau, P. (2007). Users' Perception of Mobile Information Security. *Hacker Journals White Papers.*

Zhang, Y., Hong, J. I., & Cranor, L. F. (2007, May). Cantina: a content-based approach to detecting phishing web sites. In *Proceedings of the 16th international conference on World Wide Web* (pp. 639-648). ACM.

Zhang, Y., Wei, T., & Xue, H. (2014, November 25). SMS Worm Runs Wild in Singapore. Retrieved from: https://www.fireeye.com/blog/threat-research/2014/11/sms_worm_runs_wildi.html