A Malware Threat Avoidance Model for Online Social Network Users

A thesis submitted for the degree of Doctor of Philosophy

By

Ehinome Ikhalia

Department of Computer Science

Brunel University

September, 2017

Abstract

The main purpose of this thesis is to develop a malware threat avoidance model for users of online social networks (OSNs). To understand the research domain, a comprehensive and systematic literature review was conducted and then the research scope was established. Two design science iterations were carried out to achieve the research aim reported in this thesis. In the first iteration, the research extended the Technology Threat Avoidance Theory (TTAT) to include a unique characteristic of OSN – Mass Interpersonal Persuasion (MIP). The extended model (TTAT-MIP), focused on investigating the factors that needs to be considered in a security awareness system to motivate OSN users to avoid malware threats. Using a quantitative approach, the results of the first iteration suggests perceived severity, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy and mass interpersonal persuasion should be included in a security awareness system to motivate OSN users to avoid malware threats. The second iteration was conducted to further validate TTAT-MIP through a Facebook video animation security awareness system (referred in this thesis as Social Network Criminal (SNC)). SNC is a Web-based application integrated within Facebook to provide security awareness to OSN users. To evaluate TTAT-MIP through SNC, three research techniques were adopted: lab experiments, usability study and semi-structured interviews. The results suggest that participants perceived SNC as a useful tool for malware threat avoidance. In addition, SNC had a significant effect on the malware threat avoidance capabilities of the study participants. Moreover, the thematic analysis of the semi-structured interviews demonstrated that the study participants' found SNC to be highly informative; persuasive; interpersonally persuasive; easy to use; relatable; fun to use; engaging; and easy to understand. These findings were strongly related to the constructs of TTAT-MIP. The research contributes to theory by demonstrating a novel approach to design and deploy security awareness systems in a social context. This was achieved by including users' behavioural characteristic on the online platform where malware threats occur within a security awareness system. Besides, this research shows how practitioners keen on developing systems to improve security behaviours could adopt the TTAT-MIP model for other related contexts.

Acknowledgements

I am happy to express my deepest gratitude to my principal supervisor: Dr Alan Serrano for his endless insightful guidance throughout the duration of this thesis. Dr Serrano's contributions and consistent feedback influenced the momentum of this thesis positively; and I am indeed appreciative of the level of enthusiasm he demonstrated during our meetings to further improve the research quality. Dr Serrano was not just my research advisor, he demonstrated genuine care for my welfare and wellbeing like a father would especially during my most challenging periods.

I am also grateful for the timely corrections and insights provided by my second supervisor – Dr Derek Groen. Dr Groen was always ready to discuss any issue concerning my research even during unscheduled hours. Special thanks to Dr Kathy McGrath, whose guidance on how best I could adopt theories for my research was immeasurable. Dr McGrath made research methodology a "walk in the park" as I was able to understand information systems paradigms through her research methodology sessions. Thanks to Professor Robert McCredie for his valuable time management and viva preparation skills which ensured I got more done within the shortest time available. I cannot complete this acknowledgement without mentioning Dr David Bell, whose advice propelled me to acquire more relevant data during the second iteration of this research. I am also grateful to the head of department – Professor Tracy Hall for creating an enabling research atmosphere in the department of Computer Science.

I would like to appreciate all academic and non-academic staff and my colleagues for all the unique roles they played in ensuring this thesis was successfully completed.

Finally, I am deeply grateful to my dear mother and siblings who provided all the psychological support that I needed during the challenging times I faced in my PhD journey.

This thesis is dedicated to God Almighty and

My lovely mother;

Nancy Adesuwa Ikhalia

Publications

The following papers have been published, accepted for publication and submitted for peer review as a result of the research conducted for this thesis.

Published

[1] Ikhalia, E. and Arreymbi, J., (2014). Online Social Networks: A Vehicle for Malware Propagation. In *Proceedings of the 13th European Conference on Cyber warfare and Security*: ECCWS (p. 95).

[2] Ikhalia, E. and Serrano, A. (2015). A Framework for Designing an Effective Security Awareness System for Online Social Network Users. In: *European, Mediterranean & Middle Eastern Conference on Information Systems*. Athens, Greece.

[3] Ikhalia, E. and Serrano, A. (2016). Developing a New Model for the Avoidance of Malware Threats through Online Social Networks. In: *15th International Conference WWW/Internet 2016*. Mannheim, Germany: IADIS.

[4] Ikhalia, E., Serrano, A. and Bell, D. (2017). Developing and Implementing TTAT-MIP for the Avoidance of Malware Threats through Online Social Networks. *IADIS International Journal on WWW/Internet*, 15(1).

[5] Ikhalia, E., Serrano, A. and Arreymbi, J. (2018). Deploying Social Network Security Awareness through Mass Interpersonal Persuasion. In: *13th International Conference on Cyber Warfare and Security*. Washington DC, USA: ICCWS.

Submitted for Peer Review

[1] Ikhalia, E and Serrano, A. (2017). a Malware Threat Avoidance Model for Online Social Network Users: a Mass Interpersonal Persuasion Approach: Submitted to the *Computers in Human Behaviour* on September 10, 2017.

Honours and Awards

The following honours and awards were achieved as a result of the research conducted for this thesis.

[1] First Runner Up, 3 Minute Thesis Competition (3MT) https://www.brunel.ac.uk/study/postgraduate-study/graduate-school/Researcher-Development/Research-Student-Conference-and-3MT March 31, 2017

[2] Best Paper, 15th International Conference on WWW/Internet October 31, 2016

[3] Best Presentation, Computer Science Doctoral Consortium April 22, 2016 http://www.brunel.ac.uk/cedps/computer-science/news-and-events/news/ne_478615

Table of Contents

List of Figures

List of Tables

Glossary

AGFI	Adjusted Goodness of Fit Indices
AVE	Average Variance Extracted
C & C	Command and Control Server
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CR	Composite Reliability
CSS	Cascading Styles Sheet
DDoS	Distributed Denial of Service
DSR	Design Science Research
EFA	Exploratory Factor Analysis
GFI	Goodness of Fit Indices
HTML	Hypertext Mark-up Language
MIP	Mass Interpersonal Persuasion
MySQL	My Structured Query Language
OSN	Online Social Networks
PHP	Hypertext Pre-processor
RMSEA	Root Mean Square Error of Approximation
SEM	Structural Equation Modelling
SNC	Social Network Criminal
SRMR	Standardized Root Mean Square Residual
SUS	System Usability Scale
TTAT	Technology Threat Avoidance Theory
TTAT-MIP	Technology Threat Avoidance Theory – Mass Interpersonal Persuasion
URL	Universal Resource Locator

Chapter 1: Introduction

1.1 Overview

This Chapter introduces the research domain, which investigates malware threat challenges of online social network (OSN) users. The significance of malware threat avoidance within the context of OSNs is then highlighted. Afterwards, the research aim and objectives are outlined. In addition, the methodology adopted to execute the research is described and the logical arrangement of the thesis is outlined.

The Chapter is arranged accordingly: **Section 1.2** describes the research background which includes the research problem and motivation and scope. **Section 1.3** highlights the research aim and objectives. **Section 1.4** describes the methodology adopted for the research while **Section 1.5** presents the thesis arrangement.

1.2 Background

Online social networks (OSNs) have transformed the manner individuals establish social and business relationships (Bapna et al., 2017; Cheung et al., 2011). It has introduced vast benefits to society, such as helping users reconnect with lost friends and family, establishing new connections and promoting business products and services (Agnihotri et al., 2013). At the time of putting this thesis together, reports show that major OSN platforms are growing exponentially at inconceivable speed. Facebook has attained 1.86 billion active users monthly; Instagram follows with 600 million active users; LinkedIn has about 467 million active users; while Twitter and Snapchat have 319 and 158 million monthly active users respectively (Statista, 2016).

On the other hand, the distribution of malware through OSNs have grown exponentially recent times, consequently drawing interests in research (Boshmaf et al., 2012; Gold, 2010; Makridakis, A., Athanasopoulos, E., Antonatos, S., Antoniades, D., Ioannidis, S., & Markatos, 2010; Sanzgiri, Joyce and Upadhyaya., 2012). A malware is any software used to disrupt computer operations, illegally gather

sensitive information, gain access to private computing devices, or inconvenience users through unwanted advertising pop-ups (Provos et al., 2007; Tam et al., 2017). The severities of malware threats are enormous, ranging from reputation damage, financial loss, psychological traumas, data destruction and economic meltdown (Fan and Yeung, 2010; Gao et al., 2010; Ikhalia, 2013; Sood, 2011). OSNs have created new vectors for the distribution of malware threats from a user to his/her connections at an outrageously high speed that seemingly overpowers the capabilities of most anti-malware software (Faghani and Saidi, 2009a).

Computers and the Internet have both become intertwined with our lives. Every day users are becoming more dependent on digital devices and the Internet for completing even the smallest of tasks (Odaci and Çelik, 2016; Shrivastava et al., 2018). OSNs are now the leading means of communication and interaction between individuals (Penni, 2017). Users personal data generated as a result of the use of all these devices are of enormous financial value to attackers (Ullah et al., 2018). Even in offices and organizations, attackers target employees to infiltrate the organization's system instead of a direct attack (Krombholz et al., 2015). Cyber threats have evolved while cyber security is still trying to catch up. In such times, anti-malware software is almost somewhat insignificant compared to the level of threats an average user may encounter (Algarni, 2013; Robertson et al., 2010).

Most anti-malware software operates on the principle of blacklisting to identify and prevent malware from infecting users' computer devices. Sophisticated threats, however, can remain undetected by the anti-malware software for a long time and cause considerable damage to users and organisations. There are countless new malware created every day. Anti-malware software is argued as an effective measure at preventing known malware threats based on pre-defined algorithms, but when a new, unfamiliar threat arises it passes into an organisations network unnoticed. Cyber security engineers first require an understanding of the new malware before they can work on generating the solution. By the time an update comes up with the newly integrated functionalities for combatting new threats, time has already elapsed and the damage has been done to the organisation.

Malware attacks today are aimed directly at individuals instead of their systems. An untrained user is the weakest link in the cybersecurity of any organization. Social

engineering is a technique used by cyber criminals which involves manipulating individuals to gain their trust and make them unknowingly divulge valuable information. Another technique, phishing, is used mostly for obtaining credentials and ID and login information which can then be used for infiltrating the system. It involves using fake website pages that look identical to the legitimate login pages. The login information entered goes directly to the attackers. URL Links are distributed through emails, instant messaging apps and OSNs. The links and messages are cleverly designed to appear as though they are from legitimate social websites, banks, auction websites, online payment processors, etc. Malvertising is another method which pulls malware to the network of organisations. This is done without the knowledge of either employees or the legitimate website being used for this purpose. Customized attacks tailored to each target's security loopholes and weaknesses are another way to initiate a successful attack.

Consequently, anti-malware software would be relatively inadequate in combatting attacks executed through any of the afore-mentioned techniques. Anti-malware software is not necessarily useless; it is just not enough of a protection anymore. When users consider their safety from malware threats based on the supposed protection of their installed anti-malware software makes them even more susceptible to attacks. Debatably, the most efficient way to stay secure is to adopt a multi-layered security system using not just anti-malware software but other security measures such as improving user security awareness.

The speed of malware distribution through OSNs has been attributed to the inherent trust that exists amongst users and their interpersonal connections (Cao and Caverlee, 2014; Faghani et al., 2012; Fan and Yeung, 2010). Research suggests that OSN users have a high tendency to trust 'online contents' shared by their connections. Consequently, malware creators (often referred as attackers) are frequently leveraging the trust-based relationships to lure unaware users into installing malware on their devices. Prior research suggests that 300,000 unique variants of malware are being created on a daily basis (Paganini, 2015). To say the least, this astounding figure seems quite cumbersome for security practitioners to handle using anti-malware software alone. Although there have been efforts in improving the capabilities of modern-day anti-malware software using cloud technology, recent successes of malware attacks suggest that these efforts are

insufficient to combat malware threats from OSNs (Gao et al., 2011; Guo et al., 2016; Inayat et al., 2017).

As the rate of OSN adoption advances, its viability for attackers as a malware distribution platform increases proportionately. These types of pattern shifts in malware distribution have previously occurred. In preceding years, viruses attacked files due to the frequent exchange of floppy disks. Email as a message delivery platform is also exploited by attackers using spam as well as email-based worms. Instant messaging (IM) applications were not excluded as well. Today, the age of information systems development is experiencing another pattern shift in malware distribution techniques with OSNs as the foremost medium.

The underlying technique used for the distribution of malware through OSNs is social engineering (Heartfield and Loukas, 2015; Nelms et al., 2016). Social engineering, or the use of deception to obtain personal or confidential information for fraudulent purposes, is an attackers cunning manipulation of the human propensity to be trustful, helpful, lazy and fearful (Gupta et al., 2017; Luo et al., 2011; Rößling and Müller, 2009). With OSNs, the most common type of social engineering malware attacks involves persuading unaware users to click on a malware link which redirects them into a replica of a legitimate website with a prompt to update a 'software' to access the 'content'. The 'software' is essentially a malware which enables the attacker to remotely control the victims' computing device. Once the malware is installed, it posts the malware to the victim's social network profile (e.g. Facebook timeline) and notifies the user's friends/followers, thereby infecting more users at a rapid scale. OSN malware has the capability of sending private chats to other users connected to a 'victim' which spreads the infection even further (Baltazar et al., 2009; Carman, 2014; Gritzalis et al., 2014).

The functionalities of OSNs present a plethora of opportunities for malware attackers to exploit the ignorance, curiosities, and trust of users to lure them into downloading malware on their devices. For example, when Osama bin Laden was killed in 2011, a malware script masquerading as video of the incident surfaced on Facebook three hours after the news broke. Similar attacks were executed after the 2011 earthquakes in Japan. Iranian hackers lured unaware users to download malware via a variety of OSNs, including Facebook, Twitter, Google and LinkedIn.

The weakest connection in information systems security chain is the users (Safa et al., 2016). Malware threats through social engineering are the toughest security threats to mitigate because it cannot be countered solely with automated anti-malware software (Aloul, 2012c). A successful defense against social engineering malware attacks involves making users aware about the vectors of the attacks as well as effective avoidance measures (Kumaraguru et al., 2007; Labuschagne et al., 2011; Olusegun and Ithnin, 2013). A number of security systems aimed at improving user awareness have been previously suggested. Nonetheless, most existing systems are rather cumbersome, inconsistent and non-specific for the average OSN user. Also, existing security awareness systems are not deployed to be rapidly distributed from one user to another especially in an OSN context. Furthermore, there is an on-going debate that awareness is not sufficient to influence a change in user behaviour. For example, an addict of smoking may not simply quit by being aware of the health hazards of smoking. Other factors can be synthesised with threat awareness to further improve threat avoidance behaviour.

While threat awareness may be a precondition to help individuals change their behaviour it is not necessarily sufficient. Within the context of OSNs, innovative measures are needed to effectively design and deploy security awareness to motivate a threat avoidance behaviour (Prestaasen, 2011; Stephanou and Dagada, 2014; Tidwell, 2010). If security compliance is excessively complex or effortful, it would be ignored by OSN users. Hence, security practitioners need to ensure that their time and goodwill are not being squandered on security methods that are overly perplexing to use.

In a previous study, Liang and Xue (2010) developed the technology threat avoidance theory (TTAT) which suggests the determinants that affects Information Technology (IT) threat avoidance by computer users. TTAT posits that the perceived severity and susceptibility of a threat has a significant effect on their threat perceptions. In addition, TTAT suggest that the threat avoidance behaviour of computer users is influenced by their avoidance motivation. TTAT argues that users consider a safeguarding measure to avoid the threat based on the perceived effectiveness of the safeguard, the safeguard costs and the self-efficacy of using the safeguard. Self-efficacy is sometimes used interchangeably with self-efficacy; while self-efficacy refers to the belief in one's capacity to perform specific tasks; self-confidence refers

an individual's belief in his/her personal worth and the possibility of succeeding (Zimmerman, 2000). However closely related they seem, it is important to clarify that self-efficacy would be used within the context of this research to measure users personal belief on their capacity to perform specific OSN security-related tasks such as verifying legitimate URL links.

TTAT provides some insights on how general computer users may avoid IT threats based on the use of a technical safeguard measure (specifically anti-spyware software). However, there is evidence in the literature which shows that OSN users exhibit online behaviour that substantially varies from typical Internet users.

Hampton *et al.* (2011) argue that the typical internet user is more than twice as likely as non-internet users to feel that individuals can be trusted. They argue that Facebook users are more likely to be trusting and engage in using the platform multiple times per day; precisely 43% more likely than other internet users and more than three times as likely as non-internet users to feel that most people can be trusted. In addition, Fogg (2008) revealed an OSN phenomenon – Mass Interpersonal Persuasion (MIP) which suggests the components that influence the behaviour of OSN users. MIP is a unique attribute of OSNs which makes it possible for users to reach and influence millions of their direct and indirect connections (friends/followers and friends of friends) within the shortest possible time. MIP is focused on changing users' behaviour and not simply disseminating information to them. Success with MIP centres on persuasive experience, social distribution and a huge social graph. OSN users have a tendency to be persuaded by the online behaviour of their connections into taking certain actions (e.g. subscribing for a product or service).

In order to overcome the limitations of existing security systems designed for user awareness, this thesis extends TTAT to include MIP. TTAT-MIP has been proposed as a new threat avoidance model which suggests the factors needed to motivate OSN users to avoid malware threats (Ikhalia and Serrano, 2016). MIP comprises of; (1) Persuasive experience, (2) Automated Structure, (3) Social Distribution, (4) Rapid Cycle, (5) Huge Social Graph and (6) Measured Impact.

Persuasive experience is an experience designed to change attitudes and behaviours. Automated structure implies that the persuasive experience is structured by

technology. Social Distribution implies that the persuasive experience is shared from one friend to another. Rapid Cycle is the swiftness at which the persuasive experience can distributed from one friend to another. Huge Social Graph means that the persuasive experience can potentially reach millions of users connected through socially connected. Measured Impact implies that the influence of the persuasive experience is noticeable by users and creators. To effectively motivate the malware threat avoidance behaviour of OSN users, MIP poses enormous benefits to developers of persuasive applications. Consequently, it is important to investigate the extent at which OSN users' threat avoidance motivation could be influenced by their interpersonal connections which is the core of the MIP phenomenon.

The outcome of this research would provide organizations a proactive and tailored security-awareness tool to equip their employees on effective malware preventive measures. The significance of making employees aware on how to spot and prevent social network malware, ransomware, email spoofing, and other cybercriminal activities cannot be overestimated (Sohrabi Safa et al., 2016). It is important for an organization to have an idea of the limitless benefits which can arise from a well planned and executed security awareness tool.

In **section 1.3** the research aim and objectives are outlined.

1.3 Research Aim and Objectives

The aim of this research is to extend the technology threat avoidance model for OSN users.

To fulfil the aim of this study, the following research objectives were established.

1. To understand the characteristics and threats of OSNs to establish the research domain and scope.

2. To access the limitations of security awareness systems in the literature and formulate a conceptual framework for the development of security awareness for OSN users.

3. To evaluate and extend the technology threat avoidance theory (TTAT) by integrating mass interpersonal persuasion (MIP).

4. To validate the extended technology threat avoidance theory (TTAT-MIP).

5. To develop a Web-based Facebook video animation security awareness app (namely - Social Network Criminal (SNC)) based on the principles of TTAT-MIP.

6. To practically evaluate the effectiveness of TTAT-MIP through the SNC app.

1.4 Research Methodology

Design science research (DSR) methodology has been adopted to execute the overall research. It is occasionally termed "Improvement Research" and this description stresses the problem- solving/performance improving nature of the research activity (Vaishnavi and Kuechler, 2004). Propositions for a problem solution are normally drawn from existing theories relative to the problem domain. Thereafter the researcher attempts to implement an artefact according to the advocated solution.

To accomplish the objectives of this study, four phases were included into the research design and implementation process. These phases were used in two DSR iterations reported in this thesis. The phases are; (1) Problem awareness (2) Suggestion (3) Development; and (4) Evaluation.

In the first iteration, the problem awareness phase includes a literature review of social engineering, OSN characteristics and malware threat vectors. In the suggestion phase a systematic literature review was carried out on existing IT security awareness systems. The development phase includes the proposal for TTAT-MIP and the corresponding research hypothesis. The evaluation phase includes the validation of TTAT-MIP using questionnaire surveys and the data was analysed using structural equation modelling (SEM) statistical technique.

For the second iteration, the problem awareness was drawn from the results of the tested TTAT-MIP model. In the suggestion phase, a conceptual architecture was

formulated based on TTAT-MIP for the development of a Facebook video animation security awareness app (termed “Social Network Criminal” (SNC)). In the development phase, various software development tools were utilised for the development of SNC. While for the evaluation phase, techniques such as System Usability Scale (SUS), Lab experiments and Semi-structured interviews were employed for the evaluation of the SNC app.

1.5 Thesis Arrangement

Chapter 1: this presents the overview and background of the research. The need to improve the malware threat avoidance behaviour using TTAT-MIP is highlighted. Also, the research aim, objectives and methodology are elucidated. Afterwards, a well-detailed outline of the thesis arrangement is presented with a synopsis provided for each chapter.

Chapter 2: In this Chapter, the state of the art is explored. Firstly, social engineering issues are described and characteristics of OSNs are analysed. Next, a systematic literature review is conducted on existing information technology (IT) security systems/strategies designed for user awareness on malware threats. Thirdly, an overview of TTAT is presented with justifications for its extension to include MIP in order to further improve the malware threat avoidance behaviour of OSN users.

Chapter 3: this explains how design science research (DSR) was used for this thesis. The chapter begins with a background on the paradigms of information systems research and discusses the various phases of a design science research. Then, the research methods/techniques are justified. In addition, the Chapter discusses how the phases of DSR were implemented for the two iterations reported in this thesis to achieve the research aim.

Chapter 4: this presents the results from the data analysis of the questionnaire survey using structural equation modelling technique. Before the results were presented, the initial study hypothesis were discussed and justified. Afterwards, the structural equation modelling approach used was described. The chapter describes

the measurement and structural models, the hypothesis supported and not supported which led to the refinement of the final TTAT-MIP model.

Chapter 5: this chapter proposes the design and implementation of a Web-based Facebook animated video App to evaluate TTAT-MIP. The App called "Social Network Criminal (SNC)" is introduced and its features described. In addition, the architecture of SNC is explained relative to the elements of TTAT-MIP. The Chapter concludes with an evaluation plan for SNC using three techniques; System Usability Scale (SUS), Lab experiments and Semi-structured interviews.

Chapter 6: this chapter presents the empirical evaluation of SNC using three techniques; System Usability Scale (SUS), Lab experiments and Semi-structured interviews. First, the results are presented to elicit the preliminary validity of the alternative hypothesis and to find out if SNC needed a significant amount of improvement from a usability standpoint. Secondly, the results of the main studies were presented and explained. The statistical relevance of the results is discussed as well as its potential implications to theory and practice.

Chapter 7: presents an overall reflection of the results from the first and second DSR iterations respectively. The chapter discusses the reliability and validity of the overall results and its general implications.

Chapter 8: this presents the overall findings and contributions of the research. The chapter is divided into four key sections. The first section elucidates how the research objectives were accomplished. The second section describes the research contributions; the third section outlines the drawbacks of the overall research and the fourth section presents the concluding remarks and potential areas for further research

Chapter 2: Literature Review

2.1 Overview

This chapter explores the research domain – online social networks (OSNs). **Section 2.2** analyses the art of social engineering and the psychological segments that aids in understanding social engineering. **Section 2.3** explores the nature of online social networks, its characteristics and distinctive phenomenon – Mass Interpersonal Persuasion (MIP). In **Section 2.4**, the vectors of OSN malware threat and its distribution techniques were discussed using three real life cases. In addition, the analysis of peer-reviewed publications on malware attacks carried out through OSNs are presented and discussed. **Section 2.5** describes the concepts of security awareness, training and education; further, a systematic review of IT security systems including their potential limitations relative to OSN users is reported. **Section 2.6** explores the technology threat avoidance theory and justifies the need for its extension to include MIP. Finally, **Section 2.7** summarizes the key points of this Chapter.

2.2 The Art of Social Engineering

Social engineering is generally a malicious user's (commonly referred as attacker) cunning manipulation of the human susceptibility to be trustful, helpful, lazy and fearful (Gupta et al., 2017; Luo et al., 2011; Rößling and Müller, 2009). The key objective of an attacker is to illegally obtain information that allows unauthorised access to one or more systems. Through social engineering, an attacker can commit fraud, steal identities, invade a network, execute industrial espionage or simply disrupt a network system. Victims of social engineering (especially large business organisations) are usually reluctant to admit their vulnerability due to the reputational damage the disclosure of such attacks may create (Ferreira et al., 2015).

The adoption of social engineering by attackers is due to the ease of gaining illegal access to systems when compared to solely using technical methods. For example, it is easier to trick the IT admin of an organisation into giving away their password than carrying out a brute-force attack to get it (Gupta et al., 2017). The art of securing systems is relatively simple; it is the human being operating such systems that creates the biggest security challenge. Many security software solutions have been implemented for decades; nevertheless, the human factor is considered the biggest weakness within the social engineering ecosystem.

2.2.1 Psychology of Social Engineering

To understand the social engineering techniques used by attackers, three vital segments of social psychology will be highlighted in this section. They include; alternative persuasion routes; beliefs and attitudes that affect human interactions and persuasion and influence techniques.

- **Alternative Persuasion Routes**

The alternative persuasion route consists of direct and indirect routes. Using the direct routes, the attacker may simply request for information from the target. The attacker may use any available prospective approach to forge a fake relationship with the target. The most common approach used by attackers is preparing logical arguments that would stir the target to perform unintended activities. Furthermore, the indirect routes involve making the target perform illegal actions by making a provocative statement to trigger an emotion of fear or excitement (Mohammed and Apeh, 2016).

- **Beliefs and Attitudes That Affect Human Interactions**

Workman, (2007) argues that the emotional aspect of human interaction is often distracting and interferes with ability of a potential victim to carefully examine the message contents delivered by attackers. Attitudes and beliefs refer to the differences between the victim's attitude and beliefs about the attacker and the attacker's attitudes and beliefs about the potential victim. During a typical interaction within

an organisational setting, the attitudes and beliefs of employees when a service is requested is that parties are who they claim to be. In the context of a social engineering interaction, only potential victims act based on this belief.

- **Persuasion and Influence Techniques**

Persuasion and influence are deeply ingrained in social psychology. They depend on exterior paths to persuasion that are effective to influence the behaviour of others. Effective persuasion factors includes; scarcity, authority, similarity, liking, consistency, commitment, reciprocation and social proof (Schaab et al., 2017). Authority implies that people are highly likely to be responsive to the assertions of authority, notwithstanding the absence of the person who is in the position of authority. Scarcity implies that people are responsive to indications that a particular item on demand may be in short supply. Liking and similarity describes how people tend to like other persons alike, such as people with characteristics that are identical e.g. places of birth, tastes in sports, music, art and other personal interests. Reciprocation deals with a well-known social interaction rule that when a person gives something freely, the receiver is strongly inclined to return the gesture. Commitment and consistency describe how people tend to take certain actions that are consistent with previous actions taken in order to be considered trustworthy. Social proof deals with the reliance on people's opinion within vicinity before certain actions are taken. **Table 1** outlines the segments of psychology discussed and its corresponding elements.

Table 1: Segments of psychology and corresponding elements

Segments of Psychology	Elements
Alternative persuasion Routes	1. Forge relationship with potential victims 2. Manipulating potential victims to perform illegal actions
Beliefs and Attitudes that affect human interaction	1. Emotion-based interaction 2. Trust-based relationship
Persuasion and influence techniques	1. Authority 2. Scarcity 3. Liking and similarity 4. Reciprocation 5. Commitment and consistency 6. Social proof

The outlined elements of the segments of psychology in **Table 1** suggest that attackers often take advantage of the aforementioned elements to guarantee the success of social engineering attacks. Social engineering can be human-based or technology-based. Human-based social engineering refers to a person-to-person interaction (the attacker and the victim) to achieve an illegal objective. On the other hand, technology-based social engineering involves using an online interface to achieve the desired objective.

Social engineering normally starts with collecting contextual information on potential targets. The preliminary information is usually collected through dumpster diving (i.e. gathering information through company phone books, memos, company policy manuals, organizational charts, etc.) and phone calls. Moreover, the wide-range adoption and usage of online social networks (OSNs) have introduced new opportunities for attackers to execute their illegitimate/malicious actions (Ferreira et al., 2015; Gragg, 2001). Nowadays attackers can use OSNs such as Facebook to collect preliminary background information on potential victims. OSNs presents practicable chances for attackers to explore both human and technology-based social engineering to deploy malicious softwares (commonly referred as malware) designed to steal sensitive data from the systems of unsuspecting OSN users (Nelms et al., 2016; Sanzgiri, Joyce and Upadhyaya, 2012).

In section 3.3, the characteristics OSNs are discussed to understand why it has become the favourite platform attackers to deploy malware using social engineering.

2.3 Overview of Online Social Networks

Online social networks (OSNs) have totally changed the way people establish social relationships in the online world. Arguably, it has become the most popular online platform of building social connections (Diffley and Kearns, 2011; Lin and Lu, 2011a). The growth of OSNs has introduced huge benefits to society, together with the capability to reconnect with lost friends and family, as well as establishing new connections.

Often times the term social media and online social networks have been used interchangeably. While social media is defined as forms of electronic communication (e.g. Websites for social networking and micro-blogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos); online social networks (OSNs) deals with the creation and maintenance of personal and business relationships (Conole et al., 2008). Therefore, the ultimate goal of OSNs is to build a network of friends, fans/followers and foster those relationships. Such relationships often lead to new business opportunities for the entities involved. A study by the University of Maryland, Rice University, and Max Planck Institute for Software Systems analysed the characteristics of large OSNs. As shown in **Figure 1**, characteristics identified were; user-based, interactive, community-driven, relationships and emotion over content (Mislove et al., 2007). Moreover, Fogg (2008), identified a distinctive OSN phenomenon – Mass Interpersonal Persuasion (MIP) that was introduced during the launch of the Facebook platform. In sub-sections **2.3.1** and **2.3.2**, the attributes and distinctive phenomenon of OSNs are discussed.

Figure 1: Characteristics of OSNs

2.3.1 Characteristics of OSNs

- **OSNs are End-user Based**

Prior to the popularity of OSNs, Web applications were sustained on information updated by a single user and consumed by one or more users. Information flow was in a single direction, and the directions of prospective updates were controlled by the Web administrator, or content manager. On the other hand, OSNs are built and controlled by multiple end-users. Devoid of end-users, OSNs would be an empty space filled with no posts, groups, applications, and chat rooms. OSN end-users are responsible for the content creation and re-creation in form of texts, images and videos. The contexts of content created on OSNs are also defined by content creator, while the flow could be determined by participants who contribute to the thread. The end-user based attribute of OSNs makes it a dynamic and interesting platform for users to effectively express themselves without any hindrance (Conole et al., 2008; Mislove et al., 2007).

- **OSNs are Interactive**

Interactivity is an extremely important attribute of OSNs. The scope of interactivity on OSNs goes beyond the functionality to chat with friends and family or enlist specific groups/forums. Major OSN platforms such as Facebook are packed with network-based gaming applications that allow end-users to play games (e.g. poker, candy crush, criminal case) with their connections (commonly referred to as friends/followers) and also create friendly gaming tournaments. Such OSN platforms are fast becoming a pastime that more users now prefer over traditional media (e.g. Television and radio) due to the entertainment value and the functionality to share such experiences with their connections (Lin and Lu, 2011b).

- **OSNs are Community-driven**

OSNs flourish from community driven relationships. Similar to non-virtual communities or social groups that are developed on a collection of people holding common beliefs or hobbies; OSNs are based on the same concept. For example Facebook provides a feature for users to create “Group pages” were people who share commonalities, such as alumni of a particular school, or an animal welfare group,

fans of a music star or religious affiliation can collaborate, create and consume information. This feature makes it easier for users to discover new friends and also reconnect with old friends of the past (Zhang et al., 2016).

- **OSNs foster Relationships**

One of the motivations for the continued use of OSNs is communication. Users enjoy communicating with other users whom they have established relationships. OSNs thrive on relationships, the more relationships a user establishes the more enjoyable the platform seems. Facebook provides the feature for end-users to establish a direct relationship with up to 5000 people. In the non-virtual world, such possibilities are quite unlikely and somewhat non-feasible. When a user has 5000 direct connections, he/she can easily get an information proliferated to a wider audience within the network in a cost-effective manner (Diffley and Kearns, 2011; Dunlop et al., 2016).

- **Emotion over content**

An additional exceptional characteristic of online social networks is the emotional aspect. While previous traditional Web applications were focused primarily on providing information, the content shared on OSNs tends provide emotional security for users (Mislove et al., 2007). OSN provides users with the functionality to categorise their emotional states while sharing content on the platform. Users may decide to express their feelings of excitement, happiness, sadness using the tool illustrated in **Figure 2**. OSN users believe that regardless of their emotional states or circumstances they can get support from their friends and family through direct communication or encouraging comments on their posts.

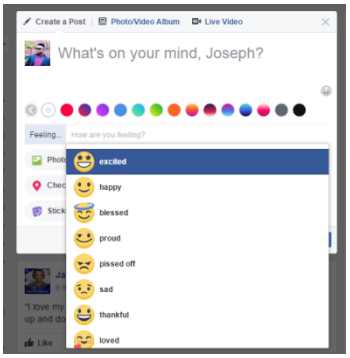

Figure 2: Categorising Emotional Content on OSNs

Table 2: OSN Characteristics with key points (Adapted from (Cheung et al., 2011; Conole et al., 2008; Mislove et al., 2007)**)**

Attributes of OSNs	Key Points
OSNs are End-user Based	OSNs present dynamic features for end-users to create, re-create and diffuse contextual content on their profile pages.
OSNs are Interactive	OSNs provide features for end-users to communicate with their friends and family. Facebook allows the integration of interactive third party applications (e.g. games).
OSNs are Community-driven	End-users who share common beliefs of hobbies can connect with each other through OSNs. (E.g. the Facebook user group).
OSNs foster Relationships	The rapid growth of OSNs relies on the number of relationships users establish with one another.
Emotion over content	Content created and diffused on OSNs are characteristically design to evoke human emotions such as anger, anxiety, fear and excitement.

The characteristics elucidated in this section shows how OSNs differ from other Web based platforms. Lately, some of these characteristics have been demonstrated by traditional Web based platforms particularly in the area of fostering relationships. Most business organisations are now adopting contextual forums to allow their clients ask questions and receive answers from each other. In addition, traditional Web apps now include product reviews sections to elicit feedback from clients to improve the quality of their products and services. However, a phenomenon known as – mass interpersonal persuasion (MIP) has been identified as the distinctive attribute of OSNs. In **Section 2.3.2**, MIP and its real world applications is discussed.

2.3.2 A Distinctive OSN Phenomenon: Mass Interpersonal Persuasion (MIP)

In this research, MIP is defined as the creation of persuasive experiences installed on a technological platform with a huge social graph and rapidly distributed between interconnected users with the aid of automated software codes. According to Fogg (2008), within a couple of days after the launch of Facebook Platform, metrics show how quickly some of the third-party applications grew through persuasion of interconnected users at rapid rate as never been seen before on Facebook. Although the six components of MIP; persuasive experience, automated structure, social distribution, rapid cycle, huge social graph and measured impact attempts to demystify MIP, Nevertheless, its success centres on persuasive experience, social distribution and a huge social graph (Fogg, 2008).

Through MIP, some Facebook app developers acquired thousands of users on a daily basis. Consequently, as they continued to leverage on MIP, Facebook experienced an exponential surge within 16 weeks of the Platform launch gaining 18 million new members. At the end of 2007, Facebook had well over 50 million users, doubling the 24 million they had in late May.

This suggests that OSN users demonstrate a subconscious attitude to partake on any trend their 'friends' and 'friends' of 'friends' are engaged with. Mass interpersonal persuasion is deterministic success factor of OSNs because it allows ordinary individuals the capability to reach and influence millions of people (direct and indirect connections). MIP is the biggest factor that influences users of online social networks to perform certain behaviours on a massive scale and it includes six components: persuasive experience, automated structure, social distribution, rapid cycle, huge social graph and measured impact.

- **Persuasive Experience:**

Fogg (2008) describes a persuasive experience as a plot to change behaviour with a lasting impact on OSN users. For example, a video with an emotional, controversial

and humorous effect is relatively a persuasive experience. A study by Chung and Han (2016), suggest that persuasive content has a positive impact on user engagement on OSNs. To create an effective user engagement on OSNs, informative content should be fused with a persuasive effect. OSN users are less likely to share a non-persuasive content with their connections. In the same way, attackers are using persuasive content to lure OSN users to perform unintended actions for malicious reasons. For example, when Osama bin Laden was apprehended in 2011, a malware script camouflaged as the video of the incident surfaced on Facebook only three hours after its announcement on mainstream media. Parallel attacks were executed after the 2011 earthquakes in Japan; as attackers succeeded in using persuasive content to lure unaware users of Facebook, Twitter, Google and LinkedIn to unintentionally download malware on their computing devices.

- **Automated Structure:**

After the creation of a persuasive experience, software codes are used to implement the experience in an automated manner. This automated method of deploying content on OSNs is relatively more efficient and scalable than non-virtual traditional techniques used by many business organisations (e.g. brochures, newspapers and magazines). The automation of a persuasive experience allows users the ease of access at their expediency. Again, attackers usually adopt an automated structured approach in the redistribution of their malware payloads.

The Facebook Zeus malware attack of 2014 began when malware was disguised as a spam link with a persuasive caption to check out a new video. When unaware users clicked the link, the malware infected their computer devices but remained in the background, monitoring their Web browser cookies for online banking activities. When users logged into a website on with their computing devices, the malware activated automatically and sent their login information to a C&C server of the attackers. The attackers remotely instructed the malware to steal bank account details and other sensitive information using automated and sophisticated software codes. Some varieties of the Zeus malware were able to create bogus versions legitimate bank websites as well as requesting personal data such as social security, credit card and customer numbers. The automated structure of the malware enabled its rapid re-distribution through the victims' infected Facebook profile to lure their

connections to download the malware on their computing devices, spreading the infection further.

- **Social Distribution:**

Popular OSN platform – Facebook, makes the social distribution of persuasive experiences relatively easy. For example, the process of delivery may start when OSN users receive a video on a particular topic through "Facebook Chat". If each user resends the video to one or more connected users through the "Facebook Chat" feature, the reiterative process has a huge likelihood of drawing the interest of the recipients. In addition, the "invitation feature" on Facebook, allows users to notify one or more of their connections about content integrated with the platform.

Practitioners promote persuasive experiences in MIP through social influence. Interpersonal influence theory and research postulate that people are usually inclined to conform to the expectations of others regarding purchase decisions (Bearden et al., 1989). Often, users demonstrate the tendency to learn about products and services by observing or seeking information from people they know and trust (Jin et al., 2013; Vladlena et al., 2015). Studies by Hutter et al (2013) suggest that online social influence does not only affect consumer perception a brand's quality but also their motivation to patronise such brand. Since OSNs are built on trust-based relationships, attackers also leverage on this component to propagate their malware.

- **Rapid Cycle:**

The time expended in sending invitation requests and accepting them within OSNs should be considerable trifling. MIP is in full effect when the time cycle needed to draw the interest of interconnected users towards persuasive experiences is shortest. This component is similar to the manner malware attacks are propagated through OSNs. Malware propagation through OSNs tends to follow a rapid cycle which makes it difficult to mitigate. Researchers revealed a Trojan that infected Facebook users on February 2015 (Cimpanu, 2016; Fischer et al., 2013); within 48 hours, the malware had infected the devices of an estimated 110,000 Facebook users'. The attack lured users into infection through an indecent video content containing a spam URL which

was also socially distributed through private chats to victims' friends, disseminating the infection even further.

- **Huge Social Graph:**

MIP can only occur on an OSN platform where millions of users are actively involved. Facebook has over 1.4 billion users, which makes it an excellent platform for MIP. Moreover, an OSN platform with an enormous social graph is a vital tool for viral content diffusion. Likewise, attackers find OSNs extremely attractive (particularly Facebook) due to the enormous amount of potential users that may fall for their malware ploys (Centola, 2010).

- **Measured Impact:**

Users need to observe the effects of using a persuasive-driven application integrated within a particular OSN platform. For example, OSN users need to see how many of their connections are using a particular app. On the other hand, the creators of the persuasive experiences need to see the number of new users added at specific time intervals as well as the number of end-user engagement. This component allows developers efficiently evaluate the impact of their persuasive experiences and gain intelligent analytics for better future improvements.

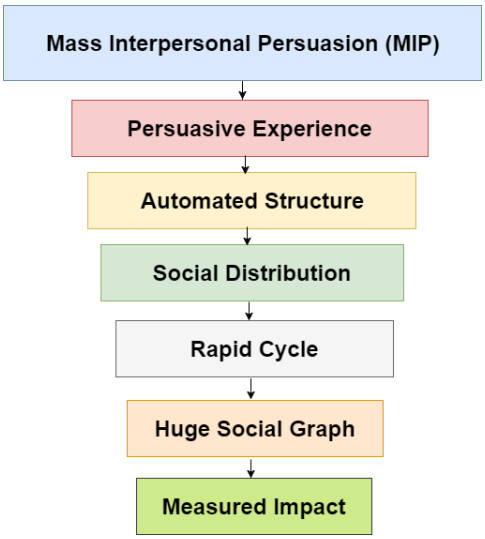

Figure 3: Components of Mass Interpersonal Persuasion

In **section 2.3.3**, the relationship between the psychology of social engineering and the characteristics of OSNs are explored in order to understand the success factors driving social engineering malware attacks on OSNs.

2.3.3 Social Engineering and OSN Characteristics

As previously discussed, social engineering thrives on trust-based relationships and the forgery of relationships between an attacker and potential victims in order to manipulate them to perform illegal actions. OSN grows on relationships built between users and very often this characteristic has been abused for malicious intentions. An attacker could steal the identity of a legitimate user that the target knows and then attempt to forge a relationship and gradually build trust. Such trust-based relationship can be used to trick the target into downloading malware on their computing devices.

Furthermore, social engineering thrives on persuasion and influence techniques which are relatable to some of the characteristics of OSNs. For example, 'Liking and similarity' explains how users are drawn to other users with whom they share some form of commonality. This is similar to the community-driven characteristic of OSNs. Because users have the high tendency to be connect with people of similar interests (e.g. football teams, vocation), there is the tendency to fall for a social engineering scheme. In addition, 'social proof', a persuasion and influence technique can be relatable to the 'social distribution' and 'rapid cycle' component of MIP. Both components explains how a user can somewhat persuade his/her connections to take certain actions in an iterative manner. For attackers to propagate their malware at a rapid rate they often adopt the 'Social proof' persuasion and influence technique and OSNs creates the setting for optimum impact.

Malware attacks through social engineering are not a new phenomenon, but OSNs has clearly created new opportunities for its seamless propagation. In section **2.4**, the vectors of malware attacks through OSN are explored with real world case studies.

2.4 Vectors of Malware Threats through OSNs

As shown in **Figure 4**, the vectors of social engineering malware attacks through OSNs are discussed in six groups: LikeJacking, Rogue applications, Private Chat, Twitter Bots and Spammed Posts, 'Friend' Connection (Faghani et al., 2012; Ikhalia and Arreymbi, 2014; Sood, 2011).

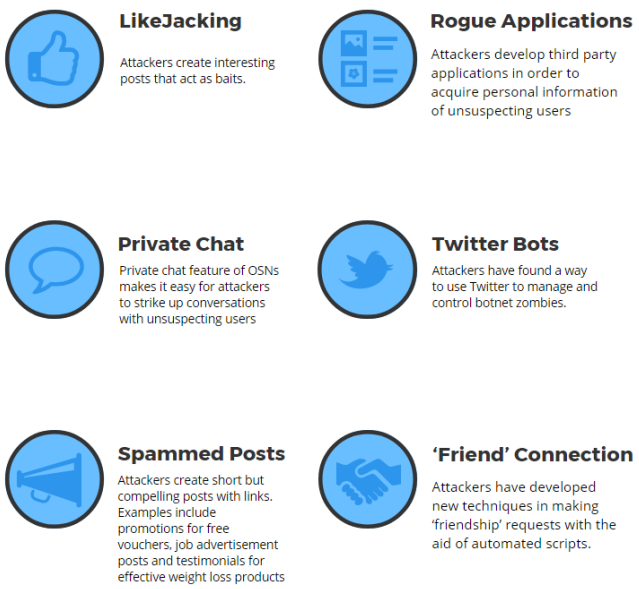

Figure 4: Malware Attack Vectors of OSNs

- **LikeJacking:**

LikeJacking is similar to a known Cyber-attack called ClickJacking[1]. The goal of this attack is to trick users into clicking items on a Website without their consent (Pawade et al., 2015). Attackers execute this LikeJacking attack by presenting a two layered Website. The backend layer of the site includes a Facebook "Like" button. The front-end layer shows the victim the lure designed for deception. Regardless of which object on the front-end layer that the victim decides to click, they are actually clicking the "Facebook like button" hidden in the back-end layer to further spread the

[1] ClickJacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on

spam. Moreover, users who click the links on the front-end layer unintentionally act as collaborators to the attacker because the malicious scripts would automatically re-posts the links, images or videos on their contacts' walls. LikeJacking has grown into a money making mechanism for attackers through affiliate marketing. Attackers get paid through affiliate marketing whenever a user views or clicks an ad on a given Website. With LikeJacking, the social network account of a victim can be remotely used to 'like' a post/page without his/her approval. OSN users need to be aware on how to defend against this form of attack in order prevent their online reputation from being blighted.

- **Rogue Applications:**

Facebook platform allows third party developers integrate their applications on Facebook for free. This feature for third-party applications is due the demand for more engaging features by end-users and the need to keep users engaged on the site. However, research suggests that a number of third party applications integrated with Facebook do not go through strict security screening or testing and thus raises doubts about their reliability (Rahman et al., 2016). Facebook makes it mandatory for users to allow third party applications access to their personal information before they install and use the applications. Due to the insufficient measures to audit third party applications by OSN platform providers, a huge gap is created for attackers to acquire the personal information of OSN users for malicious intentions (Gao et al., 2011). Moreover, studies show that some legitimate third party developers allow "fourth parties" the same access to users' personal information. In a recent study on the interaction between 997 Facebook applications and 'fourth parties'; the researchers found out that a staggering 22% of Facebook applications provide users' personal information to one or more fourth-party tracking entities illegitimately (e.g. trackers and advertisers) (Chaabane et al., 2014).

- **Facebook Chat:**

Facebook's built-in chat feature makes it easier for users and attackers alike to carry out conversations with friends and to communicate with their contacts in real time. Facebook chat system is an on-going mechanism for attackers to spread malware from one user to another (Moore and Clayton, 2015). Such attacks begin when a user receives a private chat message supposedly from their connections, the message may

simply be a JPG image. When an unsuspecting user clicks on such images, they automatically download an executable file that attempts to download further malware payloads[2] on their devices.

- **Twitter Robots (Bots):**

Attackers a have found a way to use Twitter in managing and controlling a network of robots or bots commonly referred as botnet. Users' devices that have been infected with a twitter worm such as the WORM_TWITBOT.A can be manipulated by the master-bot simply by the conveyance of commands through a Twitter account (Romera, 2010). Although Twitter is highly advantageous for the dissemination of news and global trends, malware attackers' have succeeded in turning many accounts into zombies via a command-and-control[3] (C&C) server (Antonakakis and Perdisci, 2012). At the time of putting this thesis together, studies show that twitter currently has 48 million bot accounts controlled by C&C servers. According to researchers at from the University of Southern California and Indiana University, up to 15 percent of Twitter accounts are robots and not humans.

- **Spam Link Posts:**

The most common vectors for social engineering malware attacks through OSNs is spam link posts. A typical malware infection starts with a spam sent through Facebook, Twitter or other social networking sites containing a catchy message with a link to a "video" (Baltazar et al., 2009; Micro, 2015; Thomas and Nicol, 2010; Zheng et al., 2015). Clicking the link will redirect the user to a website designed to mimic a spoofed version of YouTube or any other website. The user would be prompted to install an executable (.EXE) file or in some cases agree to share with 'friends' to be able to watch the video. The .EXE file is, nonetheless, a downloader of malware components. The downloader could be designed to report the cookies[4] of any website the victim normally visits to a C&C server that belongs to the attacker. Furthermore, the C&C server then controls the malware downloader into installing other components of malware such as CAPTCHA breakers, data stealers and Ads

[2] In computer security, the payload is the part of malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data
[3] Command and control servers (C&C servers) are computers that issue commands to members of a botnet.
[4] Cookies are small files which are stored on a user's computer. They are designed to hold a modest amount of data specific to a particular client and website

pushers. Such attacks are normally recursive in nature as the victim's device is used to re-post the spam links to their OSN connections for further malware propagation.

- **'Friend' Connection**

Prior to a 'friendship' connection between two users, social network providers e.g. Facebook, usually protect the privacy of users by default. However, the platform Facebook now allows the 'follower' type of connection, which implies that a user can have access to posts made by another user by becoming a follower. Using Facebook as an example, when two users become friends, the platform allows them to access the personal information uploaded on their profiles as well as other activity performed on profiles of their unique connections. Malicious users have developed new techniques in making 'friendship' requests with the aid of automated scripts (Yang et al., 2016). This mechanism easily allows for stealing personal information by 'befriending' enormous users. For example, 75,000 out of 250,000 random Facebook users sent 'friend requests' using automated scripts unknowingly accepted the bogus request.

Studies conducted by Bilge et al, (2009) demonstrated more sophisticated attacks. Firstly, the researchers identified same-site profile cloning, a process whereby an attacker duplicates a user's profile in the within the same OSN and then uses the 'duplicate' to establish 'friendship' connection to unaware connections of the victim. Secondly, cross-site profile cloning was also identified; a situation whereby the malicious users or attacker finds a user registered on social network A. Consequently, the attacker then replicates the profile to social network B, where the victim is not registered and establishes a 'friendship' connection targeted at the victim's already registered social network B.

In **section 2.4.1**, real-world cases of social engineering malware attacks through OSNs are described to understand the practical ways malware attack vectors are used exploit users vulnerability.

2.4.1 Cases of Malware Threats through OSNs

- **Case 1: Facebook Trojan Attack**

Cybersecurity researchers revealed a Trojan[5] that infected Facebook users on February 2015 (Cimpanu, 2016; Fischer et al., 2013). The attack lured users into infection through an indecent video content containing a spam link. Unaware users who clicked the link were able to get a preview of the indecent content, but the video stopped at the halfway point and persuaded users to download a supposed updated "Flash player" to view the entire content. The "Flash player" was actually a malware that enabled the attackers to control keyboard and mouse activities of the victims' devices. Once the malware was installed, it posted the spam link to the victim's Facebook page and notified his/her connections, which increased the chances of further proliferation. The malware sent private chats to victims' friends, spreading the infection even further.

Within 48 hours, the malware had infected the devices of an estimated 110,000 Facebook users'. After the attack, representatives of Facebook mentioned that the platform was executing several automated security technologies to identify and alleviate the damages of such spam links. Further, they reassured users that are links to such spoofed websites are being blocked, offering clean-up options and following extra measures to guarantee that users a safe online social networking experience.

Case 2: Syrian Rebels Lured Into Malware Honeypot Sites through "Sexy" Online Chats

Smith, (2016) reported that a group associated with the regime of the current Syrian President have gathered a wealth of intelligence on Syrian opposition groups. In the last two years, using a combination of fake social network and Skype accounts associated with imaginary female supporters of Syrian rebel groups, the group — seemingly operating from Lebanon, deceived opposition soldiers and their aid providers' to download malware to their devices and smartphones. The attackers succeeded in stealing personal information on their targets as well as battle plans

[5] Trojan is any malicious computer program which is used to hack into a computer by misleading users of its true intent.

and other intelligence information that probably have been used by the Syrian government's troops to counter the opposition.

Gallagher, (2015) also reported that the attack process began when an attacker pretended to be a woman working for a computer programming company. The attacker requested for a photo of the target and subsequently sent hers as well. Apparently the victim was too distracted in admiration of the photo to realise it contained cleverly concealed malware. The attackers created a number of Skype, Facebook, and other social network accounts around made-up identities, using profile photos of attractive women. In the course of Skype chats, the attackers would ask the targets whether they were using Skype with a computer or mobile device. Such information was used to choose which set of malware to offer.

In addition, the attackers offered a link to an installer for video chat software that contained malware. The profiles of the faked identities on Facebook comprised posts and links that were in support of the Syrian opposition. The process of misleading a single victim paid off several times over because the devices used by victims were frequently shared with other users owing to inadequate Internet connectivity for opposition groups. The attackers were able to steal numerous Skype databases off the same machine. Also, they identified other targets from contact lists and were able to compromise real-time communications in the field, providing them awareness into battlefield operations.

- **Case 3: Zeus Malware Re-Launched Against Facebook Users**

kaspersky, (2015) reported a Trojan horse malware – Zeus, initially discovered in 2007, re-emerged and attacked Facebook users in 2014. The Zeus malware was able to capture bank accounts and steal private information such as social security numbers using fake Facebook fan pages and compromised OSN accounts.

The attack began when the malware was disguised as a spam link with a persuasive caption to check out a new video. When unaware users clicked the link, the malware infected their computer devices but remained in the background, monitoring their Web browser cookies for online banking activities. When users logged into a website on your devices, the malware activated and sent their login information to a C&C server of the attackers.

The attackers remotely instructed the malware to steal the bank account and other sensitive information. Some varieties of the Zeus malware were able to create a bogus version of the bank's website and request user information such as social security, credit card and customer numbers.

Moreover, numerous Facebook accounts were stolen, and spam chats with malware links were sent to all the connections of victims'. The New York Times stated that the advocacy group, Fans Against Counterfeit Enterprise, also noticed links aiding the Zeus malware on bogus Facebook pages, particularly belonging to NFL fans. Such pages contained post links claiming to be football news, but were really designed to infect computers with Zeus. Experts argue that new versions of the Zeus malware have been designed to effectively attack Android phones. Nevertheless, Information security experts advocate that the best way for users to stay protected is to click links from only 'trusted' sources, as well as being skeptical of posts that persuades OSN users to click a link without having a custom personal message.

To further substantiate the cases of social engineering malware attacks through OSNs, as reported by news media, **section 2.4.2** highlights the findings from a review of 13 peer-reviewed publications on the technology implications OSN malware attacks.

2.4.2 Analyses of Malware Attacks through OSNs.

Table 3 shows the analysis of social engineering malware attacks from peer reviewed academic publications. The analysis includes the type of malware, its implication, the OSN platform exploited and the social engineering technique used. As seen in **Table 3**, the major malware variant used by attackers on OSNs is the Trojans. While the implications of most attacks includes transforming victims' computing device into zombies, identity theft, theft of personal information, distributed denial of service attacks (DDoS[6]), breach of private data and personality defamation. Also, the analysis show that Facebook is apparently the most exploited

[6] DDoS is a type of attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack

platform. Phishing[7], Spamming, Cross site scripting[8] and drive-by-downloads[9] are seen as the common social engineering techniques used by attackers.

Table 3: OSN social engineering malware attacks and its implications

Author/Year	Title	Malware	Implication	Platform	Attack Technique
Thomas and Nicol, (2010)	The Koobface Botnet and the Rise of Social Malware	Trojan	1. Turns victims computer to a zombie 2. Generates fraudulent accounts 3.Identity Theft	Facebook Twitter	Phishing
Faghani et al., (2012)	A Study of Trojan Propagation in Online Social Networks	Trojan	1. Turns infected machines to zombies 2. Identity Theft.	Facebook MySpace Twitter	Phishing
Robertson et al., (2010)	A Social Approach to Security: Using Social Networks to Help Detect Malicious Web Content	Trojan	1. Turns infected machines to zombies 2. Identity Theft	Facebook	Phishing
Algarni, (2013)	Social Engineering in Social Networking Sites: Phase-Based and Source-Based Models	Unknown	1. Theft of Personal Information 2. Identity Theft	Facebook	Phishing
Makridakis et al., (2010)	Understanding the Behaviour of Malicious Applications in Social Networks	Unknown	1. DDOS Attacks	Facebook	Phishing
Jin et al., (2013)	Understanding User Behaviour in Online Social Networks : A Survey	Unknown	1. Leakage of Private Data	Facebook	Sybil Phishing Spamming Cross-site Profile Cloning
Sood, (2011)	Chain Exploitation — Social Networks Malware	Trojan	1. Converts the victims system into a zombie 2. Tracks the user's Internet activity 3. Identity Theft	Facebook, Twitter, MySpace, Orkut and Friendster	Drive-by-Download Attacks
Yang et al., (2013)	Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers	Unknown	1. Identity Theft 2. Converts the victims system into a zombie	Twitter	Spamming
Altshuler et al., (2011)	Stealing Reality : When Criminals Become Data Scientists	Unknown	1, Theft of dyadic information 2. Theft of network-level information. 3. Theft of Personal Information	Facebook	Cross-Site Scripting
Abraham and Chengalur-Smith, (2010)	An overview of social engineering malware: Trends, tactics, and implications		1 Identity Theft 2. Victims are used for DDOS attacks	Facebook Twitter MySpace LinkedIn	Phishing

[7] The act of acquiring private or sensitive data from personal computers for use in fraudulent activities
[8] Cross site scripting enables attackers to inject client-side scripts into web pages viewed by other users
[9] Downloads which a computer user authorised but without understanding the consequences

Sanzgiri et al.,(2012)	The Early (tweeting) Bird Spreads the Worm: An Assessment of Twitter for Malware Propagation	Worm	1. Theft of Personal Information 2.	Twitter	Phishing
Boshmaf et al., (2012)	Design and analysis of a social botnet	Twitter-bots, Spam-bots Koobface	1 Theft of Personal Information 2. Identity Theft 3. Defamation of Personality	Facebook Twitter	Phishing
Gold, (2010)	Social engineering today: psychology, strategies and tricks	Trojan	1 Theft of Personal Information	All Social Networks	Phishing
Gao et al., (2011)	Security Issues in Online Social Networks	Trojan	1 Theft of Personal Information 2. Identity Theft	Facebook	Phishing Cross-Site Scripting
Luo, et al., (2009)	An Analysis of Security in Social Networks	Worm Trojan	1 Damages Network Availability 2. Theft of Personal Information	Facebook MySpace LinkedIn	Cross-Site Scripting Phishing Spamming

Points for Consideration

In **section 2.4.1** three cases of social engineering malware attacks through OSNs were described. Based on the real-world cases, four key elements of OSN malware attacks are deduced; (1) the malware ploy, (2) the attack vector (3) user interaction and users' computing device. The malware ploy describes the tricks used to persuade unaware users to unknowingly download malware on their devices. OSN malware ploys may include; fake news, trends, personal photos and videos, or any persuasive content that appeals to a particular target or a community of targets. The attack vector describes the medium through which malware ploys are being deployed to OSN users. With OSNs, attackers often exploit numerous mediums to deploy their malware ploys such as; posts, private chats, rogue applications, 'friend' connection, Twitter bots and LikeJacking.

Be that as it may, it is relatively impossible to control the creation of a malware ploy and the attack vector adopted, it is the user interaction with such ploys that determines whether the target's computing device would be infected or not. In the first real-world case, it is observed that Facebook representatives implemented automated security technologies as a reactive measure to cope with the malware attack (see **section 2.4.1**). One of the unsettling issues is; are there efficient preventive solutions to cope with OSN malware attacks? The rationality for this

question is emanates from reports on the Zeus malware (see **section 2.4.1**) which initially attacked users in 2007 and the re-emerged in 2014 to successfully attack OSN users.

Although anti-malware innovative solutions have been developed and implemented over the years it is quite apparent that more efforts should be put in to make OSN users aware on ways to avoid social engineering malware attacks instead of sole reliance on reactive software solutions. Many studies have proposed the need for security awareness, education and training as effective measures to mitigate social engineering malware attacks (Aloul, 2012c; Arachchilage and Love, 2014; Olusegun and Ithnin, 2013; Thomson and Solms, 1998). In **section 2.5**, a clear definition of awareness, education and training are presented in order to set a clear path for the direction of this thesis.

2.5 Security Awareness, Education and Training

- **Awareness**

The purpose of security awareness is largely to focus attention on security and compliance issues. Awareness expositions are intended to allow individuals to recognise IT[10] security threats and efficiently respond accordingly (Rezgui and Marks, 2008). An example of a topic for an awareness session is - malware protection. The subject can be addressed by describing what a malware is, their consequence, actions needed for users to protect their devices, and what recovery measures to implement should they become victims of a malware attack. Awareness connects people to the consequences of their actions, creating a shift in thinking that inspires behaviour change.

[10] In the context of this thesis, IT stands for Information technology

- **Training**

Training strives to produce relevant and needed security skills and competencies. The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues (Katsikas, 2000). The skills acquired during training are built upon the awareness foundation, in particular, upon the security basics and literacy material. Training is not concerned about future learning, nor does it consider ways to extend beyond the process taught. Rather, the objective of training is to achieve a specific objective in a consistent and repeatable manner.

- **Education**

Education incorporates all of the security skills and capabilities of the various functional subjects into a collective body of knowledge (Katsikas, 2000). It attempts to create IT security experts' proficient with unique ideas and measurable practical skills. An example of security education is a degree program at a University. In addition, some security enthusiasts take several courses to develop their professional skills in a particular discipline (e.g. the certified ethical hacker course - CEH); this is not education but training at best. Education is basically a method of extending professional ideas into advanced theoretical realms (Trustnetinc, 2011).

Points for Consideration

Based on the distinct objectives of security awareness, training and education coupled with the nature of the research domain – social engineering malware attacks through OSNs, this thesis focuses on improving the security behaviour of OSN users through security awareness. With this focus, **section 2.5.1** describes the recommended factors to consider when designing effective IT security awareness systems. In addition, results from findings of a systematic literature review on IT security awareness systems are presented in **Section 2.5.2**. The aim of the systematic literature review is to identify the strengths and limitations of existing systems relative to our research domain and the recommended guidelines for effective IT security awareness design.

2.5.1 Designing Effective IT Security Awareness Systems

This section discusses the factors that need to be considered when designing effective cyber-security awareness systems. From the theoretical and practical suggested factors for implementing an effective cyber-security security awareness program found from previous studies (Aloul, 2012a; Cone et al., 2007; Gao et al., 2011; Peltier, 2005; Shaw et al., 2009; Tsohou et al., 2008), five factors have been conceptually considered which are; end-user learning preference, time efficient, multi-media delivery mechanisms, non-technical means of communication, and contextual based approach.

- **End-User Learning Preference**

Peltier, (2005) argues that emphasis must be made on the content as well as the technique for delivering security awareness for different user groups within a technological setting. The needs of the end-user must be considered to aid the effectiveness of security awareness programs.

- **Time efficiency**

Tsohou et al., (2008) recommended time efficiency for developing security awareness programs for college students. However, most organisations place more emphasis on delivering gigantic curriculums about security awareness, which often takes hours to disseminate.

- **Multi-Media Mechanisms**

In today's technological setting, the role of multi-media in persuasive learning cannot be under-estimated. Previous research works have evaluated the significance of multi-media systems in persuading the interests of targeted end-users have clearly proved the use of this method over other conventional educational methods of learning (Shaw et al., 2009).

- **Non-technical Communications**

Rowe et al (2011), highlights that it is the role of information technology practitioners to ensure that users effectively and securely utilize systems through the design of usable user interface for providing security awareness. In addition, the authors supported the need to educate end-users on how to avoid malicious social engineering threats. One of the important issues raised by the authors is that cyber-security professionals do not necessarily need to educate end-users using technical security terminologies such as (cross-site scripting and man-in-the-middle attacks). These terminologies are best suited for system administrators. End-users only need to be aware of the characteristics of malicious threats using non-technical security terminologies.

- **Awareness That Addresses Threats Based on Context of Each Organisations' Context (Contextual)**

Abawajy (2014) examined the preference of computer users concerning the delivery techniques of cyber-security awareness. The findings of the study show that despite the buzz around game based security awareness; most users prefer the use of videos for cyber-security awareness. In addition, the research recommended that further investigation needs to be conducted regarding the effects of security awareness through videos for different organisational context. This is due to the fact that the videos created for the study were relatively generic and does not address the unique threats faced by different organisations and their technological settings.

According to (Abawajy, 2014), *"Although many of the concepts included in cyber security awareness training are universal, such training often must be tailored to address the policies and requirements of a particular organisation."*

The results from their empirical study on users' preference for cyber-security awareness delivery methods shows that out of 60 voluntary participants, the percentage of participants who preferred to get security awareness through games were 5%, 50% preferred videos, 33% preferred texts while 12% were undecided.

2.5.2 Existing IT Security Awareness Systems

This section presents findings from a systematic literature review on publications regarding IT security awareness systems published from 2005 to 2015. The rational for choosing this time-range is due to reports of the escalation of cyber-attacks experienced between these periods as well as concerns for security awareness. The analysis was conducted between November 2014 and February 2015.

- **Inclusion criteria**

The inclusion criteria used to select the publications analysed are;

1. The publication mentions cyber-security threats which are relatively similar to threats faced by online social network users. Some of the threats mentioned are not exclusive to OSNs, but their methods of execution are similar to OSNs

2. The publication explains the working process of the IT security systems developed for security awareness. This is important because in order to evaluate a security awareness program, the operational procedures must be known.

3. The targeted end-user group for which the security awareness systems were developed are clearly known. This is important because there are diverse groups of internet users with varying behaviour. It is important to ensure that the method of deploying an IT security awareness system is coherent with target users' behaviour to evaluate its potential effectiveness.

4. The publication must either be a journal or conference article.

The following databases where searched; IEEE/IET Digital Library, ScienceDirect, and Google Scholar. IEEE/IET is amongst the leading publishers of computer science and information systems research articles with top quality. This database was selected because it contains high quality technical literature in engineering and technology which have been published since 1998. ScienceDirect is amongst the trusted source for journal articles by millions of researchers with over 13million content pieces available. Google Scholar is considered as the 'database' of all other databases, Google Scholar, provides a comprehensive and scalable access to

conferences, journals, whitepapers, and books in academia and the industry. It often assists researchers in accessing papers from the originals source.

- **The Search Results**

Research on the development of IT security awareness systems is relatively emerging, hence, a broad search term was initially used; ‘cyber-security awareness programs’. Since cyber-security implies the collection of tools, technologies guidelines, risk management techniques and training that can be used to protect the assets of individuals and business organisations (Wamala, 2011). It was important to include the terms cyber-security, awareness and programs as it best describes the goal of the study and describes part of the definition of cyber-security.

The initial search using the search term 'cyber-security awareness programs' returned a total number of returned 13041 results (11,300 from Google Scholar, 1741 from ScienceDirect and 12 from IEEE). Four publications appeared in the three databases and the duplicates were deleted. Out of the 11,300 results from Google Scholar, 15 were selected for review and 12 were included.

From the 1,741 results found on ScienceDirect, 8 were selected for review and only 3 were included. 12 publications were found using the same search term on IEEE but none of them were found to be relevant. Therefore, the search term was modified to 'designing security awareness' which returned 386 results, from which 5 were reviewed and 4 were excluded based on the aforementioned inclusion criteria.

Similarly the search term 'designing security awareness' was used on Google Scholar and ScienceDirect databases which returned 64,300 and 7,212 results respectively. However, all the relevant results identified were previously found using the search term 'cyber-security awareness'. Therefore a total number of 16 articles were included for the systematic literature review.

2.5.3 Analysis

This section presents the analysis of the systematic literature review on existing cyber-security awareness systems. As shown **Table 4**, the publications were

evaluated based on the guidelines recommended for designing effective cyber-security awareness programs (See **section 2.5.1**). In Table 4, the letter Y denotes YES, i.e. the reviewed paper complied with one or more recommended guidelines, while the letter N denotes NO, i.e. there was no written evidence that one or any of the recommended guidelines were followed. The Limitations of the systems relative to OSN users and the recommended guidelines are discussed in **section 2.5.4.**

Table 4: The reviewed security awareness systems

Author	Program Developed	Objectives	End-user needs	Time efficiency	Multi-media mechanisms	Non-technical	Contextual	Method of Delivery	Evaluation	Findings
Kumaraguru et al (2007).	Embedded training email system	1. To teach people about phishing during their normal use of Email	N	N	N	N	N	1. Text and graphics 2. Comic strip format	Lab Experiments	1. Embed the training into users' regular activities .
Sheng, Steve MagnienBryant (2007)	Online game	1. Online game that teaches users good habits to help them avoid phishing attacks	N	N	N	N	N	Interactive game	Lab Experiments	Learning science principles to training materials can stimulate effective learning
Olusegun, OjIthnin, Nb (2013)	ISAT	Change the perceptions of people's thinking and reactions when it comes to information security issues	N	N	N	N	N	Mass e-mail, newsletter articles,	None	ISAT program does not address all the needs required by the users
Cone et al (2007)	Video game	To provide basic information awareness training programs for general computer users	N	N	Y	Y	Y	Video game	None	CyberCIEGE engages typical users in an engaging security adventure
Denning et al (2013)	Card Game	To increase people's awareness of computer security needs and challenges, so that they can be more informed technology builders and consumers	N	N	N	Y	N	Card Game	None	The graphic design, illustration, and production quality of the game seem to have a large effect at least on its initial reception.
Kritzing	E-Awareness	To make users	Y	N	N	N	N	E-Awareness	None	The model as

er, E. von Solms, S.H.(2010)	Model	understand the risks of using Internet, the importance of securing their personal information and the consequences if this is not done properly						Model		proposed is still very abstract.
Labuschagne et al (2011).	Interactive Game	To show the effectiveness of using a virtual tool in cyber awareness creation	Y	N	N	Y	N	Facebook game App	None	The overall objective of the project is to promote perception. To achieve this that hypertext and multimedia would be ideal.
Arachchilage, Nag Love, S Scott, Mj (2012)	Mobile game	This paper focused on a design that develops the conceptual knowledge that is necessary to combat phishing threats	N	Y	N	N	Y	Google App Inventor Emulator	Lab Experiments	Conceptual knowledge helps users avoid phishing attacks more robustly
Lehrfeld et al (2013)	Video creation tool	East Tennessee State need is a security Awareness program to decrease the number and severity of computer virus outbreaks across campus.	Y	Y	Y	Y	N	Videos	None	Over $30,000/year is spent directly on spyware removal in East Tennesse Univeristy This number does not take into consideration data lost or potentially exfiltrated.
Potgieter et al (2013)	Browser Plugins	To promote security values and provide security suggestions based on users behavioural pattern.	Y	N	N	N	Y	Texts	None	The innate knowledge provided by the browser can deliver targeted information security awareness content to the user on possible information security dangers.

2.5.4 Strength and Limitations of Existing Security Awareness Systems

The reviewed papers presented in **Table 4**, shows some commendable progress in the cyber-security awareness community towards the development of interactive and informational security awareness systems. Most of the studies reviewed made huge strides in delivering information security awareness using unconventional approaches such as comic strips, video games and app emulators. Such approaches have greater likelihood in drawing the attention of users when compared to other traditional methods e.g. email notifications and print media. Moreover, the reviewed studies suggest that a good amount of work have been done to educate users on the threats associated with phishing attacks. Phishing has been one of the foremost techniques used to gather sensitive information from unsuspecting users by manipulating fake websites to appear as legitimate ones (Hong, 2012; Wu et al., 2006). As seen in **Table 3**, phishing is a predominant technique used to lure victims during social engineering malware attacks and much work have been done to educate users in identifying fake websites and bogus applications.

Although OSN social engineering malware attacks are rapidly growing, the analyses in **Table 4** suggest a sluggish progress in research towards the development of security awareness systems tailored for specific end-users particularly that of OSN users. Previous studies have shown that employees behaviour have a significant effect on the intention to comply with IS security policies (Pahnila et al., 2007). Many existing security awareness systems do not consider the behaviour of users on the technology platform through which malware attacks occur. Effective security awareness systems must consider the desires of the intended users in order to communicate the security information in a more effective manner (Shaw et al., 2009; Tsohou et al., 2008).

Furnell, (2010) argues that the method through which security awareness are delivered could obfuscate the process in a way that makes it difficult for users to access the information needed to avoid malware attacks. Many existing security awareness systems are designed to overwhelm users with extensive monumental training, without carefully considering how to effectively deliver security awareness

to distinct user groups. For example, the security awareness program developed for a business organisation by (Kumaraguru et al, 2007) utilised texts and comic strips to implement an embedded email security awareness system for employees. The researchers, did not consider how best to tailor the delivery of security awareness to employees in a manner that could be more appealing and persuasive.

Due to these limitations, organisations are spending a huge amount of time teaching people generic technical security topics and worst of all delivering such information in a non-persuasive manner. Moreover, security awareness systems for OSN users need to be on an automated incessant life-cycle to keep users continuously updated and consequently influence a behaviour change.

In **section 2.5.5**, this research proposes a conceptual framework for designing security awareness systems for OSN users by taking into account the behaviour of OSN users (See **section 2.3.1**) and the recommended guidelines for IT security awareness design (See **section 2.5.1**).

2.5.5 A Framework for Designing Security Awareness Systems for OSN Users

In this section the proposed framework for designing security awareness systems for OSN users is discussed. The five key components of the framework are; Timeboxing, End-User Engagement, Platform Integration, Activity-Specific and Knowledge Testing.

- **Timeboxing**

In the context of software development, Timeboxing refers to the process of placing strict time limits around an activity (Jalote et al., 2004). For example, when creating a video for security awareness, developers need to place strict time boundaries on the time stretch of the video to avoid information overload. Zhang et al (2016) conducted a study to investigate the factors that influence social network fatigue, dissatisfaction and intention to discontinue usage by OSN users. Their findings show that information overload has a significant impact on social network fatigue, dissatisfaction and discontinuous usage intention Kim, (2014), recommended time

efficiency for developing security awareness programs for college students to sustain their attention span. Also, time boxing helps to avoid a common challenge in system design and development known as “feature creep” (Elliott, 2008). “Feature creep” arises when developers incrementally add features to a system without scrutinising its relevance. Feature creep results in wasted effort in both the development and maintenance of systems.

- **End-User Engagement**

Designing an engaging security awareness system for OSN users involves two aspects; (1) related content; and (2) interactivity. Diffley & Kearns (2011) argue that delivering relevant information is a key factor in engaging OSN users. Security awareness information must appeal to users’ needs. For example, a good technique to keep users’ engaged on security awareness information is to present contextual topics on stories that have made the news. The analysis of previous cases reported on the news about malware attacks has a tremendous potential to engage users due to relatable elements with the OSN activities of users.

Furthermore, an OSN security awareness system should allow users some form of control and functionality to persuade and engage their connections recursively. For example, a security awareness video-based web application that provides the functionality for users to choose their preferred video and share the content with their connections may be a possible technique for achieving this. There is empirical evidence in the literature showing that the key motivation for the continued use of OSNs is enjoyment derived from interpersonal relationships (Lin and Lu, 2011a). An engaging OSN security awareness system should be designed to incorporate such principle.

- **Integration**

According to a report, Americans aged 18-64 who use social networks confirm that they spend an average of 3.2 hours per day on the platform (Kietzmann et al., 2011). Due to the enormous amount of time devoted to OSNs daily, practitioners need to consider integrating their security awareness strategies within OSN platforms. Facebook, for example, allows the integration of third party applications for the purpose of creating an enjoyable and valuable experience for users (Wang et al.,

2011). Such an enormous opportunity for platform integration suggests an efficient delivery technique for security awareness systems, especially for OSN users.

- **Activity-Specific**

There are threat-related activities on OSNs that makes users vulnerable to malware attacks (Braun & Esswein 2012). As previously mentioned, accepting a counterfeit 'Friend Request' on Facebook could lead to a breach of privacy for an unaware user. Likewise, playing a bogus game on Facebook could result in attackers gaining unauthorised access to users' sensitive information (e.g. email and passwords). An effective security awareness system for OSN users' should address each of these the specific activities and how attackers can exploit them. For example, a video system on Facebook may provide security information on the best ways users can securely click links, play games, send and receive private messages as well as accepting 'Friend Requests' without compromising their online safety. Activity-Specific security awareness information necessarily means presenting users information relative to a specific risk-related social network activity - one instance at a time Ikhalia and Serrano (2015).

- **Knowledge Testing**

An effective security awareness system should allow practitioners measure the effect of the scheme on users (Kim, 2014). Such measurements would enable them to improve upon the information content of the system and strengthen its effectiveness. Moreover, knowledge testing should not only be conducted in a classroom setting or with survey questionnaires as adopted by many organisations on a one-time or once-in-a-week basis. Knowledge testing should be integrated to work automatically and recurrently with a security awareness system to estimate consistent and real-time insights on user behaviour.

Points for Consideration

The ultimate goal of a security awareness system is to improve the malware threat avoidance behaviour of users. An organisation may have advanced cyber security software in place, but if one employee falls for a well-crafted malware ploy on OSNs or becomes ensnared in an elaborate online trap, then even these defences may

become ineffective. Organisations have to refocus their security efforts on improving safety behaviour, not just security algorithms and firewalls (Ng et al., 2009).

A few theories attempt to predict the factors that influence human behaviour. Amongst them are; Theory of Planned Behaviour (TPB) (Sniehotta et al., 2014), the Technology Acceptance Model (TAM) (Legris et al., 2003), and the Technology Threats Avoidance Theory (TTAT) (Liang and Xue, 2010). TPB attempts to explicate all behaviours over which people have the ability to use self-control. It postulates that behavioural intents are influenced by the attitude about the probability that the behaviour would have the expected outcome and the subjective evaluation of the risks and outcome benefits.

TAM attempts to predict the acceptability of a tool as well as identifying the modifications which must be brought to the system to make it acceptable to users. On the other hand, TTAT suggests the determinants that affect IT threats avoidance behaviour of computer users which includes; perceived susceptibility, perceived severity, perceived threat, safeguard effectiveness, safeguard cost and self-efficacy. TTAT seems better suited with the objective of this study, which seeks to improve the security behaviour of OSN users. It would be interesting to explore the principles of TTAT and evaluate its suitability to predict the determinants that may help OSN users avoid social engineering malware attacks.

In section **2.6**, the TTAT model is discussed as well as potential limitations for its application within the context of this research domain. In addition, a debate on the need to include MIP (see section **2.3.2**) as a determinant for OSN users' threat avoidance behaviour within the TTAT model is presented.

2.6 The Technology Threat Avoidance Theory (TTAT)

The fundamental principle of TTAT suggests that when computer users perceive a malware threat, they are motivated to use a safeguarding measure to avoid it as long as they recognize that it would be effective when using it. In the process of preventing malware threats by users of computer systems, Liang and Xue (2010) proposed a set of the main factors that demonstrates the perceptions, motivations, and behaviour of

users. According to TTAT, users' malware threat perceptions are affected by the perceived likelihood of the threat's occurrence as well as the perceived severity of its adverse impact. By drawing from previous studies on health protective behaviour, TTAT suggest that there are three main factors considered by computer users when evaluating the degree of avoidance of a malware threat: the effectiveness of the safeguard, the self-confidence in applying the safeguard and the costs of using the safeguard.

To empirically validate TTAT, Liang and Xue (2010) conducted a questionnaire survey with 152 college students within the business department. Their findings suggest that perceived threat and safeguard effectiveness have a negative interactive effect on the motivation for IT threat avoidance. They argue the existence of a correlation between an increase in users' perception of malware and a decrease in the relationship between safeguard effectiveness and avoidance motivation. Also, their findings suggest that an increase in users' perception of a safeguarding measure is correlated with a decrease in the relationship between perceived threat and avoidance motivation. In their study, spyware was used as the IT threat and anti-spyware software as the safeguarding measure. While these measures are theoretically valid, they recommended that further studies could be carried out to validate the TTAT using a security awareness system as a safeguarding measure.

2.6.1 Limitations of TTAT

The findings of Liang and Xue (2010) could have produced more improved information on the IT security behaviour of computer users if the narrative of their study focused on the use of a particular computing platform (e.g. online social networks, online banking, e-government portal and aviation industries). For example, the core computing practices and behaviours' of traffic air controllers would be entirely different from that of online social media marketers. Previous studies argue that the degree of malware threat varies based on the type of technology platform (Bada, 2014; Braun and Esswein, 2012; Faghani and Saidi, 2009a; Szewczyk and Murray, 2008). Using general computer users to explain the

security behaviours of IT users are less likely to provide contracted insights to understand the behaviour of diverse computer user groups. Various user groups utilise specific technological platforms more than others and thus, may encounter wide-ranging forms and delivery techniques of malware (Albesher, 2017; Beye et al., 2010; Rosenstock IM, Strecher VJ, 1988; Rößling and Müller, 2009; Schaab et al., 2017).

Besides, a study conducted by Hampton et al (2011) found that the typical Internet user is more than twice as likely as others to feel that people can be trusted. The research found that Facebook users are even more liable to be trusting and engage in using the platform multiple times per day; precisely 43% more likely than other internet users and more than three times as likely as non-internet users to feel that most people can be trusted. OSNs social engineering malware attacks are mainly successful because its characteristics are ingrained with the segments of psychology in social engineering which the TTAT model does not address.

Consequently, adopting TTAT to examine the threat avoidance behaviour of OSN users must include a construct that embodies a characteristic element of OSNs. The process of making OSN users improve their security behaviour extends beyond dissemination of security information; emphasis should focus on the persuasiveness of the information and how such information can be rapidly shared from users to their connections recursively. Based on this premise, the inclusion of MIP as a determinant factor to improve the security behaviour of OSN users in a persuasive manner is proposed. **Section 2.6.2** presents a further justification for the inclusion of MIP within the TTAT model by elucidating the potential benefit of a MIP driven security awareness system (TTAT-MIP).

2.6.2 The Inclusion of Mass Interpersonal Persuasion to TTAT (TTAT-MIP)

Retrospectively, MIP is the biggest factor that influences the behaviour of OSN users on a massive scale. One of the important keywords within this research is behavioural influence and suggestively MIP embodies this keyword. Theories such as

the social influence theory argue that individuals in a social network are influenced by the behaviour of others to imitate the behaviour pattern within the network (Chia-Ying, 2013). There are variations to this type of influence – informational and normative. Informational social influence is accepting information from another; on the other hand, normative social influence describes the influence to adapt to the expectations of another individual as well as a group of individuals. Furthermore, users under normative influence are inclined to adapt to a greater level of social pressures to behaviour to carry out or not to carry out behaviour notwithstanding their attitudes or personal beliefs relative to the behaviour (Chia-Ying, 2013). Arguably, MIP exemplifies these two variations of social influence as it supports the design of a persuasive security awareness system as well as the techniques for social distribution from one user to another.

This research attempts to further justify the inclusion of MIP within the TTAT model, by elucidating how some of its six components; are related to some of the five key elements of the framework for designing a security system for OSN users. Also, the possible benefits of their interrelationship with MIP components are highlighted.

The framework proposed for designing a security awareness system for OSN users mainly deals with structuring the content of the information security system. One the other hand, MIP focuses on the delivery of the content from one OSN user to another in a recursive manner. The first point to state is that the Integration of a security awareness system within the OSN platform that malware ploys are carried out could make the process of gaining security awareness convenient and fast for OSN users. The social distribution and rapid cycle component of MIP optimise such convenience and speed.

"Activity-Specific" as an element for designing security awareness suggests that certain OSN activities could make users vulnerable to malware attacks; therefore, an effective security awareness system should be designed to make users aware of their social networking activity related threats one instance at a time. This research proposes the design of a Facebook animated video application that would consist of several animated videos, each addressing one threat-related activity. The MIP component "persuasive experience" could optimise this process by conveying such activity-specific information in an emotional and humorous manner. Such a

combination may have a tremendous potential in engaging OSN users and making the process of security awareness enjoyable.

In the context of our study, MIP deals with the motivation of OSN users to share their persuasive experiences with their interpersonal connections. The current research considers this feature an extremely vital significance of MIP within TTAT because the success of MIP can be predicted by a large social graph as well as the rapid social distribution regardless of the efforts put into the system design. If OSN users may not be influenced by their interpersonal connections to improve their security awareness, and consequently avoid a malware threat, then a MIP effect would not occur. However, interpersonal influence theory postulates that individuals are usually inclined to conform to the expectations of others regarding purchase decisions (Bearden et al., 1989). Often users demonstrate the tendency to learn about products and services by observing or seeking information from others. Moreover, study suggest that online social influence does not only affect consumer perception of quality of a sports brand but also their buying intention (Bullee et al., 2015; Hutter et al., 2013). In this regard, it would be interesting to study the effect of MIP on the motivation of OSN users to avoid malware threats when they are influenced to do so by their interpersonal connections.

MIP has real world applications, Foster et al (2009) carried out a study focused on determining peoples' attitudes on domestic electricity usage. Through a Facebook application termed 'Watts Up', they presented visualisations of users' electricity consumption as well as that of their interpersonal connections; consequently leading to reduced energy consumption by users of the application.
Furthermore, due to the "Measured Impact" component of MIP, it would be feasible for users to observe the security awareness levels of their connections and likely induce a competitive spirit. Security practitioners may see the improvement in the awareness of users on a daily, weekly, monthly and yearly basis. The "Knowledge Testing" component of the proposed security awareness framework may provide data to measure the impact of the persuasive experience.

Points for Consideration

MIP presents a novel technique for delivering a well-designed security awareness system by leveraging on the interpersonal connections that exists on OSNs. This is a significant approach to consider because the speed of malware propagation through OSNs centres on the unawareness of users; as a result, users have now unknowingly become counterparts of the attackers on a rapid level as never seen before the emergence of OSNs.

By combining MIP with TTAT (TTAT-MIP), there is a huge prospect of improving the threat avoidance behaviour (or security behaviour) of OSN users significantly and massively within the shortest possible time.

2.7 Summary

This chapter explained the art of social engineering through three segments of psychology - alternative persuasion routes, beliefs and attitudes that affect human interactions and persuasion & influence techniques. Through these psychology segments, it becomes relatively clear why attackers opt for social engineering for the success of their malicious intentions. The characteristics of the research domain – OSNs – end-user based, interactive, community-driven, foster relationships and emotion over content were discussed. In addition, this Chapter explored a unique phenomenon of OSNs – Mass Interpersonal Persuasion (MIP) which includes the following elements; Persuasive Experience, Automated Structure, Social Distribution, Rapid Cycle, Huge Social Graph and Measured Impact. Thereafter, the relationship between the OSN characteristics and the psychology segments of social engineering was used to describe why OSNs have become biggest platform for malware attacks.

Moreover, in describing the vectors of malware attacks, issues such as LikeJacking, Rogue Applications, Facebook Chat, Twitter Bots, Spam Link Posts and ‘’Friend’

Connection suggest that most OSN activities could be exploited by attackers, making it a huge security challenge for users. Using 3 reported cases; the current research describes how OSNs malware attacks are executed and established an attack process flow which includes; the malware ploy, the attack vector, user interaction and users' computing device. Furthermore, by exploring the concepts of security awareness, training and education, the development of effective security awareness is highly recommended as a path to consider in this research. As a result, a systematic literature review was conducted on IT security awareness systems. The review produced a conceptual framework for designing security awareness systems for OSN users. Nevertheless, since our goal was to provide an OSN security awareness to improve users' malware threat avoidance behaviour, the extension of the Technology Threat Avoidance Theory to include MIP (TTAT-MIP) is established as the scope of this research. In the next Chapter, the research hypothesis and results of the empirical validation of TTAT-MIP are presented as part of the first DSR iteration.

Chapter 3: Research Design

3.1 Overview

This Chapter explains the research design process followed to develop an effective malware threat avoidance model for OSN users. A comprehensive description of the research methodology and methods used in designing and testing the proposed TTAT-MIP model is provided. The Design Science Research (DSR) paradigm is implemented in this research as the overarching research framework. Also, this Chapter presents the rational for the selected research methods/techniques and tools.

This Chapter is organised accordingly: **Section 3.2** highlights the DSR paradigm in Information Systems (IS) research. It provides the outline of the development research phases that characterise these paradigms. **Section 3.3** justifies the

methods/techniques used to accomplish the research aim. The methods used includes: structural equation modelling (SEM), paired samples t-tests, system usability scale (SUS) and semi-structured interviews. **Section 3.4** illustrates the application of DSR to this study along with the three research phases. The Chapter concludes by summarising the main areas of the research design.

3.2 Research Paradigms in IS

As with other disciplines, a multidisciplinary paradigm such as information systems consists of various research approaches, paradigms, techniques, methodologies and methods used for the systematic production and validation of knowledge (Baskerville and Myers, 2002). To avoid conflicting interpretations of specific terms such as; paradigm, methodology, technique and method, the next section seeks to clarify how these terms are defined within the context of this research.

3.2.1 Defining Paradigm, Methodology and Techniques

In IS research, paradigm is defined as the fundamental philosophical assumptions which guide the activities carried out all through the research process (Mingers, 2001). There are two paradigms which characterises much of the research in the IS discipline: behavioural science and design science. The behavioural science paradigm seeks to develop and substantiate theories that predict human or organisational behaviour. The design science paradigm seeks to extend the boundaries of human and organisational capabilities by creating new and innovative artefacts. Both paradigms are complimentary and form the foundation of the IS discipline (Hevner et al., 2004).

Research methodology consists of the procedures adopted to carry out a research. It includes elements such as research phases, activities, methods, techniques and tools. Often, misunderstandings arise between the terms methodology and methods. Mingers (2001) provided insights on the three meanings of the term methodology,

which are; (1) the study of methods, (2) specifically describes the methodology of a particular research, (3) the generalisation of a particular research study. Such generalisation consists of all the principles used in a specific area of study. In this thesis, the term methodology describes the procedures adopted to undertake the research.

Often used synonymously, methods or techniques are used to perform activities within the different processes of a methodology. According to Mingers (2001), methods a sequence of operations that produces predictable results when executed adequately.

In this research, mixed methods were used for the purpose of strengthening the value and significance of the results. For example, this research used structural equation modelling (SEM) and semi-structured interviews to understand the factors that influences the malware threat avoidance behaviour of OSN users. Also this research adopts ideas from the design science research paradigms discussed in the following sections.

3.2.2 The Design Science Research Paradigm

Design science research (DSR) is described by March and Smith (1995) as an effort to produce solutions (models, frameworks, artefacts) that help human resolves. DSR is technology-oriented and its results are evaluated against standards of value or usefulness. While other Information systems research paradigms are focused on developing theoretical knowledge, researchers adopting the principles and practices of design science try to produce and apply knowledge on tasks targeted at developing innovative artefacts.

Vaishnavi and Kuechler, (2004), argue that DSR is different from other paradigms as it entails the creation and communication of knowledge gained all through the design process. Characterised by the reconstruction of artefacts iteratively, DSR accepts that knowledge arises in the process of iterations. In this research, two iterations were carried out using the phases of DSR and they are discussed in section **3.3** of this

Chapter. Arguably, DSR could be termed as a learning curve through which knowledge is enhanced from iterations, which further assists in improving the quality of the artefacts.

3.2.3 Design Science Research Processes

According to Vaishnavi and Kuechler (2004), DSR processes are structured into phases which include: awareness of problem; suggestion; development; evaluation and conclusion. The phases are elucidated below.

Problem Awareness:

At the start of DSR is the problem awareness phase where the researcher adopts a wide range of sources in the literature to clearly identify and define the research problem. In addition, this phase involves establishing research scope leading to the stimulation of new research.

Suggestion:

In the suggestion phase, possible solutions are explored and evaluated. Also more insights are gained on the research problem during the analysis and design of this phase. The outcome of this phase is a conceptual design of the proposed solution.

Development:

In the development phase the artefacts are developed based on the solutions recommended in the previous phase. The artefacts identified in this phase makes up the principal outcome of the overall DSR process. There are four categories of artefacts derivable from a design science research; constructs, models, methods and instantiations. Constructs are concepts normally used to characterise a phenomena of interest such as security in online social networks. Additionally, the combination of constructs in an orderly form can be used to explain tasks, situations or artefacts often termed as models. To perform goal oriented tasks, design scientists develop

methods or techniques and then instantiated in innovative products intended to perform certain tasks.

Evaluation:

In the evaluation phase, the developed artefacts are then analysed and evaluated. The evaluation is normally done against the recommendations that were predefined in the suggestion phase. Supposing the outcomes of the development or evaluation phases are not suitable the design cycle is repeated from the first phase combined with new findings gained from the previous phases. The key performance indicators are the output of the phases intended to enhance the effectiveness and reliability of the artefacts.

Conclusion:

The DSR cycle is concluded in this phase. The outcomes of the overall DSR phases as well as their implication to theory and practice are disseminated to the general public. Moreover, distinct findings from each DSR phase can also be applied by practitioners when implementing the artefacts in other similar contexts.

3.3 Research Methods and Techniques

3.3.1 Quantitative and Qualitative Methods

The research employed diverse techniques/methods (quantitative and qualitative) due to the multidisciplinary nature of IS. The three main methods used were: Surveys, Lab experiments and Semi-structured interviews. Studies carried out using quantitative methods produces results that are analysed statistically. With quantitative data analysis, produces results are founded on numbers; researchers usually gather data through questionnaire surveys and experiments. Besides, quantitative studies are often adopted by positivist researchers (Kaplan and Duchon, 1988).

On the other hand, studies carried out using qualitative studies are not usually based on numbers. The data sources for such studies are usually interviews, case studies and observations. Researchers who aim to explain social behaviour of individuals or groups often adopt qualitative studies (Myers, 1997). Qualitative data are mainly analysed by critical and interpretive researchers. The mixture of quantitative and qualitative data further enriched the overall outcome of this research (Creswell, 2007).

3.3.2 The Research Methods and the Research Aim

In the first DSR iteration, a quantitative data gathering method was adopted while both quantitative and qualitative methods were used for the second iteration. The aim of the first iteration was to develop a malware threat avoidance model for OSN users. A quantitative method was chosen to achieve this aim because it provided the flexibility to represent a broader population of OSN users. Also, the first iteration aimed at finding out the factors that should be considered to motivate OSN users to avoid malware threats. Hence, the researcher took a positivist stance due to the survey-driven hypothesis derived from the initial research model (Details of the hypothesis are discussed in **section 4.3**).

The aim of the second iteration was to evaluate the malware threat avoidance model through a web –based Facebook video animation app termed "Social Network Criminal" (SNC). In the second iteration, a pre- and post-test experiment was undertaken to measure the effect of SNC on the threat avoidance behaviour of OSN users. This was followed by a usability study to measure the subjective satisfaction of OSN users about SNC. Afterwards, a qualitative method was used through semi-structured interviews to gain further insights on how SNC had impacted OSN users. The second iteration takes both a positivist and interpretive philosophical stance due to the mixed methods adopted (quantitative and qualitative).

3.3.3 Lab Experiments

As earlier mentioned, the second study employed experiments to measure the impact of SNC on the malware threat avoidance behaviour of OSN users. There are two kinds of experiments: Laboratory and Field experiments (Oates, 2006). Laboratory experiments are usually controlled; this implies it could involve the participant's using specific hardware and software systems. One of the key advantages of laboratory experiments is that by controlling the variables, the researcher can adequately measure the cause and effect of a particular system (Oates, 2006).

According to (Coolican, 2004), field experiments are challenged by the issues such as; extraneous variables; the problematic nature of replicating the experiment; ethical challenges and accurate recording of data. The ethical challenges of conducting field experiments raised a cause for concern in this research especially putting with regards to the sensitive information participants are required to share before using SNC. Many participants might be unwilling to disclose such informative in a real world setting without the physical presence of the researcher reassuring them of the safety of their data.

On the other hand, laboratory experiments are somewhat secluded from distractions and enhanced with software and hardware infrastructure that enables a succinct and seamless data collection process. Previous studies have reported on the security behaviour of individuals using laboratory experiments. Egelman et al., (2008) carried out a laboratory experiment that required participants to purchase products from eBay and then they were sent fake malicious "eBay" emails. Dhamija et al., (2006) embarked on a laboratory experiment with twenty two participants' to investigate the reasons why people are vulnerable to phishing attacks. It is important therefore, to adopt laboratory experiments as a useful technique in investigating cyber security related issues that deal with human vulnerability. In the next section, the data gathering techniques are described.

3.3.4 Survey Questionnaire

Questionnaires are efficient data gathering methods in conducting a scientific research (Zaharias and Poylymenakou, 2009). Questionnaires are widely accepted

and used to identify opinions and patterns of behaviour of participants' in a particular context. Questionnaires have the capacity to enable the study participants focus on the research topics. Additionally, it helps to maintain consistency in the data collection process because the same questions are administered to all the participants. Walliman (2001) suggest that the anonymous nature of Questionnaires encourages participants to share information based on their truths regardless of the sensitive nature of the research.

When designing a questionnaire (Coolican, 2004; Brooke, 1996) recommended some guidelines that researchers need to adhere. Firstly, it is important that the minimum information needed for the research is requested. This is because most participants are less likely to spend extensive time responding to lengthy questions. Besides, the questionnaire should not address questions that are no longer used or obtainable elsewhere. Secondly, the structuring of the questions should be done in a manner that makes it relatively easily for the participants' to provide answers. For example, a question such as "*how many hours per week do you spend on online social networks?*" would be considerably difficult for most participants to answer. Thirdly, the researcher must ensure that all questions are answered to avoid many missing data which may consequently impact the reliability of results.

In this research, a survey questionnaire was employed for the two studies reported. The first study used a survey questionnaire to evaluate the proposed extended malware threat avoidance model (TTAT-MIP). For the second study, a questionnaire was also used to evaluate the usability of SNC. To measure the usability (usefulness and user satisfaction) of SNC, the system usability scale (SUS) technique was adopted. SUS has been empirically validated by Bangor et al., (2008) as a useful technique within the usability community for easily and quickly collecting user's subjective assessment of a system's usability. A "closed" questionnaire design was used because they assist the participants to understand the questions clearly through alternatives provided and also they provide a more significant basis for comparison. (Details about each questionnaire design are discussed in Chapter 4 and 6 of this thesis).

Moreover, open-ended questions are best used when the phenomenon of interest is relatively complex. They are also usually used when critical factors within the

research context are unidentified. A 5-Point Likert scale was employed for the questionnaires of the two studies. Likert scales are efficient measures for examining participants' opinions and attitudes as well as their subjective satisfaction with software artefacts.

Using a 5-point Likert scale, it is relatively seamless for the researcher to read out the whole list of scale descriptors ('1 equals strongly disagree, 2 equals disagree' etc.) (Likert, 1967). This explanation is lengthier for the 7-point arrangement. Such a vocalized clarification becomes rather unfeasible for a 10-point arrangement as the degrees of agreement become difficult to express in words. Relative to the distribution of data about the mean, more scale points, by definition, provide more options for the respondent. Dawes, (2008) argue that either 5-, 7- or 10-point scales are all similar for analytical tools such as SEMs or confirmatory factor analysis.

Quite a number of scales exist in the literature such as: the semantic differential; equal appearing intervals and summated rating. Likert (1967) introduced the "summated rating" which follows the steps below;

1. The presentation of a set of statements about an attitude object (statements can be positive or negative).
2. Participants are then asked to provide their responses to each statement ranging between strongly disagree to strongly agree.

Likert scales of 1 to 5 were used in this thesis because they are known to be more effective. Each value of the scale denotes a score for the items of each respondent. "5" denotes a score for "strongly agree" and "1" for "strongly disagree". "3" was used to denote a "neutral" or "undecided" score. Coolican (2004) stated that Likert scales provides greater degrees of reliability and validity while ensuring that participants provide accurate answers due to its highly structured measures.

3.3.5 Semi-structured Interviews

Semi-structured interviews are widely employed for conducting qualitative research. It allows the researcher to easily elicit the participants' opinions on a specific topic

and does not lead them towards supporting the preconceived choices of the researcher. A key advantage of suing semi-structured interviews is that it allows the researcher/interviewer to ask follow-up questions to gain further information or clarity about the topic of interest. For example, during the interviews conducted for the participants in the second study, they were asked to briefly describe their opinion about SNC. Some participants used phrases such as “I found it persuasive or interesting”. Thereafter, the interviewer probed them on what they meant by “persuasive” or “interesting”.

Hove and Anda, (2005) argue that that investigations related to issues in software development are usually qualitative in nature and relevant measures are gathered through semi-structured interviews. They argue that semi-structured interviews involve high costs and good quality which are often relative to the how the interviews are conducted. During a semi-structured interview process, interviewees are free to describe critical happenings and chat about them. Such exploration supports in better explanation and exemplification of the topic of interest.

Barriball and While, (1994), argue that semi-structured interviews are adequate for exploring participants’ perceptions with regards to complex issues. The stressed that it enables the interviewer the flexibility to probe for more information as well as clarity on answers provided. In addition, a huge advantage of this technique is the possibility of establishing a sense of rapport between the interviewer and the interviewee which could make them more comfortable to share sensitive information.

3.3.6 Data Analysis

In Chapter 4, an empirical investigation was carried out to find out the factors needed to enhance the malware threat avoidance behaviour of OSN users. The study extended and tested the Technology Threat Avoidance Theory (TTAT-MIP) and

included a unique construct – Mass Interpersonal Persuasion (MIP). A quantitative data analysis technique – Structural Equation Modelling (SEM) was adopted to undertake this investigation. Structural equation modeling was adopted for the empirical validation of TTAT-MIP because it estimates multiple and interrelated dependence in a single analysis. SEM is a largely confirmatory technique used to determine whether or not a certain model is valid as opposed to finding a suitable model (Gefen et al., 2000a). By explicitly modelling measurement error, SEM seeks to derive unbiased estimates for the relations between latent constructs. Compared to regression and factor analysis, SEM is a somewhat a new field. As such, it is still developing, and even fundamental concepts are subject to challenge and revision. Moreover, this rapid change is a source of enthusiasm for a number of researchers and a source of hindrance for others. Traditional statistical approaches to data analysis specify default models, assume measurement occurs without error, and are somewhat inflexible (Gefen et al., 2000a). Nevertheless, SEM requires specification of a model based on theory and research, is a multivariate technique incorporating measured variables and latent constructs, and explicitly specifies measurement error. SEM resolves problems of multicollinearity. Multiple measures are required to describe a latent construct. Multicollinearity cannot occur because unobserved variables characterize distinct latent constructs.

To carry out the initial analysis, the study used SPSS (a statistical software package) and the AMOS 21 to complete the final phase of the analysis. SPSS is preferred by statistical researchers due to its robust capabilities and ease of use. AMOS 21 is a mainly used as a structural equation modelling software that enables researchers to perform multivariate analysis such as: regression, factor analysis, correlation and analysis of variance. (Chapter 4 shows more details on how SEM was carried out in this thesis).

The first statistical test done in Chapter 4 was to calculate the Cronbach's alpha; it is known as the coefficient alpha which measures the reliability of the questionnaire. To measure the adequacy of the sample size of the study, Kaiser-Meyer-Olkin (KMO) value measure was used (Williams et al., 1996). After the sample adequacy and data reliability where established, the analysis commenced using structural equation modelling (SEM). SEM is increasingly adopted for behavioural studies involving causal modelling of complex multivariate data sets. Unlike other regression

techniques, SEM examines both the structural model (the expected causation amongst a set of dependent and independent constructs) and assesses the measurement model (the loadings of observed items on their estimated latent variables). Gefen et al., (2000) argue that the advantage of merging the analysis of the measurement and structural models allows measurement errors of the observed variables to be evaluated as part of the model. In addition, this rigorous analysis allows factor analysis to be joined in one operation along with the research hypothesis testing.

The study reported in Chapter 6 was aimed at evaluating TTAT-MIP using a Web-based Facebook video animation app (SNC). To carry out the evaluation, a pre- and post-tests was designed to access the OSN security awareness of the participants. The participants were presented with online images showing legitimate and illegitimate OSN activities. The images were designed based on previous cases of OSN malware attacks reported in the literature. The participants' were then required to rate the images in the following order (Definitely Not Malicious, Not malicious, Malicious, Definitely Malicious). They were automatically scored based on their level of accuracy (Details of the experimental procedures are reported in Chapter 6). Thereafter, the participants' were allowed to use the SNC app to learn about malware threats on OSNs (Details of the SNC app are reported in Chapter 5). Immediately after they interacted with the SNC app, they were required to provide feedback on their subjective opinion about the app. Therefore, a usability study (particularly a system usability scale (SUS)) was employed and the data analysed using a quantitative approach.

The SUS is relatively a simple and reliable Likert style questionnaire that is used to evaluate the subjective view of users notwithstanding their sense of taste. A study by Tullis and Stetson, (2004) recommends that SUS produces more reliable outcomes with various sample sizes when matched to other techniques such as; Questionnaire for User Interface Satisfaction (QUIS) and Computer System Usability Questionnaire (CSQU). Their studies recommend that sample sizes of at least 12-14 participants are sufficient to achieve reliable results. In this research, the data gathered through the SUS study were analysed by using SPSS statistical software.

When the participants completed the SUS questionnaire items, they were required to repeat the initial experiment to assess whether or not their malware threat awareness had significantly improved. Again their scores were recorded and then a paired samples t-test was employed for the data analysis. T-tests are forms of hypothesis test that enables the researcher to compare means. T-tests examines whether the mean scores from two experimental conditions are statistically dissimilar from each other. There are two main techniques of conducting t-tests; (1) repeated measures or paired samples t-test and (2) independent t-test. The paired samples t-tests are used in situations when participants contribute data for the dependent variable in all the conditions of the experiments. On the other hand, when different participants' contribute data for different conditions of experiment then an independent t-test would be required for the analysis.

In this thesis, a paired samples t-test was adopted because it controls for effects of the environment as opposed to independent t-test which does not. In addition, it eliminates subject-to-subject variability, requires fewer participants and yields a more powerful result (Zimmerman, 1997).

The small scale semi-structured interview session was conducted after the lab experiments. During the interviews, a smart phone device was used to collect the participants' viewpoints about SNC. The audio data was then transcribed and analysed using a deductive and an inductive thematic analysis (Details of the thematic analysis are reported in Chapter 6). Thematic analysis was used to identify whether or not there were patterns in the data consistent with TTAT-MIP. The next section discusses how the various phases of DSR were adopted to achieve the research aim.

3.4 Implementation of DSR in this Research

This section describes the development phases carried out to achieve the overall research aim. This research uses ideas from different paradigms and adopts three research methods; questionnaire surveys, lab experiments and semi-structured interviews to validate the proposed TTAT-MIP model. TTAT-MIP considers the

factors that influence the malware threat avoidance behaviour of OSN users. TTAT-MIP consists of components of the Technology Threats model and the unique characteristic of OSN – mass interpersonal persuasion (MIP). In the first iteration, the validation of TTAT-MIP was conducted by carrying out a questionnaire survey of active OSN users. In the second iteration, the model is practically evaluated through a Facebook video animation security awareness app (named – Social Network Criminal (SNC)).

It is important to reiterate that the development of the artefacts developed in this thesis was facilitated through the theoretical framework of DSR. The following sections demonstrate how DSR phases (described in **section 3.2.4**) were implemented to execute the iterations in reported in this thesis. The phases include: (1) Problem awareness; (2) Suggestion; (3) Development; and (4) Evaluation. The figure below depicts the phases, iterations and outcomes of this research.

3.4.1 First DSR Iteration

Figure 5 shows the DSR phases, methods, data sources and outcomes of the first iteration in this thesis.

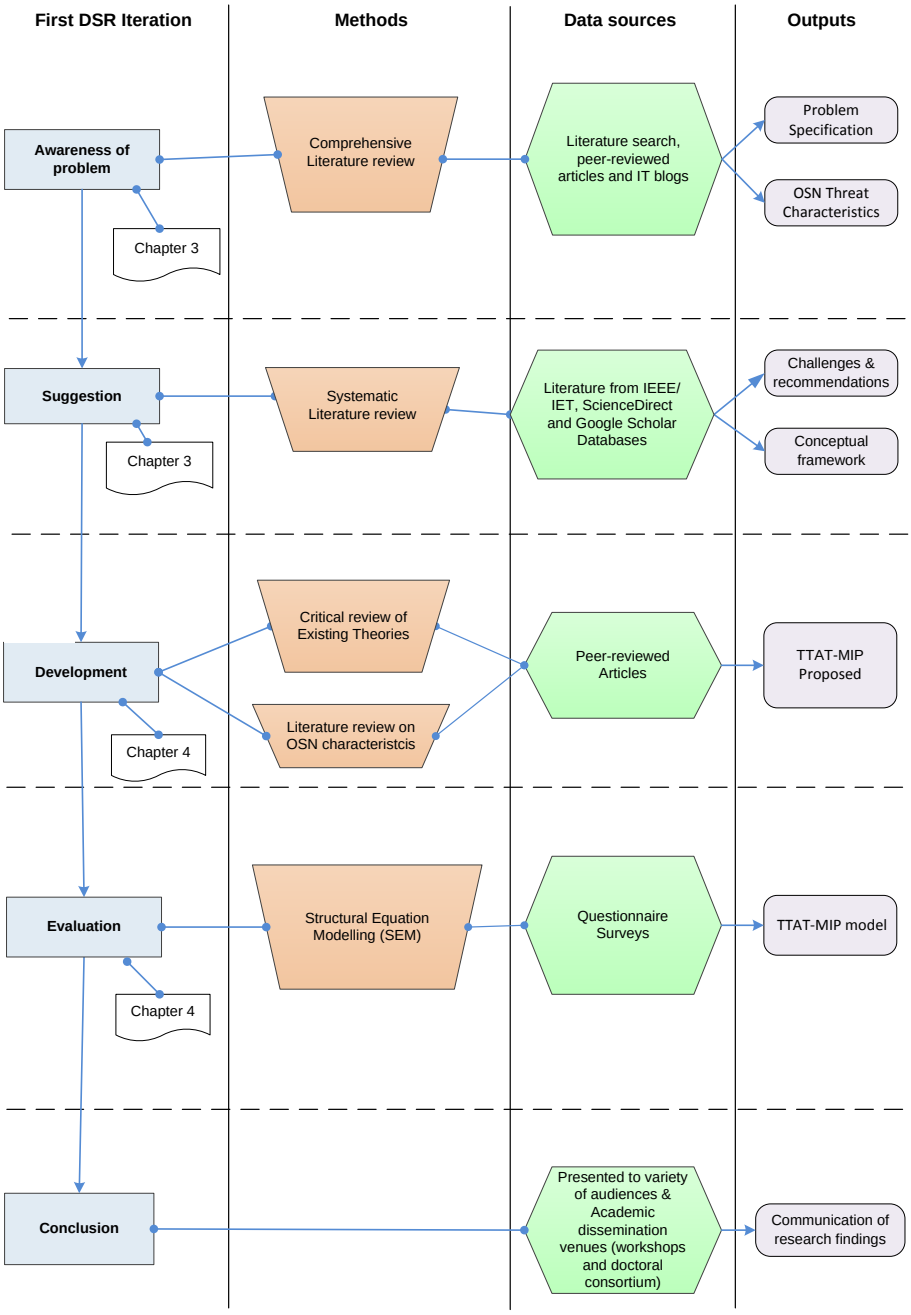

Figure 5: First DSR iteration

Problem Awareness

The fast-growing distribution of malware through OSNs leverages on the trust-based interpersonal relationships inherent amongst users. OSN users have unknowingly become passive actors in malware distribution as they are easily lured into clicking malware links and also encourage their connections to do so (it's essentially social engineering on steroids). It is therefore essential to consider the behaviour of OSN users when deploying an effective security awareness system to influence conscious security behaviour.

As OSN malware threats continue to rise, the need to raise effective security awareness to enhance the threat avoidance behaviour of users has become a necessity. Several efforts have been made to develop cyber security awareness systems in the literature; however, they are marred with challenges such as lack of end-user learning preference; lack of context about user behaviour; lack of time constraints; lack of end-user engagement and lack of platform integration. As a result, existing security awareness campaigns are ineffective, non-scalable and immeasurable over a long period of time.

The underlying problems were identified using the following sources: (1) a review on the characteristics and security issues of OSNs; (2) a systematic literature review on existing security awareness systems.

The scope of this research involves finding out the factors that needs to be considered in a security system to motivate and improve the threat avoidance behaviour of OSN users.

Suggestion

Based on the systematic literature review as well as the review on OSN characteristics and malware threat issues, a conceptual framework to guide the design of an effective security awareness system for OSN users is proposed. The conceptual framework suggests that when designing security awareness systems for OSN users, practitioners should consider factors such as: (1) Timeboxing; (2) End-user Engagement; (3) Knowledge Testing; (4) Platform Integration; and (5) Activity Specific. When deploying effective OSN security awareness systems, it is important to consider the characteristics that stimulate user behaviour. One of such unique characteristic identified in the literature is – Mass Interpersonal Persuasion (MIP) (Details of MIP are discussed in **section 3.3.2**).

In addition, this research identified a behavioural theory (TTAT) that explains the factors that influence the threat avoidance motivation of general computer users. While TTAT has been empirically validated in other research contexts, this study proposes the need to extend TTAT by including MIP as a construct to effectively formulate a model that best describes the malware threat avoidance motivation of OSN users. Hence, a case was made of the inclusion of MIP within TTAT (Details are presented in **section 3.6.2**).

Development

In this phase, hypotheses were developed based on the proposed extended model (TTAT-MIP). The constructs within the model includes: (1) Perceived Susceptibility; (2) Perceived Severity; (3) Perceived Threat; (4) Safeguard Effectiveness; (5) Safeguard cost; (6) Self-efficacy; (7) MIP; (8) Avoidance Motivation and Avoidance Behaviour. Also, the research questionnaires where formulated to measure each construct included in the TTAT-MIP model. A pilot study was conducted to assess whether or not participants understood the wordings of the questionnaire, this allowed the researcher to reword items that were not clearly understood.

Evaluation

In order to conduct an efficient and rigorous validation procedure for TTAT-MIP, structural equation modelling (SEM) statistical analysis was employed. The analysis began by screening the datasets for missing values, unengaged responses and outliers. Using SPSS software, an exploratory factor analysis was carried using which include a test for adequacy, convergent validity, discriminant validity and reliability.

Furthermore using AMOS 21 software, a confirmatory factor analysis was conducted which include a test for model fit, validity and reliability check and final model fit. This was followed by the development of the structural model which includes a test for outliers and influentials, multicollinearity and tests for mediation and interaction effects.

3.4.2 Second DSR Iteration

Figure 6 shows the DSR phases, methods, data sources and outcomes of the second iteration in this thesis.

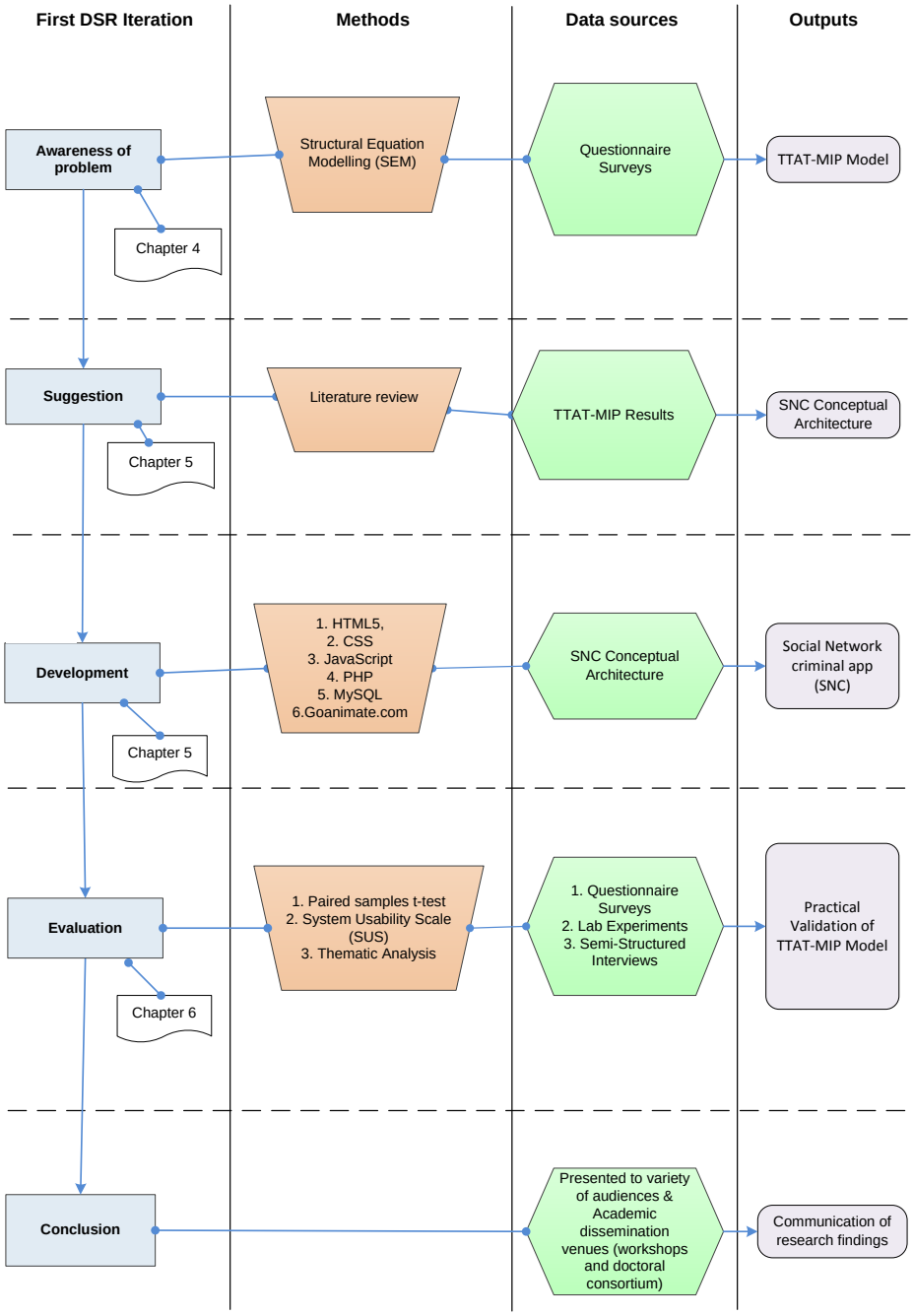

Figure 6: Second DSR iteration

Problem Awareness

After the SEM analysis carried out in the first iteration, the results suggest that some of the initial hypothesis were not supported by statistical evidence. For example, the construct "Perceived Susceptibility" had no significant influence on the perceived threat of OSN users. Therefore, in the final TTAT-MIP theoretical model, "Perceived Susceptibility" was excluded. The next proposal is to adopt the theoretical model of

TTAT-MIP to conceptualize architecture for the development of a Facebook video animation app termed Social Network Criminal (SNC).

Suggestion

In this phase, a low level architecture is conceptualized for the development of SNC based on the theoretical model of TTAT-MIP. The SNC app is proposed as a security system to raise awareness about OSN malware threats. A story-telling technique of previous incidences of OSN malware threats has been adopted to help users become aware about the vectors and avoidance techniques of malware threats. To convey the stories persuasively, drama-like scripts were written for two voice-over actors per video. The scripts were interpreted using video animation human-like characters to create a visualization of the threat situation for the users. More details about SNC's architecture are discussed in Chapter 5 of this thesis.

Development

In this phase, the requirements analyses for the development of the SNC app were conducted. The SNC app was developed using software development tools such as HTML5, PHP, JavaScript, MySQL database system and Facebook APIs. In addition, a cloud-based video animation app (goanimate.com) was used to construct the animation characters for the SNC videos. As earlier stated, SNC was developed following the theoretical guidelines of TTAT-MIP. It is expedient therefore, to evaluate the app in order to access its effectiveness, usefulness and compliance with the constructs of TTAT-MIP.

Evaluation

The first evaluation technique adopted for SNC was a pre- and post-test. Participants were accessed on the degree of accuracy to which they were able to detect malicious activities on OSNs before and after they engage with the SNC app. Using SPSS software, a paired samples t-test was employed to analyse the participants test scores. The results show a significant p-value less than 0.05 which suggest the SNC app was effective in helping OSN users detect malware threats.

The second evaluation technique adopted a usability survey to access whether or not the participants' perceive SNC as useful tool. Using SPSS software, the data was analysed and the results show a high usability score.

Lastly, a semi-structured interview was conducted to investigate the opinion of users about the SNC app. The responses of the participants' were analysed manually using inductive and deductive thematic analysis approach. The findings from the analysis suggests SNC exemplifies the constructs of TTAT-MIP (Details of the evaluation of SNC are presented in Chapter 6).

3.5 Summary

This research design Chapter discusses the IS paradigms, research methods, techniques and methodology used to conduct the overall research study. The Chapter began by explaining the objectives of DSR and behavioural science research paradigms. Then, a detailed discussion on the research techniques and data analysis approach used was presented. The Chapter concludes by elucidating how the various phases of DSR were adopted for the two iterations reported in this thesis. In the next Chapter, the literature review on the research domain is conducted to highlight and justify the scope of the overall thesis.

Chapter 4: Model Development

4.1 Overview

As discussed in **Chapter 2**, improving the malware threat avoidance behaviour of online social network (OSN) users is gaining traction in research. It is quite clear that the unique characteristics of OSNs have introduced new vectors for social engineering malware exploits. Although considerable research has been done to enhance the threat avoidance behaviour of computer users; not much work has been done within an OSN context. In this Chapter, we conducted empirical research to modify the technology threat avoidance theory (TTAT) using a survey questionnaire. We analysed 285 samples by structural equation modelling (SEM) approach, particularly Covariance-based SEM. The findings suggest that avoidance motivation predicts malware threat avoidance behaviour of OSN users. OSN users develop threat perceptions if they believe that the effect of a malware attack would be severe. Further, when tackled with a threat, users are motivated to avoid the threat based on the following factors; safeguard effectiveness; safeguard cost; self-efficacy and mass interpersonal persuasion (MIP). Dissimilar to previous studies, the findings suggest that perceived susceptibility has no significant effect on the threat perception of OSN users. Our extended model (TTAT-MIP) provides new insights on OSN users' threat avoidance motivation and a mass interpersonal persuasive approach for deploying security awareness in an OSN setting.

4.2 The Extended Technology Threat Avoidance Theory (TTAT-MIP)

In the preceding Chapter, the need to extend TTAT to include MIP within an OSN context was proposed. TTAT-MIP suggest the factors that influence the malware threat avoidance motivation of OSN users (Ikhalia and Serrano, 2016). The essential principle of TTAT-MIP is that when OSN users perceive a malware threat, they are motivated to use a safeguarding measure to avoid the threat if they perceive that it would be effective for threat avoidance. Following Liang and Xue, (2010), TTAT-MIP suggests OSN users' malware threat perceptions are affected by the perceived likelihood of the threat's occurrence as well as the perceived severity of its negative consequences. Furthermore, the determinants that influence threat avoidance motivation includes; the effectiveness of the safeguard (safeguard effectiveness), the self-confidence in using a safeguard (self-efficacy), the cost of using the safeguard (safeguard cost) and the mass interpersonal persuasion (MIP) of the safeguard.

In this research context, MIP focuses on the deployment of an efficient safeguard measure by leveraging on OSN interpersonal relationships. While previous studies have laid more emphasis on the design of effective safeguard measures, the current research argue that OSN users are more likely to avoid a malware threat when persuaded by their interpersonal connections. Therefore, MIP is perceived to have a positive influence on malware threat avoidance motivation. In **section 4.3**, the research hypotheses of TTAT-MIP are discussed.

4.3 Research Hypothesis

Following TTAT, this research posits that the malware threat avoidance behaviour of OSN users is determined by the motivation to avoid the threat (avoidance motivation) which is affected by perceived threat. Perceived threat can be defined as, the degree to which a user views that a malware threat can be dangerous. According to TTAT, threat perception is developed by perceived susceptibility and perceived

severity. Perceived susceptibility is simply defined as, the subjective belief that a user will be negatively affected by malware threat. Meanwhile, perceived severity is the degree to which a user perceives that the negative consequences of a threat will be severe (McClendon, 2012; Stretcher and Rosenstock, 1997). For this reason, the current study posits that perceived susceptibility and severity positively affects threat perception.

H1a: *Perceived susceptibility of being attacked by malware through online social networks positively affects perceived threat.*
H1b: *Perceived severity of being attacked by malware through online social networks positively affects perceived threat.*

According to Liang & Xue (2010), when computer users perceive a malware threat, they are usually motivated to avoid it. They defined avoidance motivation as the degree to which computer users are motivated to avoid malware threats using safeguarding measures.

H2: *Perceived threat of malware attacks through online social networks positively affects avoidance motivation.*

The effectiveness of a safeguard is defined as the subjective assessment of a safeguarding measure on how effective it can be applied to avoid the malware threat. This theory was drawn from the concept of perceived benefits of health belief model as postulated by Janz & Becker (1984) and the concept of response efficacy in protection motivation theory (Rogers, 1997), which predicts behaviour motivation.

Furthermore, Liang & Xue (2010) argue that when computer users perceive a malware threat, they usually begin a coping assessment process to examine potential safeguarding measures. They argue that the factors considered for using safeguarding measures are; effectiveness, cost and the self-confidence. In addition, the current study suggests that OSN users would be motivated to avoid a malware threat when a safeguarding measure is delivered to them through their interpersonal connections on a massive scale.

H3: *Safeguard effectiveness positively affects avoidance motivation.*

According to Liang & Xue (2010), safeguard effectiveness negatively moderates the relationship between perceived threat and avoidance motivation. They argue that computer users are less likely to be motivated to avoid a threat if they feel their safeguarding measure is effective. Presumably, the safeguard measure (anti-spyware software) used for their study may have informed such hypothesis. Rationally, it makes sense for computer users to depend on anti-spyware software installed on their devices to deal with malware threats. Such dependence could make users unruffled about malware threats and negatively impact on their motivation to avoid them proactively.

Nevertheless, the current study proposes a Facebook video animation app as a new safeguard measure. The app would provide security awareness through dramatised story-telling about previous OSN malware attacks; such measures would ensure users are more proactive about threat avoidance. Therefore, established in the context of our proposed safeguard, the research posits that safeguard effectiveness positively moderates the relationship between perceived threat and avoidance motivation. As a result, when OSN sense the effectiveness of our proposed safeguard, it would positively influence their threat avoidance motivation.

H3a: *Perceived threat and Safeguard effectiveness have a positive interaction effect on avoidance motivation.*

Safeguard cost is defined as the physical and cognitive efforts – such as money, time, comprehension and inconvenience needed to make use of a particular safeguard measure. It implies that users are more likely to use a safeguard if it takes less time, money and effort to adopt. In Chapter 3, "Timeboxing" was identified as a key element needed for designing effective security awareness systems for OSN users. When a security awareness system is the safeguard measure, Timeboxing places strict time boundaries on time needed for users to consume the security awareness information. Besides, an effective safeguard measure for OSN users must be engaging and not bore users. The research posits that lower the cost of using a particular OSN safeguard measure the higher the motivation to avoid malware threats.

H4: *Safeguard cost negatively affects avoidance motivation*

Self-efficacy is defined as the confidence in applying a safeguarding measure to avoid a malware threat. Self-efficacy is an essential factor that affects the motivation to avoid malware threats. Self-efficacy has been studied in previous research (Ng et al., 2009; Woon et al., 2005) and found to have a positive influence on IT security related behaviours of computer users. Hence, the greater the self-efficacy on using a security awareness system as a safeguarding measure, the greater the motivation to avoid a malware threat.

H5: *Self efficacy positively affects avoidance motivation*

As described in the preceding chapter, MIP is described by six key components; persuasive experience, automated structure, social distribution, rapid cycle, huge social graph and measured impact (Fogg, 2008). MIP is an experience designed to change human behaviours and influence behaviour. To comprehend the social influence on persuasive experience, it is important to reflect how OSNs such as Facebook, LinkedIn, and WhatsApp invitations are modelled. When a Facebook user is invited by his/her friend to use an application (e.g. a malware threat awareness video system), the system sends an invitation request with a message as highlighted below.

"Here is Joseph's IT security awareness score on this Video APP, you can get your score too by viewing the Video APP and together we can become aware on how to stop the spread of malware on Facebook".

MIP presents a novel technique for delivering a well-designed security awareness system by leveraging on the interpersonal relationships that exist on OSNs. MIP is a significant approach to deploying security awareness since the speed of malware propagation through OSNs centres on the unawareness of users; as a result, users have now unknowingly become counterparts of the attackers on a rapid level as never seen before. To empirically measure MIP, the research focuses on the success determinants of MIP which are; persuasive experience, social distribution and a large social graph (Fogg, 2008). OSN users have a tendency to be persuaded by the online

behaviour of their connections into taking certain actions (e.g. subscribing to a product or service).

The majority relatively influences the behaviour of OSN users; when a significant portion of an individual's referent social group holds a particular attitude, it is likely that the person will behave in like manner. Grounded on the rationality as mentioned above, the current research argue that the motivation to avoid malware threats by OSN users would be positively and significantly affected by the mass interpersonal persuasiveness of a particular safeguard measure.

H6: *MIP positively affects avoidance motivation*

Furthermore, the current research argues that MIP positively moderates the relationship between safeguard effectiveness and avoidance motivation. Interpersonal influence theory and research postulate that individuals are typically inclined to conform to the expectations of others regarding purchase decisions (Bearden et al., 1989). Often, users demonstrate the tendency to learn about products and services by observing or seeking information from others. Studies suggest that online social influence not only can affect consumer perception of quality of a sports brand but also consumer buying intention (Bullee *et al*, 2015; Hutter *et al*, 2013; Lee *et al*, 2014). Therefore, MIP is viewed to positively moderate the relationship between safeguard effectiveness and avoidance motivation. This implies that the higher the mass interpersonal persuasive attribute of the safeguard, the higher the motivation to avoid malware threats by OSN users.

H6a: *MIP and safeguard effectiveness has a positive interaction effect on avoidance motivation*

In accordance with Liang & Xue (2010), the research theorizes that avoidance motivation has a positive effect on avoidance behaviour.

H7: *Avoidance motivation has a positive effect on avoidance behaviour of using the Safeguard*

Figure 7 shows the relationship between the constructs (dependent and independent) variables of the proposed TTAT-MIP model.

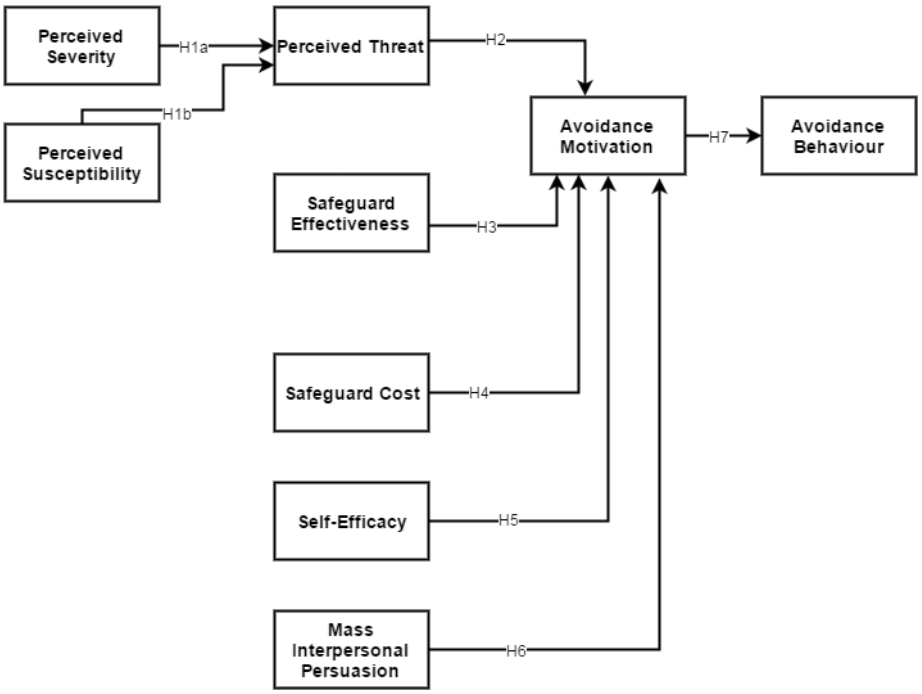

Figure 7: The Proposed TTAT-MIP Model

4.4 Research Method

4.4.1 Data

An in-person survey was used to collect data for this study during January/February 2016. The respondents were under-graduate and graduate students randomly selected from three colleges (Engineering, Design and Physical Sciences, Business, Arts and Social Sciences and Health and Life Sciences) from a university in the UK. The student group was selected for this study because they epitomise a group of individuals possibly aware of malware and OSNs and are likely active be users of at least one of the major OSN platforms. No incentives were offered to the students as they were enthusiastic about the nature of the survey. Approximately 300 students were given the questionnaire and 285 surveys were completed for a response rate of 95%. The average time they spent on online social networks daily was 6.12 hours (SD = 3.79). They had 7.34 years of online social networking experience (SD = 2.25). We had 5 variables with missing values less than 5 percent, which were replaced with the

medium from ordinal scales and the mean for continuous scales. The demographic makeups of the sample are presented in **Table 5**.

Table 5: Sample Demographics

Measure	Item	Frequency	Percentage (%)
Gender	Male	154	54
	Female	131	46
Age	Under 18	1	4
	18-24	243	85.3
	25-34	35	12.3
	35-44	6	2.1
Education	Undergraduate	236	82.8
	Postgraduate	49	17.2
Social Networks	Facebook	244	85.6
	Twitter	98	34.4
	LinkedIn	35	12.3
	MySpace	5	1.8
	Instagram	110	38.6
	SnapChat	75	26.3

4.4.2 Measurement

All model constructs were measured using a five-point Likert scale anchored at 1 = "Strongly disagree", 2 = "Disagree", 3 = "Neutral", 4 = "Agree" and 5 = "Strongly agree". The items were adapted from previous studies except for the measure of MIP. The measures of perceived threat were based on the context of malware attacks on OSNs following the recommendations of Liang & Xue (2010). Measures for perceived susceptibility was developed based Liang & Xue (2010). The measures of perceived severity were based the negative effects of malware attacks (Ikhalia, 2013; Neal, 2013; Thomas & Nicol, 2010). Measures of safeguard effectiveness were consistent with that of Liang and Xue (2010). Self-efficacy was measured based on the theoretical foundation of Compeau & Higgins, (1995). Mass interpersonal persuasion (MIP) was measured based on recommendations of Fogg, (2008). Furthermore, avoidance motivation was measured based on the behavioural intention from technology adoption studies (Davis, 1989; Davis et al., 1989). Measures for Safeguard

cost and avoidance behaviour were based on recommendations of Liang & Xue (2010).

A pilot study was conducted with twenty five OSN users to elicit relevant feedback through physical interviews; based on the feedback of the respondents we revised the wording of several items. Our questionnaire consists of four items on perceived susceptibility, five items on perceived severity, two items on perceived threat, three items on MIP, four items on safe-guard effectiveness, three items on safe-guard cost, four items on self-efficacy, three items for avoidance motivation and three items on avoidance behaviour (**See Appendix A**).

4.4.3 Analytical Method

To test our hypotheses and validate the measurements, structural equation modelling (SEM) was used, specifically covariance analysis technique. Covariance-based SEM is thought to provide better coefficient estimates and more accurate model analyses. A combination of factor analysis and multiple regression analysis with SPSS and AMOS 21 was used to analyse the structural relationship between the measured variables and the latent constructs. SEM was adopted for our analysis because of the complex nature of our conceptual model. SEM estimates multiple and interrelated dependence in a single analysis, which are limited by other first generation regression techniques such as linear regression, ANOVA and MONOVA.

4.5 Results

The overall results from the tests of the measurement and structural model suggest that TTAT-MIP model provides useful insights on how the threat avoidance behaviour of OSN users is influenced. The measurement model determined the constructs (latent variables) that were used while the structural model defined the causal relationship among the latent variables. The measurement model was used to assess the degree that the observed variables load on their latent constructs and the

results are presented in **section 4.5.1** The structural model was used to estimate causal and covariance linear relationships among the latent constructs; The results are presented in **section 4.5.2**

4.5.1 Tests of the Measurement Model

In the confirmatory factor analysis (CFA) AMOS 20 was used for testing the measurement model. Hair et al (1998) suggest that most model fit indices should attain accepted standards before deciding model fitness. Kaiser-Meyer-Olkin (KMO) value measure was used to examine the adequacy of the sample. The benchmark used for the KMO was greater than 0.6 for satisfactory analysis to be carried out (Kaiser, 1974). The KMO value for the sample used in this study is 0.812 with a good significance value of 0.000. To examine the reliability of the latent constructs, Cronbach's alpha and composite reliability (CR) was used to assess the model's internal consistency. The reliability coefficients (Cronbach's alpha) for the scales were (Perceived Susceptibility = 0.816; Perceived Severity = 0.771; Perceived Threat = 0.830; Safeguard Effectiveness = 0.863; Safeguard Cost = 0.739; Self-Efficacy = 0.808; MIP = 0.920; Avoidance Motivation = 0.796; Avoidance Behaviour = 0.765). This shows larger values than the recognised level of 0.7 recommended by Nunnally (1975). Besides, all the CR scores exceeded 0.7 recommended by Fornell & Larcker (1981) which indicates good reliability for the measurement items of each construct.

To examine the convergent validity, the current research used the three standards recommended by Bagozzi & Yi (1988) to assess the measuring model: (1) all indicator factor loadings should exceed 0.5; (2) CR should be above 0.7; and (3) the average variance extracted, AVE of every construct should exceed 0.5 (Fornell & Larcker, 1981). Exploratory factor analysis was carried out to determine the correlation amongst the variables in the dataset (**See Appendix B for results**). As evidence of convergent validity, all loadings were above 0.4 except one observed variable (0.391). Hair et al (2013) argue that loadings of 0.40 are acceptable in exploratory studies. Composite reliability of constructs ranged from 0.779 to 0.92, AVE ranged from 0.55 to 0.71, therefore satisfying all conditions for convergent validity.

Table 6: Discriminant Validity

Constructs	CR	AVE	1	2	3	4	5	6	7	8	9
1. Avoidance Motivation	0.805	0.579	**0.761**								
2. Safeguard Effectiveness	0.882	0.660	0.418	**0.813**							
3. Mass Interpersonal Persuasion	0.922	0.799	0.501	0.285	**0.894**						
4. Self-Efficacy	0.810	0.587	0.401	0.281	0.373	**0.766**					
5. Perceived Susceptibility	0.820	0.605	-0.039	-0.015	-0.015	0.002	**0.778**				
6. Perceived Severity	0.788	0.560	0.165	0.058	0.042	0.143	0.124	**0.748**			
7. Safeguard Cost	0.779	0.556	-0.384	-0.385	-0.334	-0.328	-0.001	0.020	**0.746**		
8. Avoidance Behaviour	0.798	0.575	0.616	0.386	0.404	0.391	0.159	0.131	-0.456	**0.759**	
9. Perceived Threat	0.835	0.718	0.482	0.383	0.502	0.494	0.072	0.255	-0.409	0.505	**0.847**

Note: The diagonal elements represent the square roots of AVE.

A configural invariance test was carried out and adequate goodness-of-fit was obtained when analysing a freely estimated model across the two gender groups (as evidenced by CFI = 0.904, SRMR = 0.711 and RMSEA = 0.49). In our measurement model, the research had a good model fit evidenced by CFI = 0.966, PCLOSE = 0.940, RMSEA = 0.042, Chi-square = 391.188, degrees of freedom = 261 and Standardized RMR = 0.392. To find out if there were influential respondents/records in the data-sets, a cook's distance analysis was carried out and found out that there were no records that exhibited abnormal cook's distances. In addition, a test for multicollinearity was conducted by examining the VIF values to be less than 3 and the tolerance values to be greater than 0.1.

Moreover, the study examined the discriminant validity based on the recommendation of Fornell & Larcker, (1981); the square root of the AVE should be greater than any inter-factor correlation on the correlation matrix table. **Table 6** shows the matrix correlation coefficients for all constructs. Diagonal elements are the square roots of average variance extracted for the constructs. The correlation coefficients between any two constructs are smaller than the square root of the average variance extracted for the constructs. Constructs in the measurement model of this study different from each other, which implies that all constructs have sufficient discriminant validity. Hence, the measurement model shows satisfactory reliability, convergent validity, and discriminant validity.

4.5.2 Tests of the Structural Model

The present study tested the structural model using AMOS 20. The model-fit indices for the structural model provided evidence of a good model fit (CFI = 0.997, GFI = 0.994, AGFI = 0.942, PCLOSE = 0.590, RMSEA = 0.38, χ^2/df = 1.409 and Standardized RMR = 0.0162). Based on the recommended thresholds of Hu & Bentler, (1999) our model-fit indices surpassed the recommended indices, which imply adequate fit to the collected data. **Table 7** shows the recommended indices of Hu and Bentler (1999).

Table 7: Metrics of model fit indices

Measure	Threshold	Values
χ^2/df	< 3 good; < 5 sometimes permissible	1.409
CFI	> .95 great; > .90 traditional; > .80 sometimes permissible	0.997
GFI	> .95	0.994
AGFI	> .80	0.942
SRMR	< .90	0.0162
RMSEA	< .05 good; .05 - .10 moderate; > .10 bad	0.038
PCLOSE	> .05	0.590

As shown in **Figure 7**, the model accounts for 55 percent of the variance in perceived threat, 50 percent of the variance in avoidance motivation and 61 percent of the variance in avoidance behaviour. Based on the initial hypothesis, perceived threat is significantly determined by perceived severity (b = .21, p < .01), however perceived susceptibility was found to have no significant effect on perceived threat within a social network context contrary to the findings of Liang and Xue, (2010). A Post-hoc Statistical Power calculation was conducted to assess if the model had sufficient statistical power to estimate a significant effect of perceived susceptibility if it actually exists; the result shows the observed statistical power to be 1.0 (Onwuegbuzie and Leech, 2004). This implies that the model had enough statistical power to estimate a significant effect of perceived susceptibility if it existed. Possible explanations on these conflicting findings are highlighted in the discussion section of this work

Avoidance motivation is significantly determined by perceived threat (b = .14, p < .01), safeguard effectiveness (b = .22, p < .01), safeguard cost (b = -.13, p < .05), self-efficacy (b = .15, p < .01), mass interpersonal persuasion (b = .31, p < .01). Accordingly, the findings support Hypothesis H1b, H2, H3, H4, H5, and H6. In addition, avoidance motivation was found to have a significant influence on avoidance behaviour (b = .54, p < .01).

To examine the interaction effects proposed by H3a and H6a, a product-indicator technique was adopted (Chin et al., 2003). The interaction variables were created by cross-multiplying the items of perceived threat and safeguard effectiveness and mass interpersonal persuasion and safeguard effectiveness. The items were standardized to reduce multicollinearity (Aiken and West, 2013). As shown in **Table 8**, the interaction between perceived threat and safeguard effectiveness was not significant (b = -.02, p = >.05), while the interaction between MIP and safeguard effectiveness is also not significant (b = .02, p = >.05).

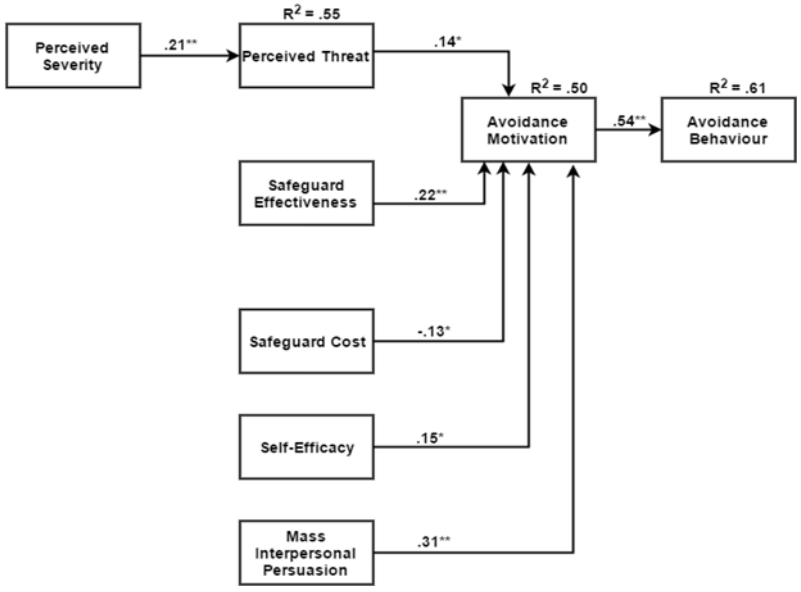

Figure 8: Validated TTAT-MIP Model

Table 8: Hypothesis Results

Hypothesis	Evidence	Conclusion

H1a: Perceived susceptibility of being attacked by malware positively affects perceived threat.	(b = .06, p = .146).	Not Supported
H1b: Perceived severity of being attacked by malware positively affects perceived threat.	(b = .21, p = .000).	Supported
H2: Perceived threat positively affects avoidance motivation.	(b = .14, p = .021).	Supported
H3: Safeguard effectiveness positively affects avoidance motivation.	(b = .22, p = .000).	Supported
H3a: Perceived threat and Safeguard effectiveness have a positive interaction effect on avoidance motivation.	(b = -.02, p = .940).	Not Supported
H4: Safeguard cost positively affects avoidance motivation	(b = -.13, p = .012).	Supported
H5: Self efficacy positively affects avoidance motivation	(b = .15, p = .004).	Supported
H6: MIP positively affects avoidance motivation	(b = .31, p = .000).	Supported
H6a: MIP and safeguard effectiveness have a positive interaction effect on avoidance motivation	(b = .02, p = .625).	Not Supported
H7: Avoidance motivation has a positive effect on avoidance behaviour of using the Safeguard.	(b = .54, p = .000).	Supported

Table 8 shows that the interaction effects proposed by H3a and H6a are not significant as evidenced by (b = -.02, p = >.05) and (b = .02, p = >.05) respectively. Furthermore, in the structural model the participants' gender, social network daily TimeHours and years were included as control variables on avoidance motivation and avoidance behaviour. None of the control variables were found to have a significant effect on either dependent variable. Therefore, the results show that all hypotheses were supported except H1a, H3a and H6a.

4.6 Discussion

This Chapter sheds light on the factors that affect the malware threat avoidance motivation of OSN users. The current study extended and tested a research model derived from TTAT using survey data analysed through structural equation modelling. The results show that the model explains a significant amount of the variance in OSN users' motivation to avoid malware on social networks (50 percent) and avoidance behaviour (61 percent). In simple terms, to motivate online social network users to avoid malware, they need to be convinced that the threats exist and are avoidable. In addition, our results show that the severity of the negative effects of malware threats positively influences their threat perception (Perceived threat). Further, findings show that when social network users decide to use a safeguarding measure to avoid a malware threat, they are positively influenced by the mass interpersonal persuasiveness of the safeguarding measure (MIP), the safeguard effectiveness, the self-confidence (self-efficacy) in using the safeguarding measure. Moreover, consistent with prior findings of Liang & Xue (2010), the current study shows that safeguard cost has a negative influence on malware threat avoidance motivation. This implies that the higher the cost of using a safeguard measure the less OSN users' would be motivated to avoid malware threats.

Contrary to the earlier findings of Liang & Xue (2010), our study shows that perceived susceptibility has no significant influence on the threat perception of OSN users'. It shows that perceived susceptibility does not affect the behaviour of OSN user' in perceiving the existence of a malware threat. Das & Khan, (2016) had similar findings in their study on the security behaviours of smartphone users; they argue that perceived susceptibility and severity has no significant effect on the security behaviour of smartphone users. Additionally, previous studies (Harris and Guten, 1979; Kirscht et al., 1966) on health risks behaviours suggest that people's relative risk judgments are positively unfair; that is, they are inclined to reflect their chances of experiencing health and safety problems are less than the chances of their peers. Reflecting on our findings; disputably, the perception of a malware threat by OSNs users is not influenced by their perceived susceptibility based on evidence in the literature which suggests that users feel less susceptible than their peers/connections. Further, unexpected results show that the interaction between

perceived threat and safeguard effectiveness as well the interaction between MIP and safeguard effectiveness were found not significant. Based on (Gefen et al., 2000b), the plausible explanation may be due to a high shared residual variance of the new variables (cross-multiplied interaction variables) with variables from which they were derived.

Mass interpersonal persuasion is shown to have the biggest effect ($b = .31$, $p < .01$) on the malware threat avoidance motivation of OSN users. While this is relatively a new phenomenon in the context of malware threat avoidance motivation, it was highly expected considering the persuasive model that defines the success of an online social networking environment.

4.6.1 Research Implications

In a malware attack kill chain, reconnaissance is the fundamental process that attackers use to gather information about their prospective victims. Attackers often utilise social engineering techniques during the reconnaissance phase of an attack and online social networks have made it relatively easy for them to deploy malware using social engineering. Numerous studies have been conducted on the security behaviours of computer users and made relevant findings to the context of the phenomena being investigated (Kumaraguru et al., 2007; Labuschagne et al., 2011; Olusegun and Ithnin, 2013). However, there is evidence in the literature that the adoption of online social networks is growing at an exponential rate, creating plausible vectors for attackers to harm millions of victims within the shortest possible time. Besides, studies argue that malware attackers mask their attacks under the guise of online social network contexts to carry out successful malware attacks, making it extremely difficult to detect (Faghani et al., 2012; Faghani and Saidi, 2009b; Websense, 2011). Nonetheless, it is essential to understand the malware threat avoidance behaviour of OSN users to formulate an effective security awareness system suitable for users.

The current research identified an existing threat avoidance model (TTAT) for general computer users and suggested the need for its extension to include a unique

online social network factor – Mass interpersonal persuasion (MIP). Our result suggests that mass interpersonal persuasion has a significant effect on the threat avoidance motivation of OSN users. A noteworthy discovery that researchers can adapt from this study is that; developing the threat avoidance motivation of OSN users should include some techniques of persuasion from users' interpersonal connections. It is essentially reverse-engineering the process through OSN users are persuaded to download malware unknowingly.

Secondly, the findings show an astounding contrast about the effect of perceived susceptibility on perceived threat when compared with the findings of Liang & Xue (2010). While the findings of Liang & Xue (2010) demonstrated a significant effect of perceived susceptibility on perceived threat, our study show otherwise, this suggests that OSN users may have a biased opinion about their vulnerability to malware attacks. OSN users perceive the existence of a threat based on its perceived severity, but apparently, they do not believe they are vulnerable. Although there is no theoretical explanation of the factors that influences the perceived susceptibility of OSN users and how it affects their threat perception, this research suggest a qualitative research could provide more clarity on these issues.

As expected, findings show a negative relationship between safeguard cost and avoidance motivation; instinctively, there is evidence the literature stating enjoyment as a key motivation for using OSNs. It is, therefore, coherent with our initial hypothesis which states that OSN users will be motivated to avoid a malware threat if the cost of using the safeguard is low. OSN users are not inclined to go through any inconvenience or process that impairs upon their perceived enjoyment derived from the art of online social networking. Researchers may need to study the elements needed to reduce the cost of using a safeguarding measure to avoid malware attacks on OSNs.

In summary, the current research has made the first attempt in explaining the need for the extension of the TTAT model and empirically validating the hypothesis leading to the development of a malware threat avoidance model (TTAT-MIP) applicable to users of OSNs.

4.6.2 Implications for Practice

The present study examines the malware threat avoidance motivation of OSN users due to the growing threats faced by organisations from the rise of malware attackers through OSNs. Malware attacks through OSNs utilise social engineering techniques that are based on the context of online social networking. The use of social engineering to deploy malware is a huge challenge faced by security practitioners because it depends on the human vulnerability that traditional anti-malware systems have not been designed to address. Some studies argue that traditional anti-malware systems are limited in their capacity to effectively and proactively protect users as a result of the signature-based malware detection model they exhibit (D'Arcy et al., 2009; Mylonas et al., 2013; Puhakainen, 2006; Stephanou and Dagada, 2014).

The findings drawn from this study can inform the development of a proactive security awareness system as a safeguarding measure to enhance their threat avoidance motivation. As the findings show, safeguard effectiveness has a positive effect on the malware threat avoidance motivation of OSN users. Similarly, self-efficacy, safeguard cost and MIP have been found to have a significant effect on threat avoidance motivation which in turn has a positive effective on their threat avoidance behaviour. Our findings expand the horizon of anti-malware mitigation strategies by stimulating a new measurable concept for security practitioners to safety policies. An automated security awareness system founded on TTAT-MIP could complement the efforts of existing anti-malware solutions in dealing with the biggest threat in cyber security landscape – the human vulnerability.

4.7 Conclusion

MIP presents a novel technique for delivering a well-designed security awareness system by leveraging on the interpersonal connections that exist on OSNs. TTAT-MIP poses a huge prospect of improving the threat avoidance behaviour (or security behaviour) of OSN users significantly and massively within the shortest possible

time. Our study shows that MIP has the biggest effect on the threat avoidance motivation of OSN users. Contrary to a previous study in this area, we found out that perceived susceptibility has no significant effect on perceived threat. Presumably, OSN users are relatively biased in estimating their vulnerability to malware attacks carried out through online social networks. Knowledge and awareness is a precondition to change behaviour but not necessarily sufficient, and this is the reason why MIP needs to be implemented in combination with other influencing constructs within the TTAT model to ensure that the experience created from a security awareness system is rapidly distributed from users to their interpersonal connections. This approach may not only impact the rapid increase of users with good security behaviour; it could dramatically improve the reliability and effectiveness of safeguarding measures. If security is too multifaceted, too effortful, users will simply ignore it. Practitioners need to consider these implications when deploying their security awareness programs to ensure that their time and goodwill are not being wasted on security measures that are too difficult to use, has a little measurable impact and ineffective.

In the next Chapter, we describe the architecture of our proposed safeguard measure – a Facebook video animation system.

Chapter 5: Social Network Criminal

5.1 Overview

This Chapter introduces “social network criminal” (SNC): a Web-based Facebook video animation app developed to raise awareness about OSN malware attacks. SNC is founded on the technology threat avoidance theory using mass interpersonal persuasion approach - TTAT-MIP. We describe the functionality of SNC and examine its architecture relative to TTAT-MIP and the framework for designing security awareness proposed in Chapter 3. The findings suggest a novel paradigm for practitioners to consider when developing effective security awareness systems.

5.2 Depiction of SNC

With great access comes great responsibility, while it’s not a direct riff of Spiderman’s philosophy, it is the driving force behind Social Network Criminal (SNC). SNC is a Web and Mobile based app that raises awareness about malware attacks while teaching OSN users how to detect and avoid on-going malware threats. The app rewards smart security choices, encourages team-building and collaboration, and encourages OSN users to invite their connections, effectively spreading information about Malware avoidance on both a macro and micro scale. SNC is pioneering new avenues within the growing field of cyber security in an engaging and interactive manner to make security awareness easily accessible and fun for users of OSNs.

SNC takes real life cases of malware attacks and presents them as a series of dramatically scripted animation videos based on previous reported cases of malware attacks. The scripts were performed by professional voice-over actors in a recording studio. Through the animation videos, OSN users learn the ins and outs of malware threat avoidance as though they are watching a scene in a movie. The core of the videos listed on SNC is to make OSN users aware about smart and simple strategies

for preventing future malware attacks in an engaging and fun filled order. At the completion of each video, an automated compulsory quiz pops up where users can put their newfound knowledge to use. Correct answers earn points, which users accrue to earn new security badges and titles. For example, with 200 points a user becomes a "1-Star Security General." In addition, the backend dashboard of SNC provides easy-to-use analytics tools evaluate user behaviour and the rate of adoption.

In an increasingly tech-dependent world, SNC is set to pioneer new ways to increase the security awareness of OSN users and improve their threat avoidance behaviour. Users need to their cyber security training in an entertaining and relatable manner to stimulate their personal interests and significantly change their security culture. After all, "in this day and age, a security-aware user is the best antivirus system."

SNC has two key objectives; (1) to create awareness for OSN users about the dynamics of social engineering malware attacks carried out through OSNs; and (2) to motivate the viral propagation of security awareness through mass interpersonal persuasion (MIP). To accomplish these daunting tasks, Ikhalia & Serrano, (2016) proposed TTAT-MIP, derived from the Technology Threat Avoidance Theory (TTAT; (Liang & Xue 2010)) which explains the motivation for technology threat avoidance by OSN users using a mass interpersonal persuasion approach. TTAT-MIP examines how OSN users avoid malware threats using a given safeguarding measure. The safeguarding measure does not necessarily have to be anti-malware software; rather it could by a well-designed user awareness system such as the proposed SNC (Arachchilage and Love, 2014).

The essential principle of TTAT-MIP suggests that when online social network (OSN) users perceive a malware threat they are motivated to use a safeguarding measure to avoid the threat if they perceive that it would be effective. According to TTAT-MIP, OSN users' malware threat perceptions are affected by the perceived likelihood of the threat's occurrence as well as the perceived severity of its negative consequences. There four key factors considered by OSN users when evaluating the degree of avoidance of a malware threat – the effectiveness of the safeguard, the self-confidence in applying the safeguard, the cost of applying the safeguard and the mass interpersonal persuasiveness of the safeguard.

Mass interpersonal persuasion (MIP) can be defined as creating persuasive experiences deployed using automated software tools to rapidly impact users in a highly socially distributed technological platform implemented with capabilities to measure its impact (Fogg, 2008; Ikhalia and Serrano, 2016). The components of MIP are described below.

- **Persuasive Experience:** This is described as an experience designed to change attitude and behaviour.
- **Automated Structure:** This implies that the persuasive experience is structured by technology.
- **Social Distribution:** Arguably the most significant component of MIP, it implies that the persuasive experience is shared from one friend to another.
- **Rapid Cycle:** This describes the swiftness at which the persuasive experience can spread from one friend to another.
- **Huge Social Graph:** This simply means that the persuasive experience can potentially reach millions of users connected through socially connected.
- **Measured Impact:** This implies that the influence of the persuasive experience is noticeable by users and creators.

The rest of Chapter is structured as follows; **Section 5.3** describes the tools utilised of SNC's development; **Section 5.4** discussed the security and reliability measures adopted for SNC; **Section 5.5** justifies the use of video animations to create security awareness; **Section 5.6** explores the architecture of SNC; **Section 5.7** elucidates how SNC relates with TTAT-MIP; **Section 5.8** describes the synthesis of TTAT-MIP, the framework for designing security awareness and SNC; then **Section 5.9** describes the functionality of SNC with suitable screen shots. The Chapter concludes with a summary and an overview of the evaluation procedure employed in the next Chapter.

5.3 Development Tools

SNC was developed using HTML, CSS, PHP, JavaScript and MySQLi database management system. The animated videos were created using cloud based software – goanimate.com. The voice-over recordings were made in English using LogicPro software at a professional recording studio. To ensure the security of SNC application, HyperText Transport Protocol Secure (HTTPS) was adopted through a Secure Socket Layer (SSL) encryption. SNC application was hosted live on a virtual private server (VPS) to avoid server downtimes, maximise page loading speed and guarantee its overall reliability.

- **HyperText Mark-up Language (HTML)**

HTML is a Mark-up language used for organising and presenting information on the World Wide Web (Anthes, 2012). HTML has several versions, but with the advent of HTML5, web pages can seamlessly integrate pictures, sound and video. HTML5 was used as the underlying programming language due to its capability to animate text, graphics and image content as well as continuous media. Besides, the proliferation of various technology devices coupled with the variety of browsers significantly motivated the adoption of HTML5 for SNC's development. HTML5 is compatible with major browsers, and as such it aligns with the modern developer slang "write once and deploy everywhere." HTML5 presents a new security model that is not only easy to use but is also used regularly by several APIs. This security model allows applications developed with HTML5 to communicate securely across domains creatively (Cazenave et al., 2011).

- **Cascading style sheets (CSS)**

A cascading style sheet (CSS) is a language that defines how HTML elements should be presented (Cederholm, 2010). By using CSS for the SNC application, a unique outlook was produced and compatible with native Web browsers without creating them externally. Akin to HTML, CSS driven applications are compatible with the majority of browsers. Factors such as usability, branding, and design are vital to any website's success, and as such utilising a language that is not entirely supported by the majority of browsers would introduce inefficiencies. CSS enabled the SNC

application to resolve common design problems more efficiently, with few lines of code and extra flexibility.

- **Hypertext Pre-processor (PHP)**

PHP is a free proficient server-side scripting language for creating dynamic and interactive Web applications (Converse et al., 2004). Mostly integrated with HTML elements, it is an open-source Web-scripting language that is compatible with all the major Web servers. We used PHP to embed code fragments in with the HTML pages of the SNC application. Also, PHP served as the connector between SNC's Web pages and its MySQL databases. PHP is a leader in the web development market with so many features which makes it the ultimate web development language. One of motivation for using PHP for SNC is the ease of use compared to the other tools like Java Server Pages or C-based CGI.

- **JavaScript**

JavaScript is a lightweight dynamic programming language commonly used as a part of web pages; it allows client-side scripts to interact with the user and make dynamic pages. With JavaScript, SNC seamlessly validated user input before sending the page off to the server; thus, saving server traffic which means fewer loads on our server. JavaScript also allows immediate feedback to the visitors without waiting for a page reload. Moreover, JavaScript helped to enhance the interactivity of SNC; through interfaces that reacted dynamically when a user places a mouse curser over various elements on the app.

- **MySQLi**

MySQLi (An improved MySQL) is a relational database management system integrated with PHP to store user data. The rational for using MySQL because it runs on all operating systems, including Linux, UNIX, and Windows. Although it can be utilised in a wide range of applications, MySQL is most often associated with web applications and is a vital element of an open-source enterprise stack called XAMPP. XAMPP is a Web development platform that is compatible with major operating systems with Apache on the Web server (Converse et al., 2004).

5.4 Security and Reliability Measures

- **Secured Socket Layer (SSL)**

Arguably, the most essential component of online applications is creating a trusted environment where users can feel safe (Heinrich, 2011). SSL certificates produce a basis of trust by creating a secure connection and browsers show visual cues, such as a lock icon or a green bar, to make users know when connected securely

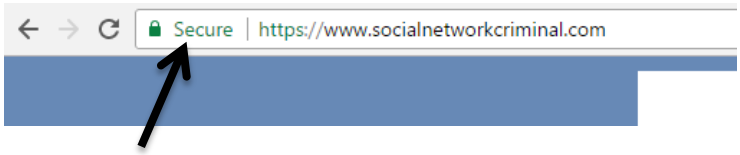

Figure 9: Shows the SSL green lock icon on SNC

SSL certificates have a public and a private key that operates together to establish an encrypted connection.

An SSL certificate was purchased for the SNC application by first creating a Certificate Signing Request (CSR) on our server. The CSR data file sent to the SSL Certificate issuer (called a Certificate Authority or CA) contained the public key. The CA used the CSR data file to create a data structure to match our private key without compromising the key itself. When the SSL certificate was received, it was then installed it on SNC's server.

- **Virtual Private Server (VPS)**

A virtual private server (VPS), is a virtual server that appears to the user as a dedicated server, but that is installed on a computer serving several websites. VPS provides more stability and reliability for web hosting needs when compared to a shared basic web hosting. The limitations of shared basic hosting are because many hosting companies are overselling their servers and loading on thousands of customers onto the same web server, consequently diminishing the reliability of their services. VPS provides easy scalability when need and more control compared to shared hosting. One of the primary reasons for using a VPS for SNC's application as opposed to a traditional web hosting service is that it allows full access to the VPS's

operating system, with unlimited administrative permissions; hence, enabling the smooth configuration of the VPS to satisfy the system requirements.

5.5 Using Video Animations

The use of animation videos to make OSN users aware of malware threats and avoidance measures could facilitate their comprehension. Lately, the rapid growth of computing capabilities and multimedia learning environments have progressed from sequential motionless text and picture frames to growing refined visualisations. Schnotz and Lowe, (2003) argue that animation concepts could be categorised by technical, semiotic and psychological levels of analysis. The technical level considers the devices used for the production of dynamic symbols. For SNC, the device used was cloud-based animation software – gonaimate.com. Next, there is a semiotic level, which considers the kind of dynamics that is conveyed in the representation. The semiotic level is concerned about what is changing in the animation (e.g., motion, transformation, changing of points of view) and how they change. The software goanimate.com allowed us the flexibility of options to fully express the semiotic level. The psychological level considers the perceptual and reasoning procedures involved when animations are observed and understood by learners.

Betrancourt (2005) suggests that that one of the significant benefits of animation is that it provides a visualisation of a dynamic phenomenon. For example, when it is not readily observable in real space and time scales (e.g., plaques tectonics, circulatory system, or weather maps) or when the real phenomenon is practically impossible to realise in a learning situation (too dangerous or too costly). Also, animation can be used to visualise events that are not impulsively conceived the way they are in the scientific domain.

The interactivity factor of animation allows the learner to understand and memorise a complex phenomenon quickly. A simple function to control the pace and direction of the animation with a suitable learning activity could make this possible. It can include several levels of interactivity from the simple “play” or “pause” function, to a complete learner control over the pace and direction of the animation. For SNC, the

HTML video player used incorporated features for users to control the speed of their learning process.

A few studies have been conducted in the use of animation to improve learning; Stiviani and Hayati, (2012) did a Classroom Action Research (CAR) to describe how the use of animation clips can improve the listening skill of the eighth graders of SMPN 21 Malang. They concluded that animation clips could be used to improve the students' listening skills if suitable animation clips are used based on the proficiency and interest levels of students'.

Arguel and Jamet (2009), states that animations and videos are repeatedly designed to present information in such a way as to aid understanding and ease learning. They carried out a study to examine the impact of showing together both a video recording and a series of static pictures. Their findings show that static pictures alone seemed to be unable to convey enough information as the study participants learning only the pictures performed worse than participant's learning through dynamic pictures and videos.

In **section 5.7**, the working operation of SNC and its relationship with the constructs of TTAT-MIP is described using screenshots from the live SNC application.

5.6 Architecture of SNC

This section focuses on explaining the architecture of the SNC to create awareness for OSN users to avoid malware attacks. A Facebook app is essentially a Web-based software application developed to adopt some of the fundamental technologies of the Facebook platform to create a broad social networking framework for the app. Facebook apps integrate Facebook's News Feed, Notifications, several social channels and other features to create awareness and interest in the app by Facebook users (Wang et al., 2011).

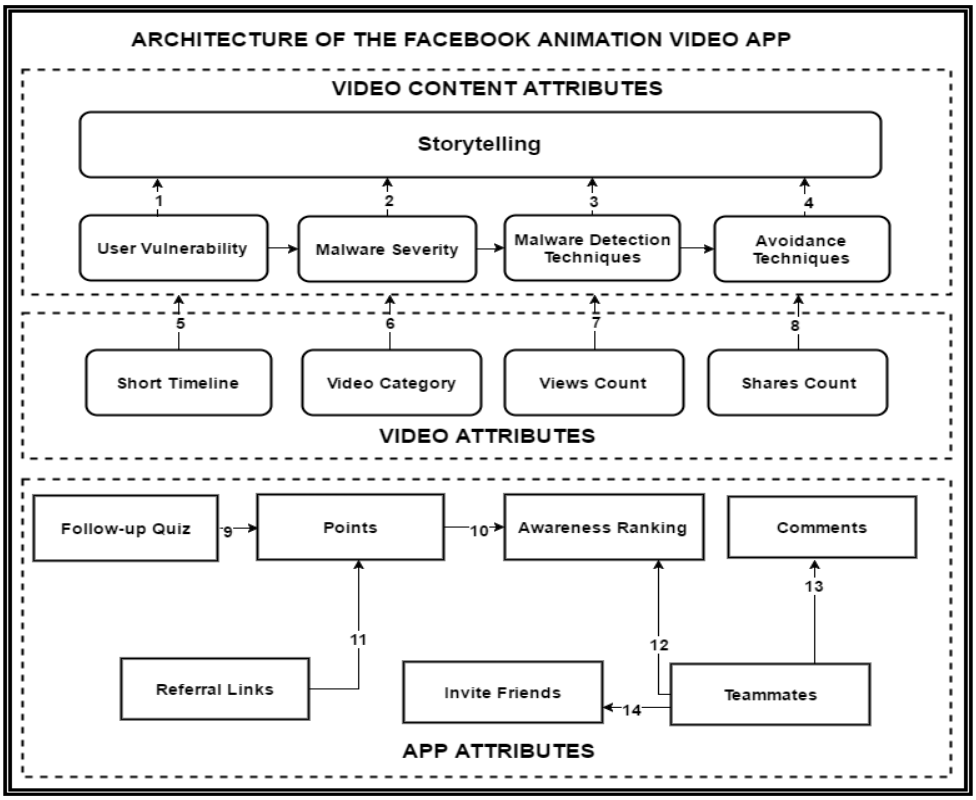

Figure 10: The Architecture of SNC

As shown in **Figure 10**; the architecture of SNC consists of three layers; Video Content Attributes, Video Attributes and App Attributes. The "video content attributes" describes the manner through which the security awareness would be disseminated to the user. The animated video content displays a dramatised script on the security awareness through storytelling of previous incidents of OSN malware attacks (Ikhalia and Serrano, 2015). The video comprises information on users' vulnerability, the severity of the attack, the potential detection techniques and non-technical mitigation strategies. **Figure 11** shows the story synopsis of one of the videos created for this research.

One afternoon during lunch hours, DR SLEEKY was working on his computer at the Anti-Malware agency and then a student MICHELLE, from business school at ABC University walked into his office to complain about a virus that corrupted all her dissertation documents.

Figure 11: Story synopsis of an animated video on SNC

'DR SLEEKY' and 'MICHELLE' are both fictitious characters created to visually dramatise a script performed by professional voice-over actors which were recruited for the purpose of this research.

Figure 9 shows the video attributes contained in the second layer of the architecture. The video attributes describe the features of the videos such as; timeframe, video category, views-count and shares-count. Consistent with the design framework discussed in Chapter 3, the videos were Timeboxed to effectively focus on the most important message. Zhang *et al.* (2016) suggest that the complications of information overload would be avoided when a video on OSNs disseminates information within a short timeframe.

The "video category" attribute allows users to efficiently select video types that are suitable to their interests (Lin and Lu, 2011b). For example, the stories of malware attacks contained in the videos of SNC are categorised based on the type of social network platform (e.g. Facebook, Twitter, and LinkedIn). Also, each video was categorized based on the vectors of OSN malware attacks (e.g. Accepting fake friend requests, Installing malicious Social Network Apps, Clicking on malicious links on a friends timeline) (Yan et al., 2007). The "views count and share-count" attributes allow users to examine the reach of the videos and may have a huge impact on their engagement on SNC.

The "app attributes" shown in the third layer of the architecture presents the features that were included in SNC to ensure that users are constantly active. Specifically, the 'Follow-up Quiz' works when a user has finished watching a video; SNC automatically displays a pop-up menu with questions about the video content. The Quiz pop-up has a timeframe of 60 seconds. The aim of the quiz is to evaluate whether the security awareness of the user has significantly improved. At the completion of the 60 seconds countdown and after the user has answered the questions, points are automatically allotted which contributes to their overall security awareness rank on the app. A correctly answered question attracts 5 points for the user. The "knowledge ranking" attribute implies that when a user has accumulated a specified number of points by providing solutions to corresponding quizzes, SNC is designed to automatically rank users awareness level using the pattern shown in **Table 9**.

Table 9: Security Awareness Ranking Pattern of SNC

Points	Rank
200 points	1 Star Security General
400 points	2 Star Security General
600 points	3 Star Security General
800 points	4 Star Security General
1000 points	5 Star Security General
1500 points and above	Field Marshal

When a user has more than two weeks of inactiveness, SNC automatically deducts 5 points from their security awareness ranks (i.e. they need to regularly watch new videos on SNC to retain/increase their ranking). Furthermore, the "Referral Links" attributes, infers that the SNC is connected to external website/blogs which extend the knowledge about the subject of social network security for the user. When a user clicks on a referral link, they gain 2 points extra automatically.

As with other Facebook apps, users would be able to automatically send app requests and receive requests from other users as well. SNC has the feature that allows users to articulate a list of 'security teammates' whenever personal invitations sent through a link to their Facebook friends gets clicked. Moreover, users can share their thoughts and comments on each video which may enhance the engagement on the app. In the next section, the theoretical constructs of TTAT-MIP model with the three layers of SNC are analysed.

5.7 Relating SNC and TTAT-MIP

Table 10 attempts to describe the relationship between TTAT-MIP and the attributes of the SNC app.

Table 10: Relationship between TTAT-MIP and the attributes of SNC Architecture

TTAT-MIP Constructs	Attributes of SNC Architecture
1. **Perceived Severity** Perceived severity is the degree to which a user perceives that the negative consequences of a threat will be severe (McClendon, 2012; Stretcher & Rosenstock, 1997).	**Video Content Attributes:** When users' watch a video that addresses problems of the severity of malware attacks faced by other users, It may significantly enhance their perceived severity.
2. **Perceived Threat** Perceived threat can be defined as, the degree to which a user perceives that a malware threat can be dangerous (Lang & Xue 2009; Rippetoe et al, 1987; Weinstein, 1993).	**Video Content Attributes:** When users' watch a video that addresses problems of both the severity of malware attacks faced by other users as well as the problems of the unsafe behaviour of other users it may have a significant impact on perceived threat.
3. **Safeguard Effectiveness** The effectiveness of a safeguard is defined as the subjective assessment of a safeguarding measure on how effective it can be applied to avoid the malware threat (Lang & Xue 2009; Carver & Scheier, 1982).	**Video Content Attributes:** When users' watch a video that addresses malware threat detection techniques as well as threat avoidance techniques, their perception of the effectiveness of using a given safeguard would be significantly improved.
4. **Safeguard Cost** Safeguard cost is defined as the physical and cognitive efforts – such as money, time, comprehension and inconvenience needed to make use of given safeguard measure (Lang & Xue 2009).	**Video Attributes:** When users' watch a video that addresses threat avoidance techniques, their perception of the cost of using a given safeguard would be significantly convinced.
5. **Self-Efficacy** Self-efficacy as the confidence of users in taking a safeguarding measure to avoid malware threat (Lang & Xue 2009).	**App Attributes:** When users' are extremely successful in providing answers to the quiz questions and consequently attain high-security awareness ranks on SNC, their Self-efficacy in dealing with malware threats would significantly improve.

6. **Mass Interpersonal Persuasion (MIP)**

MIP is defined as the ability of online social network users to influence the behaviour of their direct connections into performing similar behaviours. It involves the creation of persuasive experiences deployed using automated software tools within a small amount of time in a highly socially distributed technological platform embedded with capabilities to measure its impact (Fogg & Hall 2008).

App Attributes:

When users enjoy the persuasive experience created by the videos and the overall functionality of SNC, they would be motivated to send and receive app requests to and from their inter-personal connections.

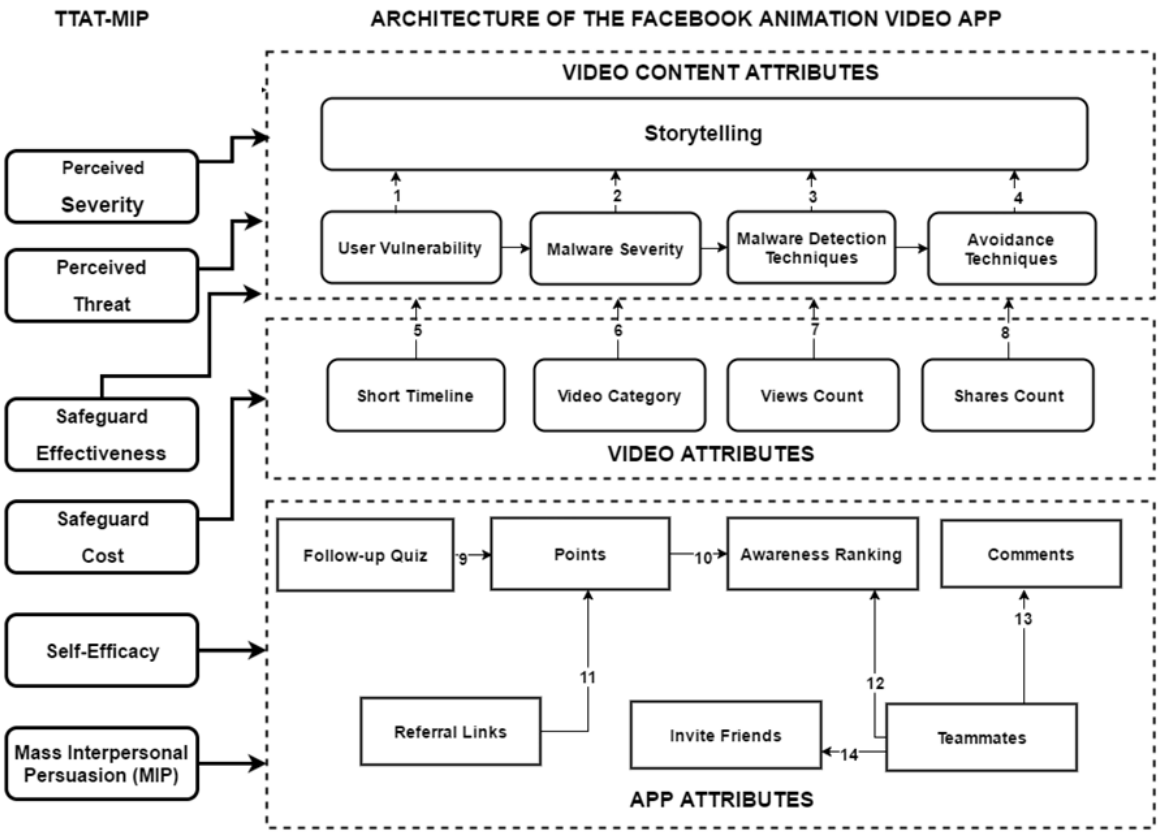

Figure 12: TTAT-MIP and the Architecture of SNC

5.8 Relating TTAT-MIP, the Design Framework and SNC

This section attempts to synthesize the three essential factors (TTAT-MIP, Design Framework and SNC architecture) to understand their relationship towards the formation of a novel and comprehensive security awareness system which symbolizes significant relevance to theory and practice.

Table 11 describes the analysis of the relationship between TTAT-MIP, the security awareness design framework and SNC App ((Ikhalia & Serrano 2015; Ikhalia & Serrano 2016; Liang & Xue 2010))

Table 11: Relationship between TTAT-MIP, the design framework and SNC app

TTAT-MIP Constructs	Design Framework	SNC App
1. **Perceived Severity** Perceived severity is the degree to which a user perceives that the negative consequences of a threat will be severe (McClendon, 2012; Stretcher & Rosenstock, 1997).	**End-user engagement:** This means that the security awareness videos will provide information to users in an amusing manner. In addition real world malware OSN malware attack stories which users are able to relate to can be very effective in having a positive impact on their **perceived severity**	When the 'fictitious victims' have finished making their complaints, the 'fictitious security expert' narrates a story of a previous real-life malware attack related to the victims' claims. This attempts to develop their perceived severity of malware attacks.
2. **Perceived Threat** Perceived threat can be defined as, the degree to which a user perceives that a malware threat can be dangerous (Lang & Xue 2009; Rippetoe et al, 1987; Weinstein, 1993).	**Activity Specific:** Similarly, the **perceived threat** of users can be positively affected if the videos make them aware about specific OSN activities vulnerable to malware attacks. **End-user engagement:** Likewise, a security awareness video that engages the emotions of users has a huge potential of positively impacting the way they **perceive malware threats**.	By combing the 'fictitious story' of the victim's malware attack and the related real-life story by the 'fictitious security expert', the watching the animated video can develop the threat perception of users.
3. **Safeguard effectiveness** The effectiveness of a safeguard is defined as the subjective assessment of a safeguarding measure on how effective it can be	**Integration:** To enhance the effectiveness of a safeguarding measure, one of our design recommendations is the integration of the system	The dramatised animated video always concludes with a recommendation to the 'fictitious victim' by the 'fictitious security expert' on actions that would have been taken to prevent such attacks. Also, within an online social networking

	applied to avoid the malware threat (Lang & Xue 2009; Carver & Scheier, 1982).	on the platform through which malware attacks are being executed. This concept allows a community of users to actively engage with the system and observe the interactions of their connections on the system. We argue that this still have a significant positive impact on their subjective assessment of the effectiveness of a safeguard measure.	context, users would be more inclined to trust the safeguarding measures proposed in the videos if their connections use the system. Therefore SNC has been integrated within a Facebook with functionalities such as "likes", "comments", and "shares" to address the effectiveness of the animated video
4.	**Safeguard cost** Safeguard cost is defined as the physical and cognitive efforts – such as money, time, comprehension and inconvenience needed to make use of given safeguard measure (Lang & Xue 2009).	**Integration:** This component would also have a considerably positive effect on the perceived cost of using a safeguard. When OSN users are able to observe the interaction of their connections with the system, especially aspects of its ease-of-use by other users, they will perceive that the cost of using the safeguard is less.	The dramatised script of the animated video occurs within a short time frame (actually 3mins), to encourage users to become aware of a malware threat and possible avoidance techniques without unnecessary complexities and stress.
5.	**Self-Efficacy** Self-efficacy as the confidence of users in taking a safeguarding measure to avoid malware threat (Lang & Xue 2009).	**Knowledge Testing:** A systematic and continuous knowledge testing process has the capacity of enhancing the self-efficacy of users in taking a safeguarding measure. Therefore this component of the framework will have a positive impact on effectiveness of the system and also the **self-efficacy** construct in the model.	SNC recognises when a user has reached the end of a video and then displays a pop-up prompting the user to take a quiz strictly related to the context of the video. The quiz has also been timeboxed (precisely 60 secs) to test how well the user awareness has improved. At the completion of the 60 seconds countdown or after answering the three pop-up questions, the user is shown how many points he/she might have earned. If any user has more than two weeks of inactiveness, they will lose ranking points (i.e. they must maintain their profiles to retain/increase their ranking). This attempts to test the knowledge of the user and consequently increase impact upon their self-efficacy in using the safeguarding measure.
6.	**Mass Interpersonal Persuasion (MIP)** MIP is defined as the ability of online social network users to influence the behaviour of their direct connections into performing similar behaviours. It involves the creation of persuasive experiences deployed using automated software tools within a small amount of time in a highly socially distributed technological platform embedded with capabilities to measure its impact (Fogg & Hall 2008).	**Integration:** Without integrating the system on the platform through which malware attacks are being executed, it would be difficult to create a mass interpersonal persuasive experience. The integration component of our framework would easily allow the demonstration of the model construct – mass interpersonal persuasion (MIP).	As with other Facebook apps, the user will automatically be prompted to share the animated video after each session. Besides, users can invite their social connections within Facebook through sharing a link from SNC to their inbox. There is also a notification feature to allow users buzz their connections about the existence of SNC. There is a comment section on each video, with "Like" and "Share" buttons. Also, SNC shows the user which friends have used the application. This attempts to develop the mass interpersonally persuade other friends to avoid malware threats.

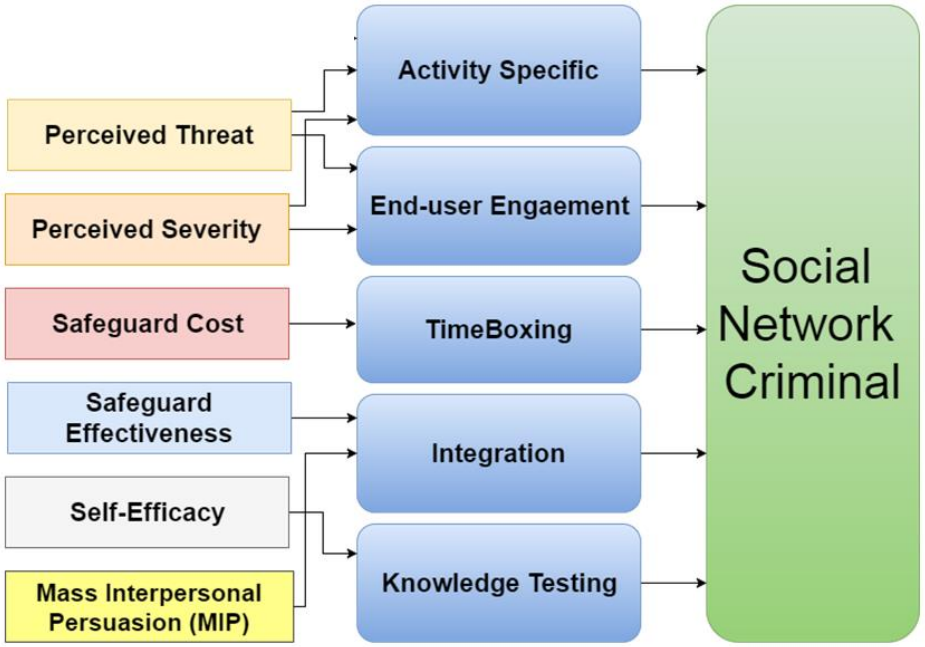

Figure 13: Depiction of TTAT-MIP, the Design Framework and SNC

5.8 SNC App Walkthrough

SNC uses real life cases of social network malware attacks to teach users how to detect and avoid social network threats. These cases are dramatically scripted and deployed through short video animation clips. For now, the use of Social Network Criminal is limited to Facebook users, but in the future, the developers intend to extend its reach to other social networks. There are two ways of accessing the app, (1) Go directly to www.socialnetworkcriminal.com and log in through a Facebook account or (2) Search for "Social Network Criminal" using Facebook's search field and click the link to the app.

Figure 14: The homepage of SNC

- **Play Video:**

This feature allows users to observe scripted animation videos based on previous cases of social network malware attacks. Each video scene is comprised of two actors, a security expert (referred to as "DR SLEEKY") and a victim of social network malware attack. In one particular video, a victim of malware attack "MICHELLE" visited "DR SLEEKY" at his office to complain about an attack that corrupted her electronic dissertation documents. "DR SLEEKY" was obliged to systematically analyse "MICHELLE's" case and relate it to a similar real-life situation. Besides, he carefully explains to "MICHELLE" how she could have prevented such attack.

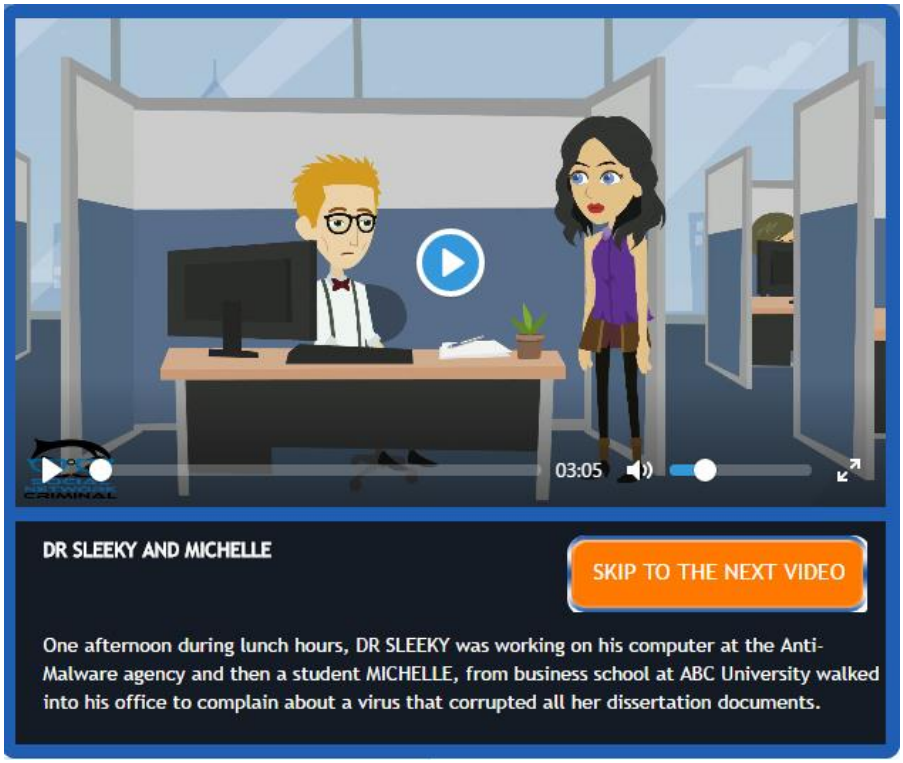

Figure 15: A Video Scene on SNC

- **Quiz:**

Immediately a video reaches the end, a pop-up quiz with a 60secs timer is automatically displayed to the user to test their information retention. There are three questions on the pop-up which are strictly related to the video context. It's almost impossible for users to provide accurate answers to the quiz without actively engaging with the video. A correct answer to a question gives the user 5 points. When a user gets through the quiz feature, the points gained by the user are automatically computed towards their security ranks. For example, with 200 points a user becomes a "1-star security general" on SNC.

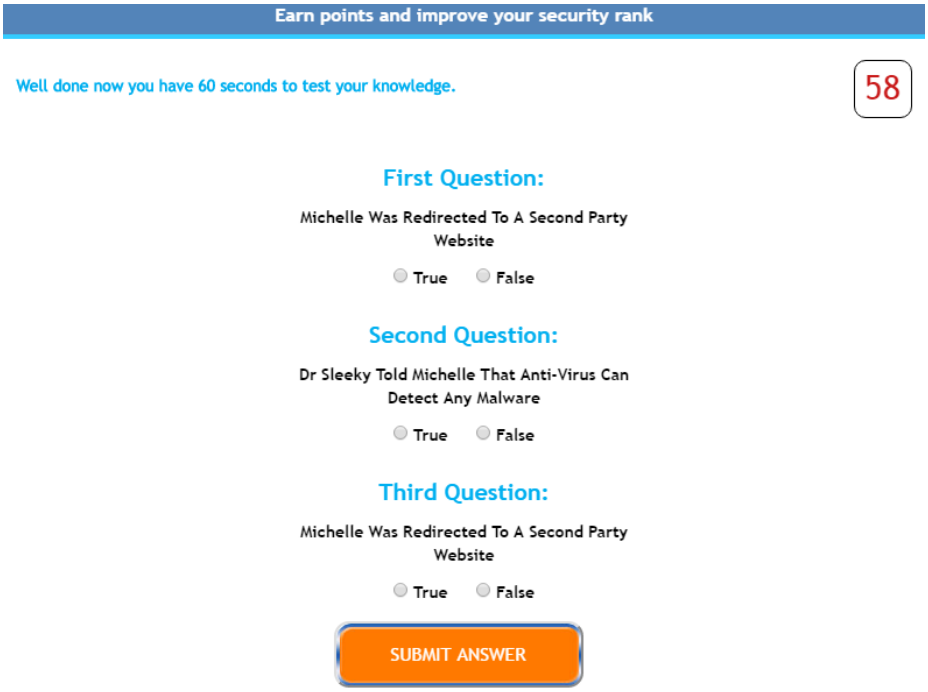

Figure 16: A Pop-up Quiz on SNC

- **My Security Team:**

This feature allows users to send invitation requests to their Facebook friends through their inbox. Teammates are created on SNC when a Facebook user accepts such invitation by clicking on the link in their inbox. This feature enhances the persuasiveness of SNC by allowing teammates to observe their security rankings and possibly stir up a competitive spirit.

Figure 17: Security Teammates of a user on SNC

- **Invite Friend:**

As with other Facebook applications, this feature allows users of "social network criminal" to notify their friends of the existence of the app. Users can inform their friends multiple times at various intervals.

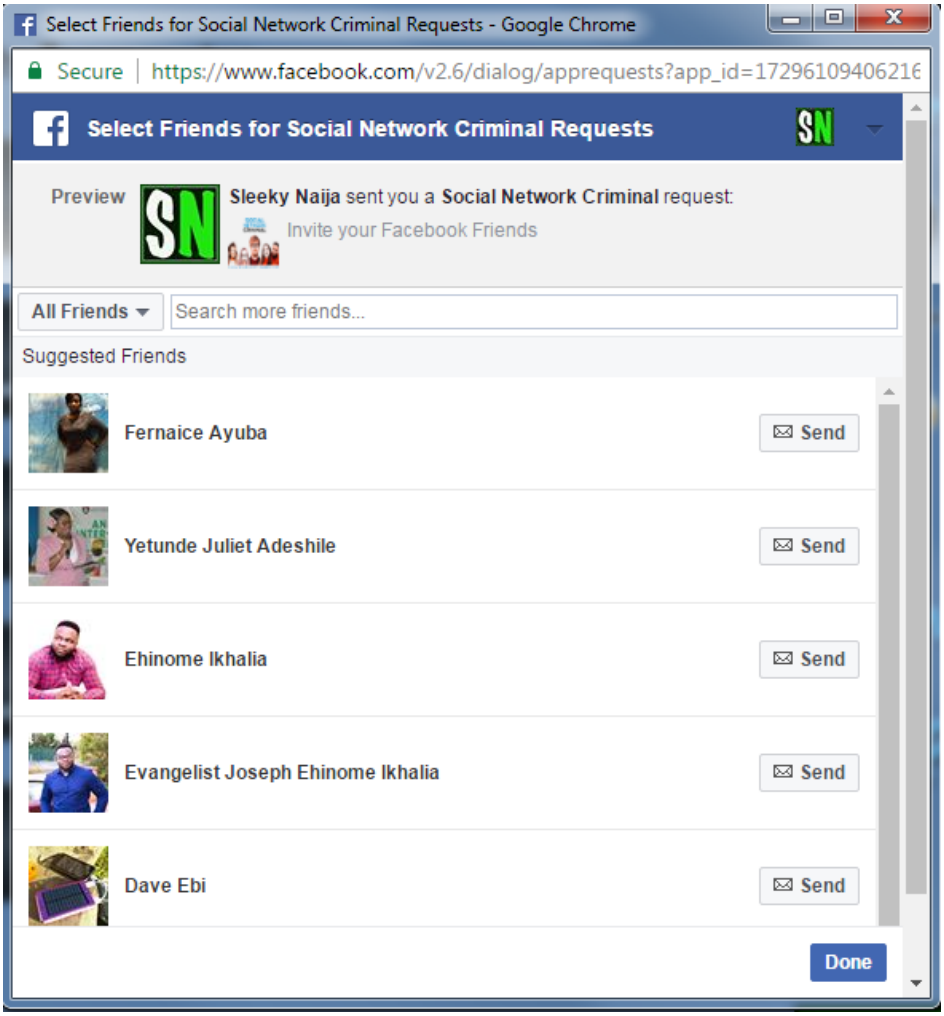

Figure 18: Informing friends about SNC

- **Earn Points:**

This feature allows users to earn extra points when they click on a link within the APP that leads to a blog article or news report about malware threats. Through this feature, enthusiastic users that are keen on going further in learning about malware threats can easily do so.

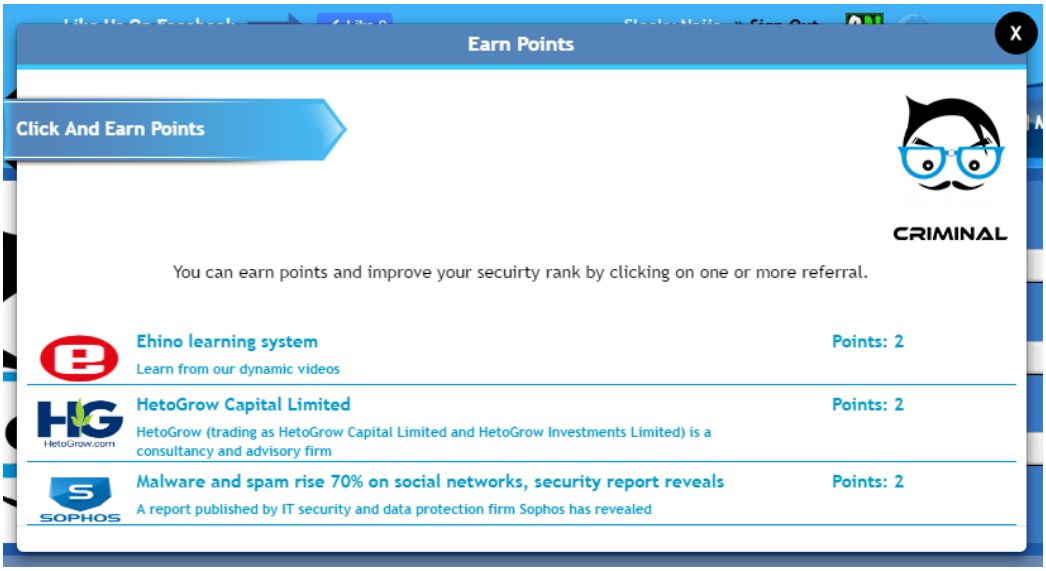

Figure 19: Earning Points on SNC

- **Messages:**

This feature allows users of SNC to send and request for free points from their security teammates. The app lets users send or ask for only 5 points per day. However, the app does not allow a user to send or request for free points if they do not watch at least one video a day and answer the similar pop-quiz questions.

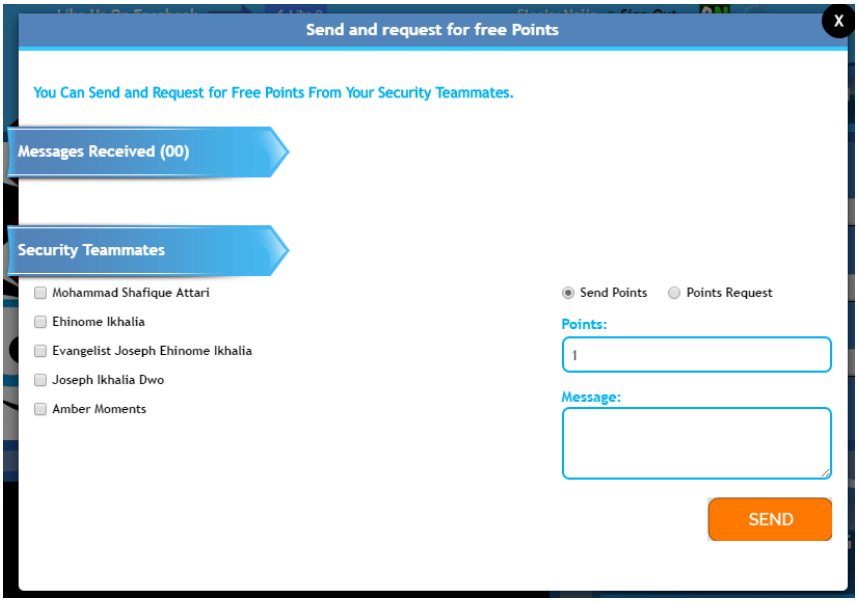

Figure 20: Sending and Receiving Free Points on SNC

- **Points Reduction:**

SNC has been carefully designed to deduct 5 points from each user if they are inactive for 14 days. This feature has been implemented to encourage users to update their security awareness with new videos consistently. For example, who attains the "5 Star Security General" status on the app and goes inactive for a year, should expect to have significant reductions on his/her points and consequent status on the app. SNC will be updated with more videos about the latest social network malware threats and techniques to avoid them.

5.9 Relating SNC and MIP

This section shows the working process of the application and how it validates the three components of MIP that are relevant to its design and implementation - persuasive experience, automated structure, social distribution, and measured impact.

Figure 21: Main Graphical User Interface of SNC

Firstly, the persuasive experience was created through the animated videos which were scripted based on previous cases of OSN malware attacks. The videos involved a well- scripted amusing dialogue between two fictitious characters (a malware attack victim and a security expert).

Next MIP suggests technology structures and automates the persuasive experience. This was achieved through the automated functionality that prompts the user to share the video with friends when a session is completed.

Figure 22: Automated Prompt on SNC

Furthermore, MIP suggests that social distribution makes it easy for friends to involve other friends in the persuasive experience. This was achieved by providing the functionality for users to send invitation requests to the connections on Facebook. In addition the functionality to allow users notify their Facebook connections about the existence of the app was also included within SNC.

Figure 23: Sending invitation requests on SNC

The measured impact component of MIP was implemented by allowing users to articulate a list of their "security teammates" (Facebook connections) and also access the security awareness ranks of their friends compared to theirs.

Figure 24: Accessing the measured impact of SNC

Furthermore, SNC includes functionalities to allow the developers measure its daily, weekly, monthly and yearly impact through metrics such as; (1) the number teammates formed (see figure 24) ; (2) the overall number of video views (see figure 25); (3) the number of page views (see figure 26); (4) the number of views on each specific video (see figure 27); (5) the time an "invitation request" was sent and when it was accepted (see figure 28)

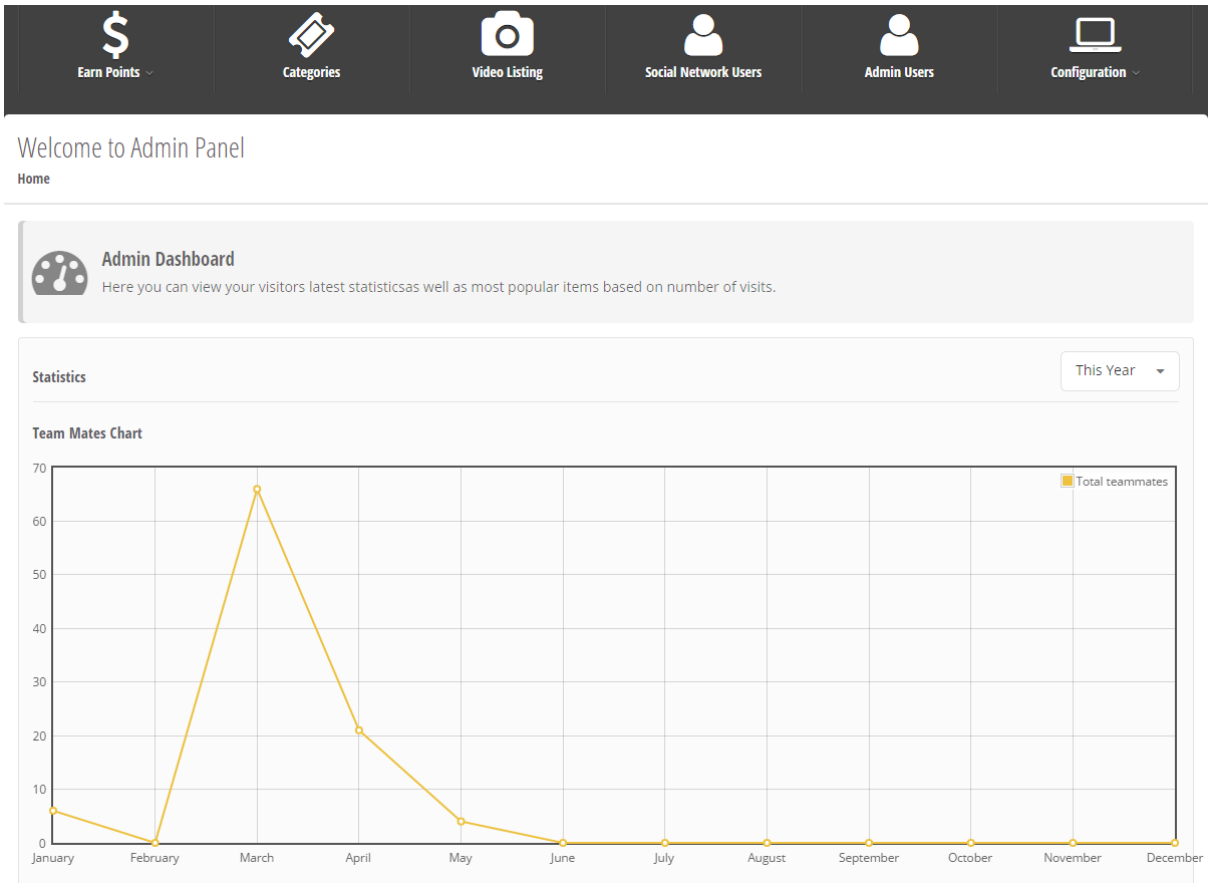

Figure 25: The number teammates formed on SNC

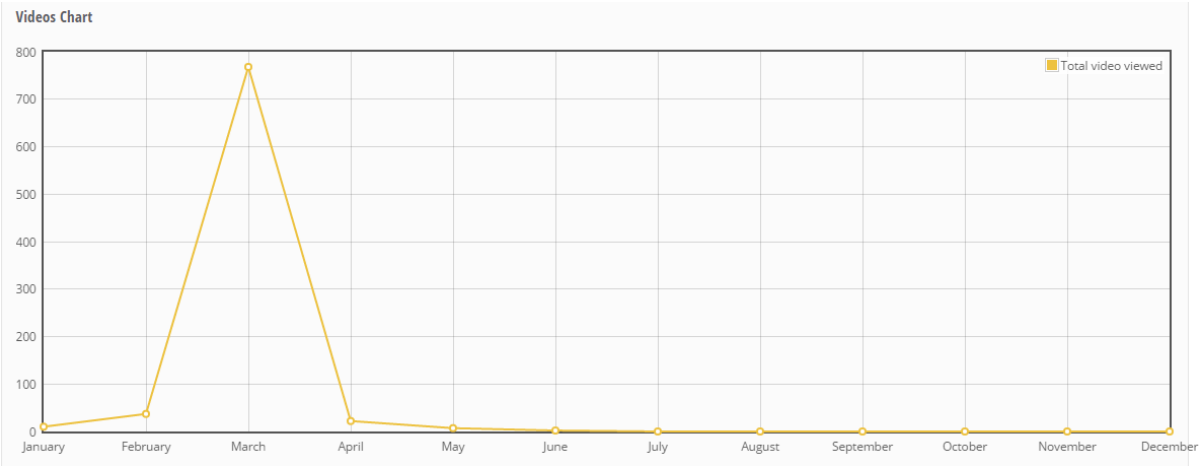

Figure 26: The overall number of video views on SNC

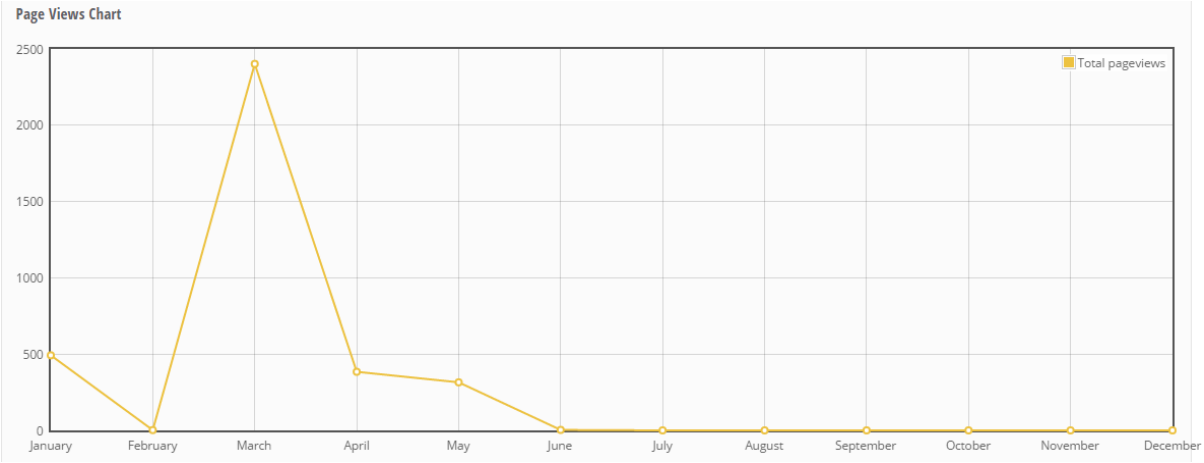

Figure 27: The number of page views on SNC

Videos Visited

Period	Video	Viewed
February	DR SLEEKY AND MICHELLE	33
February	DR SLEEKY AND JULIA	3
February	DR SLEEKY AND NIDA	1
March	DR SLEEKY AND ROSE	250
March	DR SLEEKY AND MICHELLE	156
March	DR SLEEKY AND NIDA	110
March	DR SLEEKY AND JULIA	96
March	NICKI AND VICKI	81
March	DR SLEEKY AND MCDOWELL	75

Figure 28: The views of each specific video on SNC

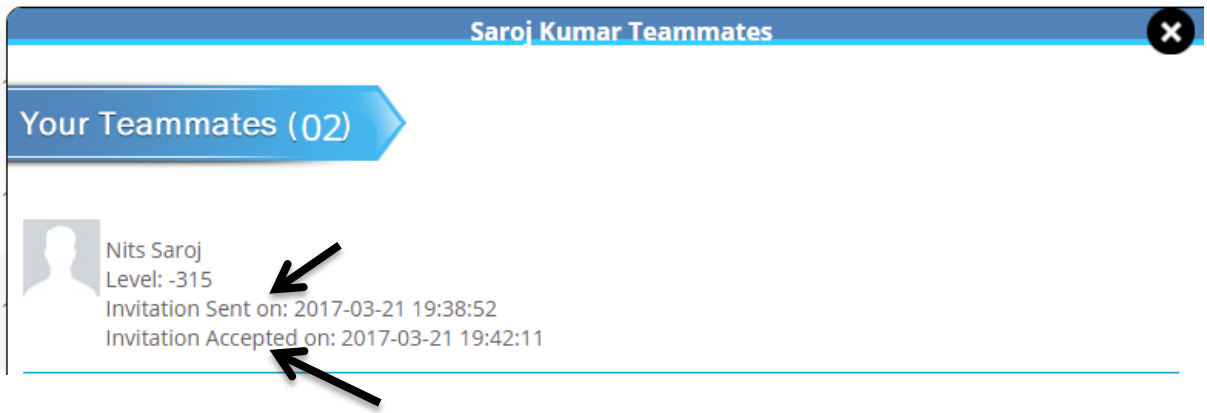

Figure 29: The time an "invitation request" was sent and when it was accepted on SNC

5.10 Chapter Summary

The current research introduced the design and development of a Web-based Facebook animated video app – SNC. The aim of SNC is in two folds: First, to make OSN users aware about the dynamics of social engineering malware attacks; second, to ensure the social distribution of the security awareness information from users to their friends. The development of SNC was based on the extended version of the technology threat avoidance theory – TTAT-MIP. Moreover, the current research combines an existing design framework in the literature which provided high level structured guidelines for developing security awareness systems for OSN users. The current research also attempts to substantiate the ongoing debate in information systems research which advocates the need for the synthesis of theory and practice in order to produce a well-grounded unique contribution to the body of knowledge. Hevner et al. (2004), mentioned that Information Systems (IS) discipline is characterised by design science and behavioural science. While behavioural science seeks to develop theories that explain human behaviour, design science seeks to create innovative artefacts that extend the boundaries of organisational capabilities. Hevner et al, (2004) strongly argue that the hazards of a design-science research idea are an overemphasis on the technological artefacts and a failure to sustain a sufficient theory base, which may result in well-designed artefacts that are ineffective in real organizational settings. Similarly, the hazards of a behavioural-science research idea are overemphasis on related theories and failure to sufficiently

recognize and predict technological capabilities, which may result in theories that address ineffective technologies.

In addition, the architecture and working operations of SNC reveals a novel paradigm organisations could adopt to provide effective security awareness for their employees in a cost-effective fashion. Organisations would have the feasibility to access how often their employees use the system and examine the effect of the intervention through the security awareness ranks that SNC displays. Be that as it may, SNC can be further developed into a mobile application compatible with IOS or android devices which would make its accessibility executed in a portable fashion. In next Chapter we focus on the empirical validation of SNC by conducting a paired t-test to compare two population means involving two samples in which observations in one sample can be paired with observations in the other sample. A Before-and-after observation on the same subjects (e.g. students' security awareness test results before and after they use SNC) would be adopted. In the next Chapter, the research aims to conduct a usability study to ascertain the satisfaction of users. The final evaluation procedure would include small scale semi-structured interviews to users to provide their opinion on SNC. The aim of the semi-structured interviews is to evaluate whether or not SNC exemplifies the constructs of TTAT-MIP.

Chapter 6: SNC Evaluation

6.1 Overview

This aim of this Chapter is to evaluate TTAT-MIP through the Social Network Criminal (SNC) app introduced in Chapter 5 of this thesis. SNC app is the Facebook video animation application developed based on the theoretical model - TTAT-MIP. Mixed methods (quantitative and qualitative) were employed for this evaluation which includes: (1) Lab experiments (2) System Usability Scale (SUS) and (3) Semi-structured Interviews. An initial pilot study was conducted to ascertain the feasibility of the evaluation methods before the main study.

The Chapter is structured as follows: **Section 6.2** describes the pilot study procedures, results and discussion. Section **6.3** describes the main study procedures, results and discussion. **Section 6.4** presents a summary of the Chapter.

6.2 Pilot Study

The current pilot study employed a usability study of SNC app as the initial phase to examine the subjective satisfaction and effectiveness of the system. Usability comprises the aspects of effectiveness, efficiency and satisfaction which was measured based on our research domain and context of use. For the experimental study (pre- and post-test), a paired samples t-test was used for the data analysis to access the impact of SNC app on user's security behaviour. Paired samples t-test is a reliable research method used for comparing the means of data from two related samples; for example, observations before and after an intervention on the same participant or comparison of measurements from the same participant using two measurement procedures.

6.2.1 Data Collection Techniques

For the pilot study, quantitative data collection techniques were employed to gather data about the usability of SNC. The usability questionnaire items used were adopted from Brooke *et al*, (1996) to suit the research context. The usability study was designed to evaluate the usefulness and learnability of the SNC app.

6.2.2 Questionnaire Design

To measure users' subjective satisfaction of SNC app, the questionnaire items of John Brooke's system usability scale (SUS) were adopted. The SUS is a modern, simple and reliable one-dimensional scale which consists of 10 questionnaire items that evaluate the subjective perception of users interacting with the system notwithstanding their personal preference. When compared with other usability measures such as QUIS and CSQU, SUS is seen as a superior assessment technique. It utilises a five-point Likert scales with anchors for "strongly agree" to "strongly disagree ". Frøkjær et al., (2000) suggest that while testing the Usability of complex computer tasks, measures of user satisfaction should be considered in formulating the questionnaire items to produce a reliable usability score relative to the application domain.

		Strongly Disagree				Strongly Agree
1.	I think that I would like to use this Facebook animated video application frequently.	☐	☐	☐	☐	☐
2.	I found this Facebook animated video application unnecessarily complex.	☐	☐	☐	☐	☐
3.	I thought this Facebook animated video application was easy to use.	☐	☐	☐	☐	☐
4.	I think that I would need assistance to be able to use this Facebook animated video application	☐	☐	☐	☐	☐
5.	I found the various functions in this Facebook animated video application were well integrated.	☐	☐	☐	☐	☐
6.	I thought there was too much inconsistency in this Facebook animated video application.	☐	☐	☐	☐	☐
7.	I would imagine that most people would learn to use this Facebook animated video application very quickly.	☐	☐	☐	☐	☐
8.	I found this Facebook animated video application very cumbersome/awkward to use.	☐	☐	☐	☐	☐
9.	I felt very confident using this Facebook animated video application.	☐	☐	☐	☐	☐
10.	I needed to learn a lot of things before I could get going with this Facebook animated video application.	☐	☐	☐	☐	☐

Figure 30: The SUS questionnaire items (Adapted from: (Brooke et al., 1996)**)**

6.2.3 Experimental Design

A pre- and post-test was carried out to evaluate the SNC app. The experimental protocol included user instructions that aided participants in undertaking the pre- and post-tests.

Experimental Protocol: Instructions for Users.

Phase 1: Malicious Activity Test (Pre-test)

Task Description: You are given 10 scenarios (with each having at least two sequence of steps) of social network activities (particularly Facebook). Rate the scenarios using one of the following options: 1="Definitely Not Malicious" 2="Not Malicious" 3="Maybe Malicious" 4="Malicious" and 5="Definitely Malicious". The test is PC based using any browser of the participant's choice.

Task: To take the test, type the link below into the address bar of your Web browser and follow the instructions given to you.

Link - https://www.surveymonkey.co.uk/r/MalwarePreTest

Phase 2: Playing Videos on SNC

Task Description: You are required to login to your Facebook accounts and search for the App "Social Network criminal". The App is designed to teach users how to detect and avoid malware threats on online social networks.

Task: Kindly watch at least 5 videos and engage with other activities within the App. The App is highly intuitive and can be accessed on a mobile device. After engaging with the App, you are required to complete a survey based on your subjective assessment of the App.

Phase 3: Malicious Activity Test (Post-test)

Task Description: You are given 10 scenarios (with each having at least two sequence of steps) of social network activities (particularly Facebook). Rate the scenarios using one of the following options: 1="Definitely Not Malicious" 2="Not Malicious" 3="Maybe Malicious" 4="Malicious" and 5="Definitely Malicious". The test is PC based using any browser of the participant's choice.

Task: To take the test, type the link below into the address bar of your Web browser and follow the instructions given to you.

Link - https://www.surveymonkey.co.uk/r/MalwarePostTest

6.2.4 Participants

The pilot study was conducted through a convenient sampling of 20 under-graduate computer science students from a top UK University. The participants were (1) active social network users; (2) they had an active Facebook account; (2) they did not have any professional background in cyber security. They had an average social networking experience of 7 years (SD: 1.694), spending an average of 8.85 hours on social networks daily (SD: 3.422). Research suggests that sample sizes of at least 12 – 14 participant (Sheng et al., 2010) are needed to achieve statistically reliable results. Moreover, a study suggests that participants between the ages of 18 to 25 are more susceptible to malware attacks than other age groups; this justified our selection of undergraduate students. For this study, each participant was taken to an available private room in the department during lunch hours. Before launching the pilot study, ethical approval was granted by the research and ethics committee of the University. A summary of demographics in the pilot study is shown in **Table 12**.

Table 12: Pilot Study Sample Demographics

Measure	Item	Frequency	Percentage (%)
Gender	Male	13	65
	Female	7	35
Age	18-24	18	90
	25-34	2	10
Social Networks	Facebook	15	75
	Twitter	7	35
	LinkedIn	7	35
	Instagram	9	45
	SnapChat	8	40

6.2.5 Procedure

The pre- and post-tests were done using a windows seven desktop computer. The online social network scenarios were designed based on previously reported incidents of OSN malware attacks. The participants gave their assessment of 10 scenarios each before after they used SNC. On the pre-test phase, legitimate OSN scenarios were randomly included with five malicious scenarios to avoid selection bias. After completing the assessment of the scenarios on the pre-test phase, they

were given 15 minutes to use SNC and engage with the videos. After that, they were asked to complete a survey containing the system usability scale (SUS) items designed to measure their subjective satisfaction of SNC. A post-test followed the SUS assessment; the participants were shown ten more OSN activity scenarios to evaluate. The researcher recorded the pre- and post-tests scores of each participant to observe whether or not their OSN security behaviour improved.

6.2.6 SUS Pilot Study Results

The current study used SPSS software package (IBM SPSS Statistics 20) for the data analysis of the system usability scale (SUS). Cronbach's alpha was calculated to measure the internal consistency of how closely related the set of items are as a group (Gliem and Gliem, 2003). Some studies argue that a given alpha greater than 0.70 is statistically adequate. Our analysis shows a Cronbach's alpha of 0.707, thereby confirming the items were closely related. To calculate the SUS score, the following rules were applied;

- For odd items: 1 was subtracted from the user response.
- For even-numbered items: the user responses were subtracted from 5.
- The scales were all values from 1 to 5 (with five being the most positive response).
- The converted responses were added up for each user and multiplied the total by 2.5. This converts the range of possible values from 0 to 100 instead of from 0 to 40.

The average participants' subjective satisfaction of SNC was significantly high (83.9 out of 100) (Brooke et al., 1996). The majority of the participants' perceived SNC to be helpful and intuitive to use. They esteemed the idea of integrating SNC within Facebook which makes it easily accessible and in line with their online social network activity. Moreover, some participants immediately invited their Facebook friends to share in the security awareness experience through SNC. The participants admitted that the animated videos were funny and addressed the security threats of online social networks as well as providing simple threat avoidance techniques. Also, they

mentioned that the characters delivered their lines in straightforward and clear English without unnecessary technical jargons.

In addition to the overall SUS score of SNC, the mean and standard deviation of each of the SUS questions we calculated in order to access the validity and reliability of the results. The SUS score of SNC from each participant and the mean and standard deviations are presented in **Table 13** and **Table 14**.

Table 13: Participants Individual SUS Score of SNC

ID	SUS Score	ID	SUS Score
1	87.5	**11**	95
2	70.0	**12**	90
3	77.5	**13**	85
4	77.5	**14**	87.5
5	92.5	**15**	70
6	80	**16**	85
7	77.5	**17**	85
8	82.5	**18**	80
9	85	**19**	95
10	92.5	**20**	82.5
Average	**Overall**	**Score**	**83.9**

Table 14: Summary of the Average Score for each SUS Question

Question	Mean Score	Standard Deviation
Q1	3.90	0.852
Q2	4.7	0.470
Q3	4.10	0.641
Q4	4.7	0.470
Q5	3.90	0.718
Q6	4.7	0.470
Q7	3.75	1.164
Q8	3.90	0.718
Q9	4.55	0.605
Q10	4.55	0.686

6.2.7 Paired Samples t-Test Pilot Study Results

The paired samples t-test compares the mean difference of the values to zero. It depends on the mean difference, the variability of the differences and the number of data (Solutions, 2017). The purpose of this study was to detect if there was a difference between the mean test scores of the participants' before and after they used SNC. Using a 95% confidence interval, procedure for conducting the paired sample t-test involves the following steps;

To calculate the sample means;

$$\bar{d} = \frac{d^1 + d^2 + \cdots + d_n}{n}$$

To calculate the sample standard deviation;

$$\hat{\sigma} = \sqrt{\frac{(d_1 - \bar{d})^2 + (d_2 - \bar{d})^2 + \cdots + (d_n - \bar{d})^2}{n - 1}}$$

To calculate the test statistic;

$$t = \frac{\bar{d} - 0}{\hat{\sigma}/\sqrt{n}}$$

Where D = Differences between two paired samples; $d_i = i^{th}$ observation in D; n = The sample size; $\bar{d}$ = the sample mean of the differences; $\hat{\sigma}$ = the sample standard deviation of the differences; T = the critical value of the t-distribution with (n - 1) degrees of freedom; t = the t-statistic (t-test statistic) for a paired sample t-test; p = the p-value (probability value) for the t-statistic (Solutions, 2017).

Similar to the first DSR iteration, SPSS software package was employed (IBM SPSS Statistics 20) for the data analysis.

Alternative Hypothesis (H_1): Using SNC can significantly improve the security behaviour of social network users.

Null Hypothesis (H_0): Using SNC does not significantly improve the security behaviour of social network users.

Each participant used approximately 45 minutes for the experiments; afterwards, the results show that the participants average mean test scores were significantly

improved after using SNC. This is evidenced by the significant p-value (p = 0.001). Results of the paired-samples t-test show that the mean test score of the participants differs before using SNC (M = 35.7500, SD = 6.231) and after using SNC (M = 53.6000, SD = 6.96155) at the 0.001 level of significance (t = 8.959, DF = 19, N = 20, p < .05, 95% CI for mean difference of 17.85000).

6.2.8 Validity of the Paired Sample T-Tests

A normality test was conducted to further access the validity of the results. For the paired samples t-test to be valid, the differences between the paired values should be approximately normally distributed. A Kolmogorov-Smirnov test was conducted to compare the study sample with a reference probability distribution (one-sample K–S test), and the results show a non-significant result (p = .200). To pass the normality test a non-significant result is required (i.e. p > 0.05), this implies that the earlier results are statistically valid and did not occur by chance (Sheng and Magnien, 2007; Solutions, 2017). The diagrams in **Figure 31** and **Figure 32** shows the histogram of differences in marks and a normal probability (QQ) plot respectively.

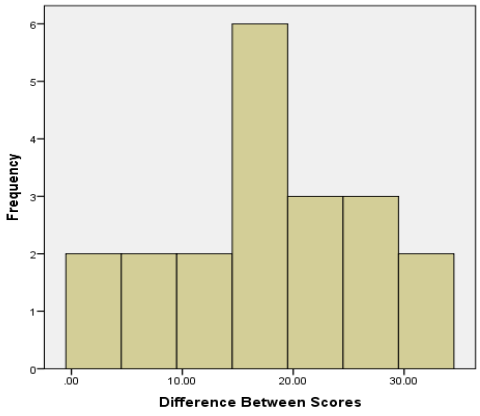

Figure 31: Difference in pre- and post-scores (Pilot Study)

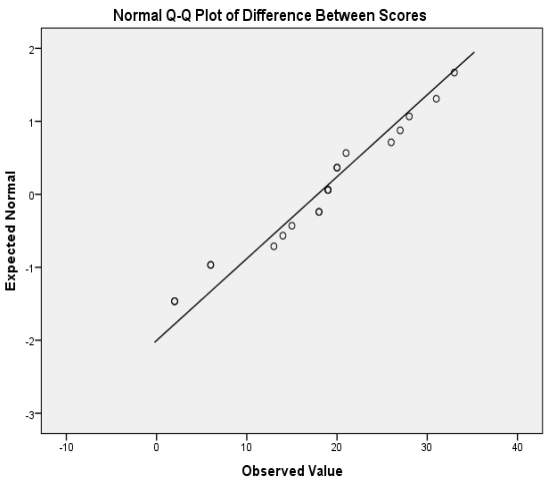

Figure 32: Normal Probability QQ plot of the Difference Scores (Pilot Study)

6.2.9 Pilot Results Summary

The current pilot study attempts to evaluate users' subjective satisfaction of SNC and its potential impact on their threat avoidance behaviour. To execute these objectives, a SUS study was employed as well as a paired samples t-test study. Preliminary SUS results show that OSN users find SNC as a useful tool for security awareness based on the average usability score of 83.9 that was achieved. The participants indicated a few areas of the application that needed to be reviewed with SNC's interface which were addressed before the main study was carried out.

Moreover, the research found substantial preliminary evidence that SNC could improve the security behaviour of OSN users as shown by the p-value ($t=8.959$ $p = 0.001$). The analyses of the results suggest an overall average improvement of 17.85 points. Though, if this experiment was repeated we probably may achieve a 'mean paired difference' in scores different from 17.85. Nevertheless, with the confidence interval (CI) of 95% and the additional validity tests conducted, this study argues that these results signify a huge step forward within the domain of usable and efficient security awareness systems.

In the next section, the main study conducted with a larger sample of 40 participants' is reported. In addition, to the existing measures used in the pilot study, the main study extends the evaluation techniques to include semi-structured interviews. The

research predicts that semi-structured interviews would provide richer insights on the usefulness, effectiveness and potential weaknesses of SNC.

6.3 Main Study

Using the same data analysis tools and procedures as reported in the pilot study, Cronbach's alpha was calculated the to measure the reliability or internal consistency of how closely related the set of items are as a group (Gliem and Gliem, 2003). The results show a Cronbach's alpha of 0.707, thereby confirming our data reliability.

In the main study, a SUS study and paired samples t-test study were employed together with semi-structured interviews to gain further insights on how the participants perceived SNC. The SUS questionnaire items used in the pilot study was adopted for the main study. Semi-structured interviews were adopted as an attempt to avoid the researchers influence on the participants' responses. The participants were told to express how they perceived the overall components of SNC freely. With their permission, their responses were recorded using a smart phone device. A manual qualitative data analysis approach was used to evaluate their feedback to find out whether or not SNC reflected the constructs of TTAT-MIP.

6.3.1 Participants

The study was run with 40 participants from a convenient sample of students in Brunel University. 40 participants voluntarily took part in the paired samples t-test experiments and usability studies respectively, while 20 of them agreed to provide verbal feedback on their experience the Brunel University's library. They were invited to St. John's building computer laboratory at Brunel University. Most of the participants were aged from 18 to 25, with a gender split of 67.5 percent male and 32.5 percent female. They spent an average of 8 hours daily on online social networks (SD: 3.163) and an average of 7 years online social networking experience (SD: 1.754). A summary of the main study demographics is presented in **Table 15**.

Table 15: Main Study Sample Demographics

Measure	Item	Frequency	Percentage (%)
Gender	Male	27	67.5
	Female	13	32.5
Age	18-24	36	90
	25-34	4	10
Social Networks	Facebook	28	70
	Twitter	9	22.5
	LinkedIn	8	20
	Instagram	17	42.5
	SnapChat	13	32.5

6.3.2 Procedure

Each participant was briefed on the nature of the experiment, its phases and was given the required participants' consent form to sign. The researcher informed them that the purpose of the experiment was to test their awareness about malware threats on online social networks through a Facebook video animation app – SNC. The pre- and post-tests were done using a windows seven desktop computer.

In the pre-test, the participants were presented with the same ten online scenarios (uploaded on surveymonkey.com) as those participants were in the pilot study. They were asked to identify malicious scenarios of online social networks from legitimate ones. After evaluating the first ten scenarios, they were given 15 minutes to complete the training activity on SNC. Thereafter, they were asked complete a SUS questionnaire items to measure their subjective satisfaction of SNC. The participants were shown ten more scenarios in the post-test similar as those participants were in the pilot study. Their pre- and post-test scores were automatically recorded to observe their awareness of malware threats and to see whether or not SNC had a significant effect on their understanding of malware threats on online social networks.

Furthermore, the participants briefly gave a verbal feedback when asked to express their opinion about receiving security awareness through SNC.

6.3.3 Data Collection Instruments

The data collection was carried out through a SUS survey questionnaire and a pre- & post tests administered to 40 participants. The participant's responses were recorded with a smart phone using a semi-structured open-ended interview. Each participant engaged in the experiment within an hour but not less than 45 minutes. Similar to the pilot study, the main study began by allowing the participants to undertake an online test to examine their understanding of malware threats on online social networks. Then their scores were recorded. Thereafter, they were allowed to engage with SNC and watch all the security awareness videos. Immediately they completed their engagement with SNC, their subjective satisfaction of SNC was accessed through the SUS questionnaire. They were required to complete a second online test, and their scores were recorded. The experiments were concluded by allowing participants to provide voluntary verbal feedback on their assessment of SNC. 20 participants agreed to complete this process. The data collected from the SUS questionnaire and the pre & post tests were analysed using a quantitative data analysis approach. A qualitative data analysis approach was used to analyse the verbal feedback collected from the unstructured, open-ended interviews.

6.3.4 Results Analysis

The purpose of the results presented in the main study is to answer the following questions;

1. Are online social network users satisfied with their experience with SNC?

2. Does the use of SNC have a significant effect on the threat avoidance behaviour of online social network users?

3. To what extent does SNC reflect the constructs of TTAT-MIP?

To answer the first question, the SUS questionnaire items were analysed using quantitative data analysis techniques (particularly the method for calculating SUS scores as specified in **section 6.2.6**). For the second question, a quantitative data analysis was conducted (specifically, a paired samples t-test). The third question was

answered using a qualitative data analysis technique (particularly thematic analysis). The results are presented in sections **6.3.5, 6.3.6** and **6.3.7** respectively.

6.3.5 SUS Main Study Results

Using the same tools and techniques reported in the pilot study, Cronbach's alpha was calculated to measure the reliability of the datasets (Gliem and Gliem, 2003). The Cronbach's alpha was found to be 0.711 which suggests adequate statistical reliability. In general, the average SUS score for the participants was significantly high (82.9 out of 100) (Brooke et al., 1996). The SUS score represents a composite measure of the general usability of SNC. The score was obtained using the same procedure reported in the pilot study (see **section 6.2.6**).

Re-affirming the findings of the pilot study, the participants' mentioned that they find SNC intuitive and easy to use. Although a few participants noted that SNC should have been available on other online social networks, they find more appealing than Facebook (e.g. Instagram and SnapChat). According to the participants, the concept of integrating SNC within Facebook which makes raises their trust on its reliability and usefulness. Most of the participants were intrigued by the structure of the videos and the clarity of security awareness message. The participants admitted that the animated videos were amusing while providing simple threat avoidance techniques. The SUS score of SNC from each participant and the mean and standard deviations are presented in Appendix B of this thesis.

6.3.6 Paired Samples t-Test Main Study Results

The same techniques reported in the pilot study section for the paired samples t-test were used for the main study. The findings show that the participants average mean

test scores were significantly improved after using SNC. This is evidenced by the p-value (p = 0.000). The participants mean test score was significantly different before and after using SNC as evidenced by the mean and standard deviations respectively. The mean and stand deviations before test, (M = 30.88, SD = 5.823) and after test (M = 48.83, SD = 6.664). (t = 15.959, DF = 39, N = 40, p < 0.05, 95% CI for mean difference of 17.950).

6.3.7 Validity of the Paired Samples t-Tests

For the paired samples t-tests to be valid the differences between the paired values should be approximately normally distributed. To calculate the differences between the pre- and post-scores SPSS statistical analysis tool was used.

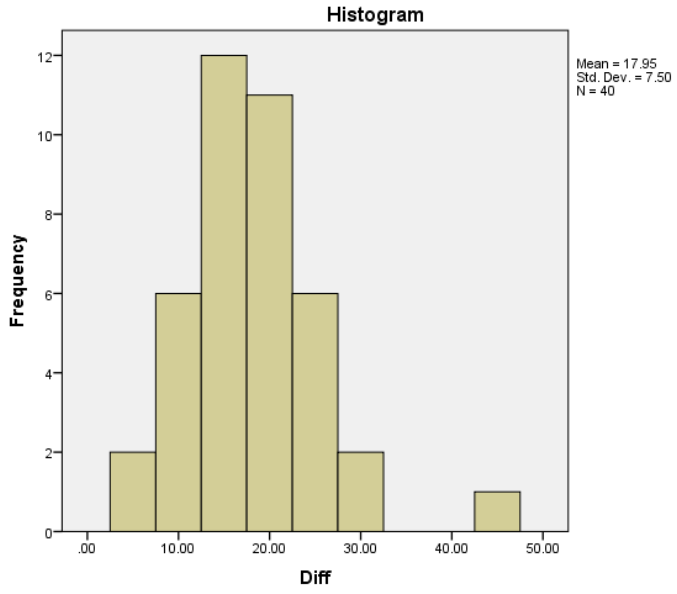

Figure 33: Difference in pre- and post-scores (Main Study)

Similar to the pilot study, the normal distribution was accessed by observing the histogram of the difference data shown in **Figure 33**. In addition, the normal distribution can also be checked by accessing the normal probability (QQ) plot shown in **Figure 34**.

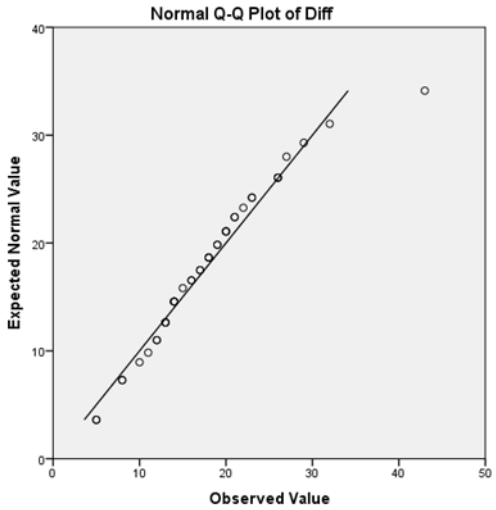

Figure 34: Normal Probability QQ plot of the Difference Scores (Main Study)

6.3.8 Semi-Structured Interviews

The semi-structured interviews allowed the participants to express their viewpoints about SNC app (Turner, 2010). Twenty participants provided verbal feedback on their perception of SNC app. The participants were asked an initial open-ended question to elicit their thoughts about SNC which was recorded with a smart phone. After that, some participants were told to clarify what they meant with particular words or phrases (e.g. "what do you mean by 'interesting'?"). The nature of open-mindedness of this approach allowed the participants to provide a reflective view on their experience with the app. According to Creswell, (2007), data gathered using this qualitative approach are often burdensome to code and analyse. However, it limits researcher bias within the study.

6.3.9 Semi-structured Interview Results

A hybrid of inductive and deductive thematic analysis approach was employed to analyse the qualitative data items. A deductive thematic analysis is an approach driven by a researcher's analytical or theoretical interests, while an inductive thematic analysis approach is mainly data driven (i.e. founded on the participants" responses) (Fereday and Muir-Cochrane, 2006). The choice of using a hybrid approach is motivated by the quest to avoid research bias by allowing the opportunity to identify potentially new factors that may have influenced SNC other than the factors inherent within TTAT-MIP. The following process was followed to conduct the analysis.

- The researcher got familiarised with the data: after transcribing the data, it was carefully read and re-read.
- Initial code generation: features of the data were coded systematically in relation to the theoretical model – TTAT-MIP.
- Searching for themes: the initial codes were collated into initial representative themes as seen in **Figure 35**.
- Reviewing themes: The themes were reviewed and their interrelationships were accessed. Thereafter, strongly related themes were combined to represent a single theme as seen in **Figure 36**.

One of the main advantages a hybrid thematic analysis approach is the flexibility it allows the researcher to utilise rational judgement in defining themes. The results of the semi-structured interviews are summarised in **section 6.3.9**. In section **6.3.10**, the findings are discussed and how it relates with TTAT-MIP.

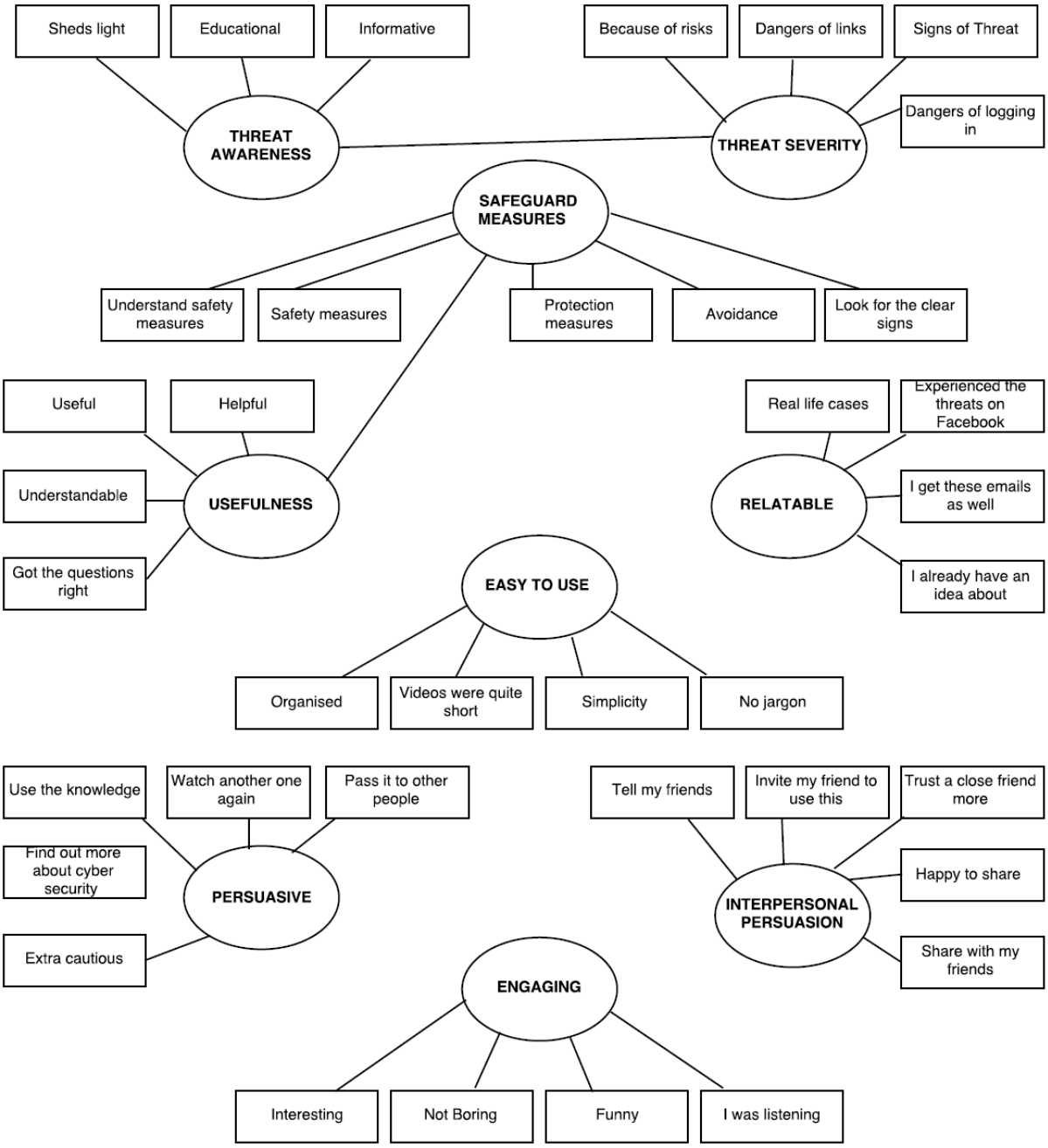

Figure 35: Initial Thematic Map, Showing 9 Main Themes

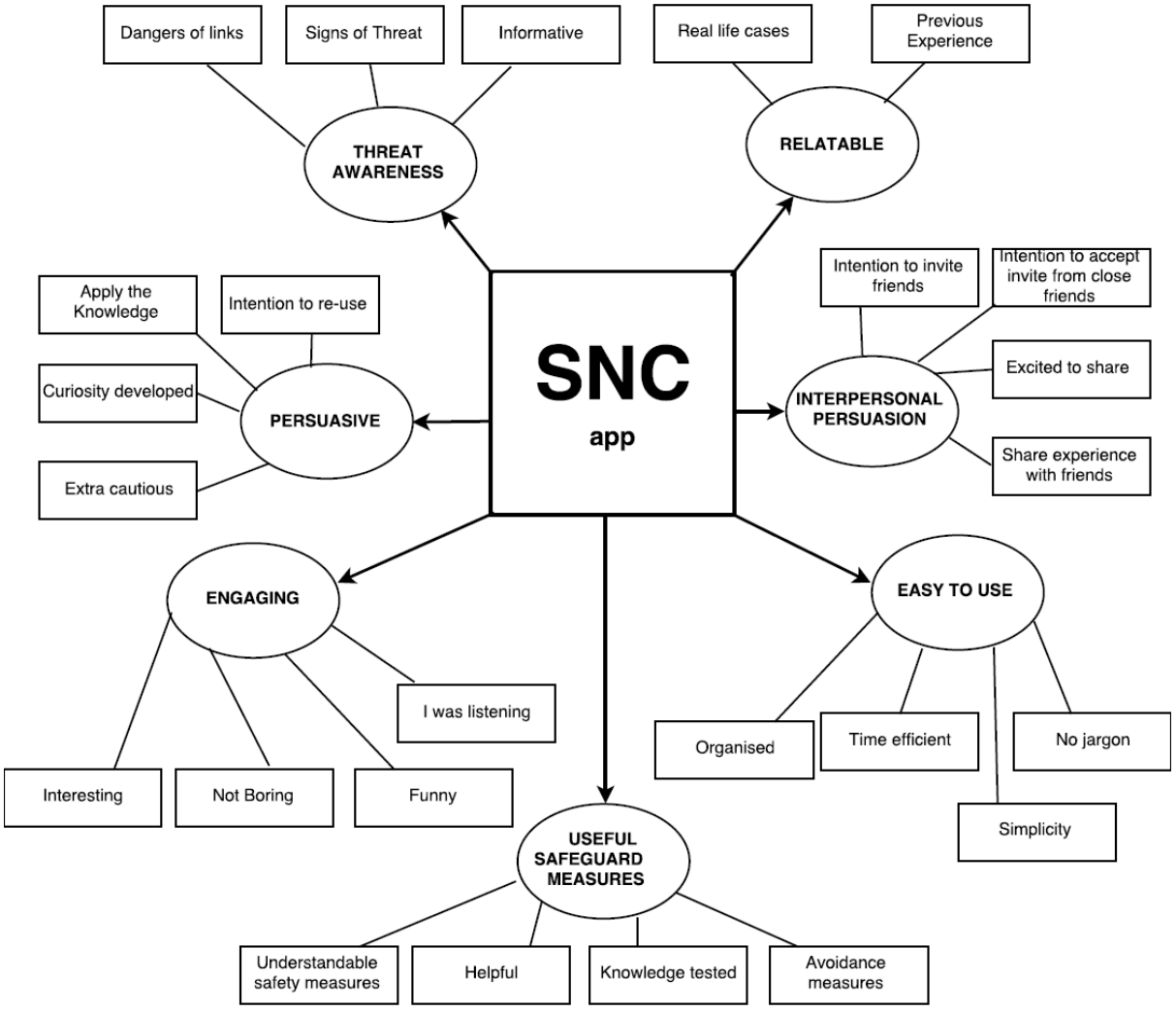

Figure 36: Final Thematic Map, Showing 7 Main Themes

Table 16: Overview of results (Final Themes and Sub-themes)

High-level themes	Sub-themes	Participants Quotes
Threat Awareness	1. Dangers of links 2. Signs of Threat 3. Informative	"The videos are good; they kinda scare you into thinking, to be more aware, and I did learn the actual signs of threat." "People can send you viruses, or like malicious links. So it's important to always be aware" ""It's an important app because you have to be aware of such risks when you are using Facebook."
Relatability	1. Real life cases 2. Previous Experience	"It iterated things I already have an idea about". "The little story really helps".

		""I think it's very useful, the real life cases idea was very good". "Telling people about the software" updates, I get that pop-up a lot. Yeah". "The cartoons are a good depiction of what could happen because with the scenarios you could understand easily what was going yeah."
Persuasion	1. Apply the Knowledge 2. Intention to re-use 3. Curiosity developed 4. Extra cautious	"It taught me a lot to be extra cautious about opening certain things". "I wouldn't mind watching another one again". "I guess I will always keep the knowledge I gained to use in the future when opening certain pages on Facebook". "It kept me wanting to listen and to find out more about cyber security". "Can you get hacked if you are using the app?
Interpersonal Persuasion	1. Intention to invite friends 2. Intention to accept invite from close friends 3. Excited to share 4. Share experience with friends	"I definitely will invite my friends to use this". It's a persuasive technique, I like the Dr and Patient form. I would definitely tell my friends about it, they are more careless than me". "I might invite my friends to watch the videos, although I expected more details". "I kinda feel my friends would find it easy to use". "I will be happy to share this information to help my friends out and fight this cause, yeah". "I would trust a close friend more if they invite me to use this than a distant friend".
Engaging	1. Interesting 2. Not Boring 3. Funny	"I thought they were very informative, but in an interesting way". "It was engaging; I was really listening and didn't find it boring so it was good".

		"Erm the animation was quite funny as well so it kept me wanting to listen".
Ease-of-use	1. Organised 2. Time efficient 3. No jargon 4. Simplicity	"I mean sheds light on things that people need to know and it's simplified. It doesn't talk too much jargon". "The message was put across very clearly". "I thought it was quite well like the way it was laid out". "Erm, it was easy to use and simple". "It was quite straightforward; I could understand what was going on". "It was well organised, and I think that the information that was set through it would help someone that needed it". "The videos were quite short and it has the information in two minutes or so, it's a good amount of time and won't bore a person and make them click next".
Useful Safeguard Measures	1. Understandable safety measures 2. Helpful 3. Knowledge tested 4. Avoidance measures	"So for me I just kind of need to be aware and what I need to do in terms of steps taken to make sure I am protecting myself correctly". "But now that I know, that if you go into a third party website and they want you to download something, you just shouldn't unless you actually check it out first". "It's a really good website to show how you can avoid them". "I think the video was quite helpful, kind of educating on malicious virus prevalent out there". "I got the questions right so it was good".

6.3.10 Analysis of Results

This study empirically evaluated the SNC app developed based on TTAT-MIP. As discussed in Chapter 5 of this thesis, the SNC app was designed to improve the security behaviour of online social network (OSN) users. To accomplish the evaluation of SNC app, a system usability scale (SUS) study, paired samples t-test and semi-structured interviews were employed. The main study employed 40 participants for the SUS study and paired samples t-tests (pre- and post-tests) while 20 participants took part in the semi-structured interview sessions.

Overall, each participant spent approximately one hour to participate in the study. In the pre-test, the average score of the participants was 30.88, and after using SNC app in the post-test, their average score was 48.83. The results from the paired samples t-tests (pre- and post-test) show a statistically significant improvement in their security behaviour on average by approximately 18 points (mean difference = 17.950). The paired samples t-test results suggest strong evidence ($p = 0.000$) that SNC intervention improves the threat avoidance behaviour of online social network users. Because the difference in scores is relatively large, it suggests that the results are not just statistically significant but practically considerable.

The results of the SUS study conducted to measure the usability of SNC app shows that the participants perceive SNC app as an advantageous tool. The SUS score of 82.9 provides substantial evidence that SNC surpassed the average usability score of 68. Also, the value of the Cronbach's alpha 0.711 provides a reliability support for the remarkable SUS score achieved.

Additionally, 20 participants gave verbal feedback on their viewpoints about the SNC app. Their responses supported the results of the paired samples t-tests and the SUS study. The participants acknowledged that the SNC app raised their awareness about malware threats in an engaging way. They appraised the story telling technique used by the SNC app and found it easy to relate with and understand. Moreover, they mentioned that they feel persuaded to apply the knowledge gained to avoid future attacks. Moreover, the results show that not only is the SNC app persuasive in changing user behaviour, it also had an interpersonal persuasive effect on the participants. Majority of the participants expressed their willingness to share the

SNC experience with their friends. Overall, the key findings from the thematic analysis suggests that the SNC app demonstrates the following 7 key themes; (1) Threat Awareness; (2) Relatable; (3) Persuasive; (4) Interpersonal persuasion; (5) Engaging; (6) Easy To Use; and (7) Useful Safeguard Measures. S**ection 6.3.11**, presents some analysis on the key themes identified in relation to TTAP-MIP.

6.3.11 Discussion of Results

In this section, the 7 key themes identified from the thematic analysis are discussed. The key themes are; (1) Threat Awareness, (2) Relatable, (3) Persuasive, (4) Interpersonal Persuasion, (5) Engaging, (6) Easy To Use, and (7) Useful Safeguard Measures.

- **Threat Awareness**

All the participants acknowledged that the SNC app increased their awareness about malware threats on OSNs. Nevertheless, it was somewhat of a surprise to find out that most of the study participants were unaware of malware threats on OSNs. Such threats are commonly distributed through malware links. According to some feedback from participants;

I don't think many people are educated when they click on the link that it could lead to something else.

"*It's scary that they can get your details "like with rose in the videos" just by clicking on a link. That's worrying, erm, is there no software that can stop these?"*

In the literature review presented in Chapter 3, we mentioned that malware threat awareness had not been given adequate attention. Organisations predominantly focus on refining the capabilities of their firewalls and anti-malware software which are solely unable to circumvent malware threats. More than often, the consequence of unawareness leads to exploitation of the biggest weakness in the cyber security landscape – humans. The videos on the SNC app demonstrated the proficiency to make users aware by provoking their thought processes. Getting OSN users to think about malware threats is a good step in the right direction to get them meticulously

conscious of every single interaction they make online. One of the participants mentioned;

"The videos are good; they kinda scare you into thinking, to be more aware, and I did learn the actual signs of threat."

Furthermore, the theme - threat awareness has a significant theoretical foundation. Recall, in chapter 4, that a key construct of TTAT-MIP which influences threat avoidance motivation is – perceived threat. Perceived severity strongly affects perceived threat. The SNC app validates this construct because most of the participants admitted their vulnerability upon discovering the dangers of carelessly downloading software through malicious links on OSNs.

According to statements of the participants;

"Erm, basically, from what I just saw, it showed me the insights into how you can easily be manipulated, like getting a virus, cause if I saw something like what the person in the video saw, I would have downloaded it".

Arguably, the findings suggest that the need to stress on the immense dangers of OSN malware threats has a huge influence on the depth of a user's security awareness. Although in other contexts it may not be the case; for example, smoking addicts simply do not quit smoking because of its associated health hazards. Other predisposing factors could influence their decision to stop smoking.

In the context of malware threats, OSN users need not just be told: "be careful of what you click". Nonetheless, they should be appraised on the core consequences of clicking a malware link, such as its short and long term downsides. By amplifying messages on the socio-technological severity of OSN malware threats, users' threat awareness could reach unprecedented depths.

- **Relatability**

Relatability describes the quality or state of being relatable. Unpredictably, some participants acknowledged this quality after watching the videos on the SNC app. According to one of the statements of study participants;

"It iterated things I already have an idea about".

A key noteworthy point in the above statement is – "iterated". Iterating an already known concept makes it relatively easy for OSN users to retain their security awareness and consequently their security behaviour. In Chapter 3, one of the limitations of existing security awareness systems identified in the literature is – lack of contextual knowledge. Contextualised awareness implies that messages on threat avoidance need to be delivered to users relative to the technology setting through which they are being exploited. A novel storytelling technique was implemented to accomplish this task. The current research adopted previous cases of OSN malware attacks and presented them to users in the form of dramatised animation videos. Such a fascinating technique was appraised by some participants because it made the security awareness information somewhat relatable to their ongoing OSN experience.

According to the participants statements;

"I think it's very useful, the real life cases idea was very good".

"The little story really helps".

From the participants' statements, it's fairly suggestive to attribute the perceived helpfulness of the SNC app to story-telling previous real life cases of OSN malware threats. By adopting a story-telling technique, the research avoided abstractly delivering security awareness messages. Reflectively, the value of relatability could be drawn from its ability to stimulate the interest of OSN users. According to a theory in IS communications - social marketing theory; a good strategy to get an audience interested in a product or service is by using recognisable and easily understandable media entities such as images/videos about the idea intended to be sold. By doing so, a pleasant setting is created for the promotion of the idea/product/service. The relatable quality of the SNC app is a useful tactic because everyday events (real life cases of OSN malware threats) are used to attach emotions to the security awareness videos.

- **Persuasive**

Persuasion describes the extent to which the SNC app influenced the participants to change their security behaviour. The study identified sub-themes such as; (1) Apply the Knowledge; (2) Intention to reuse; (3) Curiosity developed; and (4) Extra

cautious, which all provides substantial evidence to support a key construct within TTAT-MIP – avoidance behaviour.

Apply the Knowledge:

The findings show that the study participants are willing to apply the knowledge gained from SNC app to avoid OSN malware threats in the future. According to the participants' statements;

"I guess I will always keep the knowledge I gained to use in the future when opening certain pages on Facebook".

"Now that I have received the knowledge, I would definitely pass it down to other people and make them aware, people that are less tech savvy than me".

Intention to re-use:

The majority of the study participants acknowledged their intention to use the SNC app in gaining more awareness about OSN malware threats. According to the participants' statements;

"I wouldn't mind watching another one again".

"I would actually and I am not joking I would go home and use this right now".

Curiosity developed:

The findings also show that the SNC app stirred the curious instincts of the participants into seeking further information about cyber security. According to the participants' statements;

"It kept me wanting to listen and to find out more about cyber security".

"Can you get hacked if you are using the app"?

Extra cautious:

The study participants admitted that through the SNC app, they learnt the need to be extra careful when carrying out their online social networking activities. According to the participants' statements;

"It taught me a lot to be extra cautious about opening certain things".

"If I saw something like what the person in the video saw, I would have downloaded it. But now that I know, that if you go into a third party website and they want you to download something, you just shouldn't unless you actually check it out first, otherwise you will get a virus".

The sub-themes provides evidence that the SNC app was able to persuade the participants into making pronouncements to reuse the app, apply the knowledge acquired, seek further knowledge within cyber security and become extra cautious while on OSNs. In our theoretical model – TTAP-MIP, there is substantial evidence that OSN users' avoidance motivation could influence their actual avoidance behaviour. In this research context, avoidance behaviour depicts whether OSN users would develop the intention to seek awareness using the SNC app and regularly update their knowledge through the app as well. Howbeit, the persuasive nature of SNC app is found to be well-matched with the TTAT-MIP model.

- **Interpersonal Persuasion**

Almost every participant in this study showed the tendency to share their security awareness experience using the SNC app with their friends. Interpersonal persuasion defines how willing the participants are keen to invite their OSN friends to use the app for security awareness. The current research expected that the SNC app would stimulate interpersonal persuasion as our theoretical model – TTAT-MIP suggests, however, the rate which they were willing to do so surpassed expectations.

According to statements from the participants';

"I will be happy to share this information to help my friends out and fight this cause, yeah".

"I definitely will invite my friends to use this".

"I might invite my friends to watch the videos, although I expected more details".

Interpersonal persuasion that occurs within an online social network with millions of interconnected users is referred as - mass interpersonal persuasion (see chapter 3). In chapter 4, mass interpersonal persuasion was empirically validated as a construct in TTAT which influences the malware threat avoidance motivation of OSN users.

One of the significant values that interpersonal persuasion brings to the SNC app is its propensity to aid the viral distribution of security awareness videos from one OSN user to his/her connections. Although the success of mass interpersonal persuasion hinges on three key components (persuasive experience, social distribution and rapid cycle), social influence theory is a fundamental persuasion theory which supports this phenomenon.

According to Venkatesh and Brown, (2001), social influence specifies that an individual in a social network is influenced by the behaviour of members of the network to conform to community behaviour patterns. While the goal of mass interpersonal persuasion aligns with social influence theory, they both have different practical applications. Mass interpersonal persuasion is a phenomenon unique to OSN environments driven by digital technology, and social influence theory is not specific to any technology context.

Interpersonal persuasion brings tremendous benefits to the SNC app because many OSN users are more inclined to use products/services recommended by close friends. According to a statement from one of the participants';

"I would trust a close friend more if they invite me to use this than a distant friend".

No matter how well a security awareness app is designed, many OSN users may not use it unless recommended by a trusted friend. This research considers interpersonal persuasion a vital attribute of the SNC app. Therefore, the SNC app has been developed with technological features to facilitate interpersonal persuasion at scale.

Besides, the SNC app has the features for users to observe the level of security awareness of their invited friends (see chapter 5). Through this feature, it becomes relatively seamless for OSN users to access how potentially vulnerable their friends are and as such stimulate a revolutionary security culture shift.

According to one of the study participants';

It's a persuasive technique, I like the Dr and Patient form. I would definitely tell my friends about it, they are more careless than me".

The statement above is suggestive that the persuasive technique used to make OSN users aware about malware threats could be the driving force behind their motivation

to share such experience by inviting their friends. Without a persuasive experience created through story-telling of previous malware threats, it could have been somewhat unrealistic to stimulate interpersonal persuasion.

- **Engaging**

The study findings show that the participants perceived the SNC app as engaging. Engagement in this context implies how well the security awareness videos captured the attention of participants. Also, engagement in this context means that the participants learnt about OSN malware threats in a humorous manner which they did not find boring.

According to statements from some participants';

"I thought they were very informative, but in an interesting way".

"It was engaging; I was really listening and didn't find it boring so it was good".

"Erm the animation was quite funny as well so it kept me wanting to listen".

From the participants' responses, it's evident that manner security awareness was conveyed to OSN users through SNC, attracted their attention substantially. In the systematic literature review conducted in Chapter 3 of this thesis, one of the factors identified for designing effective security awareness for OSN users is – end-user engagement. Many security awareness systems reviewed in the literature solely focused on providing information to users without due consideration for active engagement. The SNC app fills this gap through the funny and exciting manner it conveys security messages through video animations.

- **Ease-of-use**

There is substantial evidence to support the ease-of-use or (easy to use) of the SNC app. In this research context, ease-of-use describes the degree to which SNC app can be used by OSN users to carry out the certain tasks. As discussed in Chapter 5, the functions within SNC include; video play; pause; like share; comments, and volume controls. In addition, it involves the feature for an automated pop-up quiz, teammate's collation and friend invitation.

According to statements of the participants';

"I mean sheds light on things that people need to know and it's simplified. It doesn't talk too much jargon".

The SNC videos were carefully scripted to avoid the use of technical jargons often associated the cyber security setting. The researcher made considerable efforts to simplify the security messages as well as the tasks to appeal to users regardless of their computing background.

According to statements of the participants';

"The message was put across very clearly".

"I thought it was quite well like the way it was laid out".

Additionally, the participants appraised the short time constraints of SNC's security awareness videos. They mentioned how straightforward the videos were organised without being boring. According to statements of the participants';

"It was quite straightforward; I could understand what was going on".

"The videos were quite short and it has the information in two minutes or so, it's a good amount of time and won't bore a person and make them click next".

"It was well organised, and I think that the information that was set through it would help someone that needed it".

Ease-of-use is found to support a construct - safeguard costs, in our theoretical model – TTAT-MIP. Safeguard costs depicts the time and effort needed to use a safety measure to avoid a malware threat on OSNs. In Chapter 4 of this thesis, we found empirical support that suggests the lower costs need to avoid a threat the higher the motivation for threat avoidance.

- **Useful Safeguard Measures**

The findings also show that the participants perceived the safeguard measures of SNC app as useful. Safeguard measures describes the steps taken to avoid a malware threat. According to the participants' statements;

"So for me I just kind of need to be aware and what I need to do in terms of steps taken to make sure I am protecting myself correctly".

"But now that I know, that if you go into a third party website and they want you to download something, you just shouldn't unless you actually check it out first".

In our theoretical model – TTAT-MIP, the construct – safeguard effectiveness provides support for this finding. OSN users always consider the perceived effectiveness of a safeguard measure before using it. The factors that affect their perception of an effective safeguard have been empirically validated which include; safeguard cost, self-efficacy and mass interpersonal persuasion.

6.3.12 Chapter Summary

This Chapter attempts to evaluate TTAT-MIP through the social network criminal (SNC) app developed to improve the malware threat avoidance behaviour of online social network (OSN) users. In Chapter 4, the research validated the extended version of the technology threat avoidance theory (TTAT-MIP) - the underlying theory that guided the development of the SNC app.

The objectives of the evaluation were;

1. To determine whether online social network users are satisfied with their experience with the SNC app.
2. To determine whether the SNC app have a significant effect on the threat avoidance behaviour of online social network users.
3. To find out whether or not the SNC app supports the constructs of TTAT-MIP.

The first objective was achieved the by conducting a system usability scale (SUS) study which measured the overall subjective satisfaction of the participants about SNC. The second objective was executed by carrying out a paired samples t-test (pre- and post-tests) which compared the average mean of the participant scores before and after they used SNC. Finally, semi-structured interviews were conducted with 20 participants to elicit feedback on the SNC app and access whether or not their responses support the constructs in our theoretical model – TTAT-MIP.

The pilot and main study results show that the participants were satisfied with the usability of SNC. Also, results from the paired samples t-test show that the threat

avoidance behaviour of the study participants significantly improved through the SNC app. Finally, the participants' verbal responses from the semi-structured interviews were analysed using thematic analysis and 7 main themes were gathered. The main themes identified were; Threat Awareness, Relatability, Persuasion, Interpersonal Persuasion, Engaging, Ease-of-use and Safeguard Effectiveness. The themes were discussed, and the findings suggest a close alignment with the theoretical model of this thesis – TTAT-MIP.

In the next Chapter, reflections about the implications of the research results reported in this thesis would be presented as well as issues of validity and reliability of the results.

Chapter 7: Discussion

7.1 Overview

This Chapter presents an overall reflection of the results from the first and second DSR iterations respectively. The chapter discusses the reliability and validity of the overall results and its general implications to theory.

7.2 Discussion of Results

The research was made up two design science studies; the first study proposed a conceptual threat avoidance model – TTAT-MIP which suggests that the malware threat avoidance motivation of OSN users are influenced by their perception of the threat (Perceived Threat) which in turn is influenced by perceived susceptibility and perceived severity. In addition, threat avoidance motivation was found to be influence by the effectiveness of the safeguard measure (Safeguard Effectiveness), the belief in their ability to avoid the threat (Self-efficacy), a low cost of using a safeguarding measure (Safeguard cost) and the mass interpersonal persuasiveness of using a safeguarding measure (MIP). To theoretically validate the model, structural equation modelling (SEM) statistical analysis technique was adopted. The results provide an estimate on the degree to which the dependent and independent variables had an effect on each other. There were no statistical evidence to support that perceived susceptibility had an influence on perceived threat ($p = 0.146$). Based on the review of the literature, OSN users are extremely susceptible to malware threats which exploit the trust users have for their interpersonal connections. Also, findings from previous studies often cite unawareness as a main cause of users' susceptibility. However, the context and extent of users' unawareness is relatively unclear due to lack of empirical support. This research have been able to expound to a certain degree the state of OSN users' unawareness regarding the subject of malware threats based on the evidence that perceived susceptibility have no effect on threat perception but perceived severity does. Suggestively, there is some level of awareness

that malware threats on OSN actually exists, nonetheless, there seem to be no awareness about how vulnerable users are to such threats.

Hypothetically, OSN security awareness needs to emphasize on the high level of users' vulnerability and not only the magnitude of the threats' consequences. A user's self-belief that he/she can be deceived or manipulated into clicking malicious links on OSNs could be a giant step in mitigating the rapid distribution of OSN malware.

The results shows statistical evidence that supports the effect of safeguard effectiveness on avoidance motivation; expected as there have been several assumptions in the literature on the need to design effective measures to protect users from on-gong threats. Nevertheless, there is lack of clarity in existing literature on the factors that makes a safeguarding measure effective. Within context of this research, the proposed a Facebook video animation application on security awareness as a safeguard measure to protect users from OSN malware threats. The choice of using a Facebook animation app was guided by previous studies which have advocated the needed for interactive multimedia systems in order to engage users actively. Moreover, the choice of integrating the application on Facebook was also founded by recommendations from the systematic literature review conducted to investigate how best to improve security awareness for OSN users.

There was statistical evidence to suggest that self-efficacy have a positive effect on threat avoidance motivation; OSN users seem to have a significant level of self-belief that they are capable of performing specific safeguarding activities to prevent a malware threat. Arguably, such belief in their abilities may somewhat affect their belief about their vulnerability to such threats. This assertion may have a few theoretical implications. Firstly, it would be important to investigate how a user's self-efficacy in applying a safeguard measure may affect their vulnerability to malware. The findings from investigations may provide alternative solutions for security practitioners when presenting their security awareness information to users. In this regards, security awareness information may stress on getting users aware of the potential dangers of their vulnerability no just to them but their connections or it may be focused on reassuring users of their inherent abilities to cope with malware threats and avoid them successfully.

Another expected finding was the negative relationship between safeguard cost and avoidance motivation. OSN users will only use a safeguarding measure when such measures cost less time, money and effort. Apparently, this result suggests that information quality is not the only factor that influences threat avoidance motivation, their threat perception. Security practitioners should endeavour to design and implement systems that that are not burdensome to use.

Mass Interpersonal Persuasion (MIP) was found to have a positive effect on avoidance motivation. Recall, in Chapter 2 of this work mentioned about the information and normative influences which constitutes the social influence theory. It is considerably logical to posit that OSN users are more normatively influenced than informatively driven security awareness. MIP principles are the underlying rules that enable third party applications to work on Facebook. Nonetheless, this research is the first to the best of my knowledge to empirically validate MIP as part of the original TTAT model.

The second iteration was conducted to practically evaluate TTAT-MIP through the proposed Facebook video animation app. Clearly, implementing the recommendation of TTAT-MIP must embody the factors needed for threat avoidance motivation of OSN users. Ensuring that the proposed Facebook video animation app strictly followed the principles of TTAT-MIP was a herculean task. At the first instance, a conceptual design framework was designed to guide the development of the app. The conceptual framework ensured that the researcher segmented the features of the app in a manner that correlates with the latent variables included within TTAT-MIP.

Although, strict design guidelines were employed to ensure the Facebook app was designed based on TTAT-MIP, a thorough evaluation process was employed to further validate TTAT-MIP practically. For the purposes of this research the Facebook app has been named – Social Network Criminal (SNC). The initial validation technique employed for SNC was an experimental design to estimate the potential effect of SNC on the threat avoidance behaviour of OSN users. Thereafter a usability study, particularly a system usability scale was employed to access users' subjective satisfaction of SNC. Lastly, a small-scale interview was conducted to elicit feedback on the overall aspects of SNC. The results of the experimental design

provide evidence to support that SNC has a significant effect on users' threat avoidance behaviour (p = 0.000). The SUS score showed a significantly higher usability level of 82.9 which suggests that SNC app is not only effective to improving users' behaviour, OSN users found system useful as well. Interestingly, the research gathered rich data from the interviews that substantiated earlier findings in the first study. According to results from a thematic analysis of the participants' feedback, SNC was found to be persuasive, interpersonal persuasive, engaging, easy to use, relatable, informative and generally useful. Reflecting back on the factors that influences the threat avoidance motivation of OSN users, recall that in the first study, safeguard cost was identified. Safeguard cost relates to the ease of use element found in the second study. Also, perceived threat relates to the informative element identified in the second study. SNC is seen to be informative due to the relatively good level of awareness it provided participants' during the experimental validation.

Furthermore, interpersonal persuasion was a key element identified by this research in the second study. Users mentioned how SNC enhanced their persuasion to invite their OSN connections, particularly the vulnerable ones to use the app to enhance their threat avoidance skills. The interpersonal persuasive element can be linked to the MIP which essentially postulates the effect of social influence on the behaviour of users connected within a social network. Overall, the findings from the interviews provided significant support for the initial empirical validation of TTAT-MIP in the first study.

7.3 Reliability and Validity of Results

To a large extent, the studies employed to execute the aim and objectives of this thesis passed validity and reliability requirements. As previously mentioned, the first study adopted the use of structural equation modelling (SEM) to test the initial hypothesis and develop the model. Convergent validity is the initial validity test for SEM analysis – it implies that the variables within the single factor are highly correlated (Savalei and Bentler, 2006). Convergent validity was evident by the factor loadings, while sufficient factor loadings depend on the sample size of the dataset

(Anderson and Gerbing, 1988). With a sample size of 285 participants used in this study, an adequate factor loading of less than 0.35 is required which was achieved.

Discriminant validity is a measure of accessing the validity of the results and is defined as the degree to which factors are distinct and uncorrelated (Anderson and Gerbing, 1988). One of the key principles of discriminant validity is that the variables should be strongly related to their own factor than any other factor. Ostensibly, there are two main methods for determining discriminant validity – pattern matrix and factor correlation matrix. In the case of the pattern matrix developed in the first study of this research, the observed variables loaded significantly on only one factor and there were no cross-loadings as seen in **Appendix B** of this work. In addition, reliability describes the consistency of the item-level errors within a single factor. In this research, the reliability was tested during the exploratory factor analysis (EFA) which computed the Cronbach's alpha for each factor. According to Gliem and Gliem, (2003), a Cronbach's alpha should have a value greater than 0.6 to be acceptable, although the values may vary based on the number of variables assigned to a given factor. In first study, all factors achieved a Cronbach's alpha value above 0.7, which suggest that there were no reliability issues.

For the second study, to determine how well the questionnaire items used in the SUS correlated with the statements concerning the concept of usability, a reliability analysis was conducted. The absolute ratings for the 10 questionnaire items were utilized to calculate the Cronbach's alpha. The value of the result achieved from the test was 0.711; this implies that there was no reliability issues associated with the SUS study. For the experimental study using a paired samples t-test, there were no validity issues as evidenced by the normal distribution of the differences between the paired values as shown in **Chapter 6**, **Figure 33**. Moreover, before choosing to analyse the data using a paired samples t-test, the researcher ensured that the data passed four validity statistical assumptions as recommended in the literature (Rietveld and van Hout, 2017). The first validity check was that the dependent variable should be measured on a continuous scale such as the scores of the participants security awareness rated from 0 – 100. Secondly, the independent variables should comprise of two categorical related groups. This implies that the same subjects would exist in both groups to ensure that each of the subjects has been measured on two instances based on the same dependent variable. Relating this

validity assumption to this research, the participants were categorised in the instance of two states; first, they were examined on their security awareness levels before using the SNC app and after using the SNC app. This makes SNC app the independent variable; and the change in their security awareness as the dependent variables. Furthermore, the third validity assumption was checked to ensure there were no significant outliers in the differences between the two related groups. For example the mean score of the participants' security awareness was 30.88 and 48.83 before and after the paired samples t-tests respectively. The existence of outliers would imply that one or two participants scored extraordinarily higher than the average mean on both instances. The last validity assumption checked, ensured that the distribution of the differences in the dependent variable between the two related groups were normally distributed. For the paired samples t-test, the normal distribution was tested using a standard QQ plot as shown in **Chapter 6**, **figure 34** of this thesis.

To ensure the validity and reliability of the thematic analysis reported in this research, a few considerations regarding issues such as theme formation, description of datasets and the nature of the analysis (inductive or deductive). The first consideration concerns technique utilised to select the appropriate themes, ideally, a theme captures something important about the data relative to the research aim and objectives. There is no hard-and fast answer to defining themes as rigid rules may not be entirely appropriate. As a result, a reasonable level of flexibility is required based on the judgement of the researcher. Within the context of this research, themes where selected based on how well they related to important areas of the developed TTAT-MIP model. For example, the theme 'relatable' was not necessarily a prevalent theme across the dataset but it captured an important element of the way users get engaged with content shared on online social networks. Another alternative technique used to ensure the validity and reliability of the thematic analysis is to provide a more detailed account of a particular theme which relates to a specific area of interest within the research. For example, the theme "interpersonal persuasion" was highly related to one of the constructs of TTAT-MIP – Mass Interpersonal Persuasion, so the researcher provided a detailed discourse on how interpersonal persuasion could actually evolve into mass interpersonal persuasion.

In addition, one of the most important validity and reliability measures used for the thematic analysis was to adopt a deductive and inductive thematic analysis approach. A deductive analysis has a tendency to be driven by the researcher's theoretical interest in the research domain; it tends to provide less rich information of the overall data and may be founded on subjective bias. To avoid such biases, a mixed thematic analysis approach was adopted to ensure quality and relevance of selected themes whilst allowing the flexibility for unforeseen themes which may not have been anticipated in the literature.

7.4 Overall Implications

Online social networks (OSNs) are designed to improve social relationships amongst the users from different parts of the world. These users share different kinds of information such as lifestyles, careers, interests, activities, and other significant information. Since the emergence of OSNs, they have been expanding exponentially and economically. Today, users of these platforms share most of their private information with the platform owners as well as third party applications. This model of information sharing and trust poses a huge risk to user privacy and security.

Arguably, the structure of OSNs is making it easier for malicious users carry out their activities without the possibility of detection. It is unfortunate considering the efforts put into the development of anti-malware softwares to curb the excesses of malware attacks. Baskerville & Rowe (2012) argue that as functionality increases in IT systems, security threats facing users' increases proportionately. However, it would be unrealistic to suggest the decrease of the features offered by OSNs in order to reduce malware attacks, since OSNs thrive on active user engagement influenced by the pleasure of using its multifarious features to interact with their connections. Therefore, there is a need for a more proactive measure to undercut these threats facing the users of OSNs. Such measures should involve effective security awareness for end-users pointing out all the threat-based activities to the user and their possible implications.

The model developed in this research has potential implications on the design and implementation of security awareness for individuals and employees working in

various organisations. When employees attend security awareness sessions and understand the concept, they will precisely get to know about web safety and online threats. Employee awareness can avoid potential risks which may have arisen in the past due to lack of proper knowledge. The IT group can identify the current and potential security concerns. They believe that the employee working for any firm/organization is the weakest link in a security breach. During Security awareness training the IT group can simulate malware attack incidents based on relatable events as suggested from the practical evaluation of TTAT-MIP, which could compel employees to think like an attacker and keep them a step ahead.

Security awareness is not only for lower and middle management, but it is also considered for senior management staff. By building a security awareness program using the TTAT-MIP model, there would be a clear and smooth security awareness interaction and persuasive knowledge sharing between lower and senior management. This approach would improve commitment from management towards a proactive and highly persuasive security culture.

Chapter 8: Conclusion

8.1 Overview

This Chapter presents the overall conclusion of the thesis. It begins by recapping how the set objectives were accomplished and also describes how the Chapters interconnect. Next, the theory and practical research contributions of this thesis are discussed. Also, the research limitations are highlighted with potential indications on how the research methodology attempted to circumvent the identified limitations. Lastly, some concluding remarks are presented and possible interesting areas of the thesis that may require further research are discussed.

8.2 Research Summary

The overall aim of this thesis was to develop an effective malware threat avoidance model for online social network (OSN) users. Although OSNs has created vast opportunities for rapid interpersonal communications and business promotions, the surge of malware threats puts individuals and organisations at enormous risk. The following objectives helped in accomplishing the research aim.

Objective 1: To understand the characteristics and threats of OSNs to establish the research domain and scope.

In Chapter 2, the overarching threat – social engineering, faced by OSN users was explored. The main reason for studying social engineering is because it embodies persuasion elements used by attackers to exploit the vulnerability of OSN users. The main persuasion factors identified in the literature include relationship forgery, psychological manipulation of humans to perform unintended actions, emotion and trust based interactions. By reviewing social engineering, specifically on its mode of

operation, the research provided a substantial high-level understanding of OSN malware threat models.

Also, a review was carried out on the nature and characteristics of OSNs. The output from the report characterised OSNs as end-user based, interactive, community driven, a platform that fosters relationships, and a platform that places value on human emotion over content. Nevertheless, a unique phenomenon – mass interpersonal persuasion (MIP) was discovered as part of the characteristics of OSNs. MIP explains how the behaviour of OSN users is influenced at a rapid pace within the shortest time through the sharing of persuasive experiences. The three key success factors of MIP articulated are persuasive experience, social distribution and rapid cycle.

Further, the medium (or vectors) through OSN users are being exploited within OSNs were described. By so doing, a good lower-level understanding of potential avenues for malware exploits was identified. The evidence in the literature suggests that OSN malware threats are often perpetuated through LikeJacking, Rogue Applications, Private Chat (Especially Facebook Chats), Bots (OSN robots), Spam Link Posts and Fake 'Friend' Connection. Also, three case studies on previous OSN malware attacks were described, and they substantiated the attack vectors as mentioned above. Remarkably, the findings suggest an alignment between the persuasion elements of social engineering and the nature and characteristics of OSNs. Such alignment makes it explicable why social engineering-based malware threats are often successfully executed through OSNs.

Objective 2: To access the limitations of security awareness systems in the literature and formulate a conceptual framework for the development of security awareness for OSN users.

In Chapter 2, a systematic literature review was carried out to investigate the state of the art of security awareness systems in the literature. Hitherto, studies by (Aloul, 2012b; Cone et al., 2007; Gao et al., 2011; Peltier, 2005; Shaw et al., 2009; Tsohou et al., 2008) recommended that in the implementation of cyber security awareness programs the factors that need to be considered include; end-user learning preference, time efficient, multimedia features, non-technical communication and

contextual approach. Therefore, these factors were used to access the review publications on security awareness systems in the current research. The findings from 15 reviewed papers suggest not much attention has been given to the development of cyber security awareness programs grounded on conceptual and empirical paradigms.

Moreover, existing security awareness programs are relatively generic in their approach and are grossly limited by their technological non-specificity in dealing with malware threats. Hence, a conceptual framework for the development security awareness systems specific to OSNs was developed as part of the contributions to the research domain.

Objective 3: To extend the technology threat avoidance theory (TTAT) by integrating mass interpersonal persuasion (MIP).

In Chapter 2, the technology threat avoidance theory (TTAT) was identified as relevant to the overall aim of the current research. TTAT suggests that computer users are motivated to avoid information technology (IT) related threats based on factors such as; perceived threat, safeguard effectiveness, safeguard costs and self-efficacy. The authors of TTAT carried out its empirical validation using anti-spyware software as their IT threat and a classroom-based awareness technique as their safeguarding measure. Though their approach for TTAT empirical validation is theoretically justifiable, it did not fit the context of our research domain.

Retrospectively, the characteristics and associated malware threats of OSNs motivated the extension of TTAT to include a construct conceptually and logically suitable to rapidly influence behavioural change. Based on the attributes of MIP and its potential capabilities the research proposed that OSN users would be motivated to avoid a malware threat if influenced by their connections. Consequently, TTAT-MIP was developed using OSN malware threats as our IT threat and a Facebook video animation app (termed – social network criminal) as the safeguarding measure.

Objective 4: To validate the extended technology threat avoidance theory (TTAT-MIP).

In Chapter 4, the research hypotheses were developed as well as the survey questionnaire items based on the uniqueness of OSN malware threats and the proposed safeguarding measure. The choice of selecting University Students as the survey population for the study was motivated by reports in the literature which suggest that people between the ages of 18-25 are most susceptible to social engineering. Structural equation modelling (SEM) was the statistical analysis technique adopted to analyse the data of 285 samples.

SEM is a combination of factor analysis and multiple regression analysis. It was adopted for this study because it allows the estimation of multiple and interrelated dependence in a single analysis. The results from our measurement model suggest that the measured variables within TTAT-MIP adequately represent the extended theory. Furthermore, the results from the structural model described how closely related the constructs of TTAP-MIP are.

The findings from the SEM analysis suggest that OSN users are motivated to avoid a malware threat based on constructs such as; perceived threat, safeguard effectiveness, safeguard costs, self-efficacy and mass interpersonal persuasion (MIP). There were two findings in the current research that contradicted TTAT; (1) Perceived Susceptibility and (2) The interaction effect between Perceived Threat and Safeguard Effectiveness. The results of the authors of TTAT suggest that Perceived Susceptibility influences Perceived Threat, on the contrary, the current research found no statistical evidence to support this. However, there is evidence in the literature that the majority of OSN users are not aware their behaviour could be susceptible to malware attacks. Therefore, the rationality of the enormous unawareness of OSN users may have attributed to the overwhelmingly non-significant effect of their perceived susceptibility.

Additionally, the current research did not find any statistical evidence that Safeguard effectiveness negatively moderates the relationship Perceived Threat and Avoidance Motivation as suggested by the authors of TTAT. The authors of TTAT argue that when computer users perceive an IT threat, they are less motivated to manage the threat if they believe their Safeguard measure is effective. This notion is based on the

nature of the Safeguard measure used by the authors of TTAT – anti-spyware software. The standpoint of the current research demonstrates that OSN users must be able to manage a malware threat which allows them the flexibility to apply safeguarding measures. Such safeguarding measure that allows OSN users to manage a malware threat is ideally a system or program that raises their security awareness. As a result of our theoretical approach in contextualising TTAT, the disparity in the findings of TTAT-MIP and TTAT are expected to exist.

Objective 5: To develop Facebook video animation security awareness app (termed - Social Network Criminal) based on TTAT-MIP.

In Chapter 5, social network criminal (SNC) was introduced and described. SNC was developed as the safeguarding measure to help OSN users avoid malware threats. To develop SNC, conceptual ideas for developing security awareness programs in the literature as well as the constructs of TTAT-MIP were considered. Further, a low level architecture in relation to TTAT-MIP was formulated which helped to order the flow of SNC's security awareness information.

At the higher level, SNC was specifically designed to exemplify the components of MIP. We adopted animation videos to ensure that the security awareness messages are delivered in a funny and exciting manner. The animation videos also ensured that message is clearly understood without distractions. The low level architecture of SNC guided the sequence of the message delivered. First, the videos explained the vulnerability of OSN users, next it described the severity of an attack, how potential threats can be detected and the video concludes by recommending useful threat avoidance techniques.

Inventively, a story-telling approach about previous incidence of social network malware attacks was used to convey the messages in the animation videos. Story-telling previous OSN malware attack incidences demonstrated the severe nature the problem. As at the time of putting this thesis together, the SNC app is still live accessible online via https://socialnetworkcriminal.com.

Objective 6: To evaluate TTAT-MIP through the SNC app using three techniques (1) Usability Study (SUS); (2) Lab experiments and (3) Semi-structured interviews.

Chapter 6 reports on the evaluation of the effectiveness of SNC in relation to the overall aim of this research using a SUS study, paired samples t-test and semi-structured interviews. The participants selected emanated from the population chosen in the initial study.

To ensure the quality and rigour in evaluation of SNC, a pilot study was carried out to access the wording of the questionnaire and also resolve any issues with SNC's interface. The pilot study provided some insights on the feasibility of the evaluation procedures and potential contingencies. The pilot study results show that SNC is usable and effective in help OSN users to avoid malware threats.

Using a convenient sample size of 40 participants, the techniques used in the pilot study were repeated for the main study. Also, a semi-structured interview was carried out to further gain insights into the effectiveness of SNC. The findings of the main study substantiated the pilot study results. Interestingly, the thematic analysis of then semi-structured interviews provided support for the SUS and paired samples t-tests results. From the thematic analysis, the key themes identified are; Threat Awareness, Relatability, Engaging, Persuasion, Inter-personal Persuasion, Ease-of-use and Safeguard Effectiveness. The themes identified best describes the major qualities of SNC from the participants' perspectives. Nevertheless, as strongly aligned the themes were with TTAT-MIP, it expatiated the significance of developing security awareness systems based on the synergy concepts and empirical theory.

In **section 8.4**, the value of the current research to theory and practice are elucidated.

8.4 Research Contribution

In this section, the research contributions are discussed relative to the challenges of the research domain.

8.4.1 Contribution to Theory

The extension of the technology threat avoidance theory (TTAT-MIP) reveals the methods researchers should adapt to investigate the impact of digital social influence on malware threat avoidance motivation. The outcome of this thesis provides new insights on users' perception of OSN malware threats. Also, the research shows the potential factors that create persuasive experiences and how it could influence mass interpersonal persuasion in the context of security awareness for OSN users.

- **Persuasive Experience and Mass Interpersonal Persuasion**

One of the significant values drawn from this research is persuasive and mass interpersonal persuasive elements that characterised the safeguarding measure – SNC app. Results from the qualitative study suggest that users find SNC app to be persuasive which aligns with a key component of MIP – persuasive experience. In this research context, persuasiveness defines how believable or convincing users find SNC. In the literature, there was no clarity on the factors that create a persuasive experience; nevertheless, two key findings from the qualitative study (Relatability and Engaging) provide a clue on the persuasiveness of SNC. Relatability describes the extent to which users could personally relate to security awareness messages delivered through SNC.

The engaging aspect of SNC also influenced its persuasiveness. In this research context, engaging describes how appealing or attractive users find the SNC app. From the qualitative study, users described the manner security awareness messages were delivered as "funny", "interesting" without any technical jargon. Such qualities made SNC appealing and consequently persuasive. From this discourse, it is,

therefore, logical to ascribe the persuasive experience of OSN users with SNC to its relatable and engaging qualities.

Furthermore, the results of the qualitative study suggest that users' willingness to invite their OSN connections to use OSN (interpersonal persuasion) was dependent on the persuasiveness of SNC. From the observations it can be inferred that it is difficult for a user to share an experience that he/she does not find persuasive. Hence, when deploying security awareness messages in an OSN context, it is not the depth or richness of information that defines users' willingness to share (interpersonal persuasion), but its persuasiveness. **Figure 33** depicts this theoretical contribution.

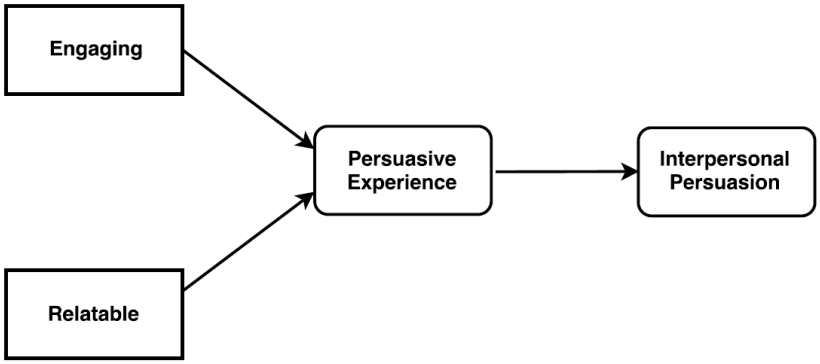

Figure 37: Relationship between persuasive experience and interpersonal persuasion

- **Users Unawareness About Their Susceptibility to OSN Malware Threats**

This research has exposed the extent to which OSN users are unaware of their susceptibility to malware threats. To a little extent, OSN users acknowledge the existence of threats on OSNs; nevertheless, the findings from the first iteration suggest their perception of invincibility to these on-going threats. As long as users feel they are not susceptible to malware, they are disposed to continue their careless online behaviour which continuously puts their devices and sensitive information at risk. In addition, when users do not feel susceptible to malware threats, they may be

less likely to make conscious efforts in gaining security awareness on ways to avoid malware threats. Consequently, researchers need to intensify efforts towards exposing the susceptibility of users in other research contexts. For example, regular ecommerce users who give permission to their Web browsers to save their credit card details are susceptible to "man in the middle" malware attacks. It is important that substantial research works are carried out to develop theories on how the perceived susceptibility of users of various online platforms could be enhanced.

- **Digital Social Influence on Malware Threat Avoidance Motivation**

Initial findings from the quantitative analysis using structural equation modelling (SEM) to validate TTAT-MIP, suggest that mass interpersonal persuasion (MIP) has a positive influence on the malware threat avoidance motivation of OSN users. In addition to its uniqueness as an OSN attribute, MIP was considered because it describes how digital social influence can stimulate a change in the behaviour of OSN users. Therefore, when conducting a study to improve users' security behaviour within a particular online platform, it is essential to consider attributes of digital social influence unique to the platform. The participants' responses from the semi-structured interviews suggest that a key attribute of digital social influence is – social distribution. Without the means to enable the interpersonal distribution of security awareness seamlessly, it becomes difficult to influence the security behaviour of a huge number of users over a short period of time. For example, studies aimed at improving the security behaviour of users on e-commerce platforms need to consider characteristics of digital social influence unique to e-commerce platforms. Such characteristics could be the ratings and reviews of each product or service listed on an e-commerce platform.

- **Users Unawareness About OSN Malware Threats**

One of the remarkable findings from the qualitative study using semi-structured interviews demonstrates the enormous level of user unawareness about OSN malware threats. Based on various discourse in the literature about malware threats of OSNs, this research initially presumed that OSN users might have a little less satisfactory level of awareness on how malware threats are distributed. However, results from the qualitative study expose how severely uninformed OSN users are;

concerning the vectors of OSN malware distribution. To the best of our knowledge, this research is the first attempt in teaching OSN users simple techniques to identify and avoid malware threats using a Facebook video animation system founded on conceptual and empirical theory. Also, the significance of malware threat awareness for OSN users helps to further alleviate the overarching research problem – social engineering-based malware attacks.

8.4.2 Contribution to Practice

The contributions of this research to industry practices would be discussed by elucidating how TTAT-MIP was adopted to conceptualise the architecture of the SNC app. Besides, this section describes how organisations can adapt the 'measured impact' component of MIP to ensure the efficient evaluation of users' engagement as well as the quality of their security awareness campaigns.

TTAT-MIP and Organisations Security Awareness Applications

TTAT-MIP is a high-level depiction of factors that need to be considered for the threat avoidance motivation of OSN users. During the development of SNC, TTAT-MIP guided the conceptualisation of the app's end-user features. Similarly, TTAT-MIP can be used as a guideline by security organisations when designing applications to raise security awareness. For example, when XYZ Company intends to build a 'game app' to help e-commerce users avoid malware threats, the implementation of the end-user features of the 'game app' can be evaluated through the constructs of TTAT-MIP. This will ensure that the 'game app' is suitably aligned with TTAT-MIP and consequently capable of helping users avoid malware threats. Besides, using TTAT-MIP as a guideline empowers security organisations to avoid including potentially irrelevant end-user features in the 'game app', thus, guarantee its efficacy.

The Measured Impact of Security Awareness Applications

One of the components of MIP is – measured impact; it describes how users' engagement on applications integrated with OSNs can be measured. In this research, we embedded automated and real-time data gathering backend scripts on the SNC app to examine the impact of our security awareness video messages. Akin to this, security organisations can adopt this approach to ensure that the impact of their security awareness campaigns is monitored at real-time. For example, at the backend, the SNC app collects data on the number of app views, video views, teammates created, security awareness ranks at real-time. Such functionality could help security organisations identify the key performance indicators and consequently upgrade weak areas in their security awareness campaigns.

Further, one of the significance of MIP for developing security awareness is its capability to ensure the rapid distribution of security messages. Moreover, security organisations can adopt the approach of the SNC app by including the functionality to measure the rapid cycle of security awareness. Recall, in Chapter 5, rapid cycle describes the time difference between the sending of invitation requests and the acceptance of invitation requests by OSN interconnected users. The lesser the time it takes for OSN users to accept an invitation request from their connections to use a security awareness app, the more likely a rapid cycle would occur. Rapid cycle of security awareness is essential to combat the exponential rate at which malware threats are distributed through OSNs.

Finally, based on the front-end measurement feature of the SNC app, security organisations could allow users' measure the security awareness levels of their connections to access how vulnerable they are to malware threats. Such possibility could be accomplished by including a security awareness ranking algorithm as demonstrated by the SNC app.

8.5 Research Limitations

This research has some limitations. First, the study demographics – University students, are less likely to provide the adequate hack value for malware attackers. In cyber security, hack value describes the extent to which potential victims are worth

targeting. Even though the literature suggests that users' within the demographics age groups are more vulnerable to social engineering attacks, the research may have had more real world impact if the SNC app was designed to raise awareness on specific threats faced by business organisations. Therefore, precautions need to be taken when generalising the overall impact of the SNC app to a wider population of OSN users.

Secondly, the items used to measure MIP may have some drawbacks. In the context of this research, MIP was measured bearing in mind its three success factors which are persuasive experience, social distribution and rapid cycle. Our persuasive experience specified in the questionnaire was a Facebook video animation app; which could pose a potential bias regarding the participants' preference for their subjective persuasive experiences (such as pop-up notifications, images or audio messages). However, the qualitative study reports suggest that majority of the participants found the SNC app as persuasive which incited their willingness to invite their friends to use the app.

Furthermore, another limitation of this research is regarding the reliability score for the MIP latent construct used during the validation of TTAT-MIP. Calculating alpha has become a normal practice in in research especially when multiple-item measures of a concept are utilised. As previously stated, Cronbach's alpha provides a measure the internal consistency of a test or scale; it is expressed as a number between 0 and 1. Internal consistency describes the degree to which all the items in a scale measures the same latent construct, as a result, it is connected to the inter-related nature of the items within the scale. As mentioned in Chapter 4 of this thesis, the Cronbach's alpha value for MIP was 0.920 (the highest amongst the latent constructs) which indicates how strongly correlated the items were correlated to each other. Nevertheless, a high value of Cronbach's alpha does not necessarily imply a high level of internal consistency because alpha is also affected by the length of the test. Therefore, the limited number of the items measuring MIP and the similar manner in which the items were worded many have slightly influenced in the high value of its Cronbach's alpha. Fundamentally, the idea of an adequate Cronbach's alpha assumes the existence of unidimensionality within the test items. According to Tavakol and Dennick, (2011), a measure is said to be unidimensional if its items measure a single latent construct. When the assumption of unidimensionality is violated, it may have a

negative effect on the reliability of the latent construct. Therefore the high alpha value of MIP should not be totally interpreted as the benchmark for its internal consistency.

8.6 Concluding Remarks and Further Work

The days are gone when Cyber security was an afterthought. Today, protecting organisations cyber ecosystem from the growing number of evolving threats external, internal, automated, socially engineered is core to running a business. It's a cyber-jungle out there and the companies do not want to be the low-hanging fruit fly! Over the recent years, online users have grown to large proportions owing to the fact that information can be sent and shared at the speed of light. This has brought the world to a global village driven by the advent of the internet of things - connected computers & servers, machines, cars, homes, retail sensors, watches, IP cameras, utility meters, and many more. According to an updated market forecast from ABI Research, over 40.9 billion connected devices are expected to be in use within five years, nearly five times the 8.7 billion connected devices recorded in 2012. That is the primary reason for a massively expanding attack surface. As a result, it is predicted that the surface area for potential cyber-attacks will grow 10 times larger from 2010 to 2020. CISCO has identified that G20 countries lose 1% of their GDP per year due to cybercrime activities.

With the popularity of software's such as Facebook, Skype, and WhatsApp which have in a way set the road map has brought up new challenges, from hackers stealing online credit cards to ClickJacking on Facebook. They have grown from old ways of just hacking the telephone for long distance calls to stealing personal information and finally credit card lending to the black market. There have been various efforts to create effective security awareness programs by platform providers and practitioners. One of the most successful methods for raising cyber security awareness is to start a campaign in order to raise awareness about the importance of cyber security.

Organisations must have a proactive, security-aware culture to be protected from cyber criminals and malware threats. Hence, the investment in a well-structured

security awareness program on how to spot and prevent malware threats is highly necessary.

The overall aim of this research was to improve the security behaviour of OSN users; this was achieved by extending the technology threat avoidance theory (TTAT) to incorporate a unique characteristic - MIP. The initial assumption in the literature was that the components of MIP are capable of changing behaviours and the quantitative and qualitative studies supported this assumption. Notwithstanding the rigorous lab experimental procedures carried out to evaluate the effectiveness of MIP, it is necessary to find out its real world in the context of security awareness. As a result, potential areas for further studies should investigate OSN users engagement with the SNC app using metrics such as; (1) the time difference between invitation and acceptance to use SNC, (2) the number of video views, app views, 'likes', 'shares' and the security awareness ranks of SNC users over a considerable period. This research proposes a field ethnographic study to undertake these tasks. SNC should be ethnographically measured with people from various geographical locations and age groups.

Moreover, the research proposes that further studies should adapt TTAT-MIP for the development of applications relevant to the threats faced by business organisations. By so doing, organisations can effectively access the level of vulnerability of their employees and ensure that persuasive security experiences are willingly distributed from one closely connected employee to the other.

A more specific future research could entail exploring other questionnaire items to measure the reliability of MIP that were apparently missed in this research work. Such items may include asking participants how they perceive a rapidly distributed security awareness app or how they would react to a security awareness app with large or few numbers of users (huge social graph). In addition, more precise studies may investigate the usability issues associated with gaining security awareness through the SNC app on a desktop or laptop computer versus a smart phone device. Finally, further studies should consider adopting a cross-sectional research approach to estimate the effect of SNC on real-world employees within various organisations, by so doing, a more improved version of TTAT-MIP specific to the security awareness challenges in an organisational setting could be developed.

References

Abraham, S. and Chengalur-Smith, I.S. (2010), "An overview of social engineering malware: Trends, tactics, and implications", *Technology in Society*, Elsevier Ltd, Vol. 32 No. 3, pp. 183–196.

Agnihotri, R., Dingus, R., Hu, M.Y. and Krush, M.T. (2013), "Social media: Influencing customer satisfaction in B2B sales", *Industrial Marketing Management*, Elsevier B.V., No. September, available at:https://doi.org/10.1016/j.indmarman.2015.09.003.

Aiken, L.S.. and West, S.G.. (2013), "Multiple Regression : Testing and Interpreting Interactions", *Journal of the Operational Research Society*, Vol. 45 No. 1, pp. 119–120.

Albesher, A. (2017), "Privacy and Security Issues in Social Networks : An Evaluation of Facebook", *IJIRST - International Conference on Latest Trends in Networking and Cyber Security*, No. March, pp. 7–10.

Algarni, A. (2013), "Social Engineering in Social Networking Sites: Phase-Based and Source-Based Models", *International Journal of E-Education, E-Business, E-Management and E-Learning*, Vol. 3 No. 6, pp. 456–462.

Aloul, F.A. (2012a), "The Need for Effective Information Security Awareness", *Journal of Advances in Information Technology*, Vol. 3 No. 3, pp. 176–183.

Aloul, F.A. (2012b), "The Need for Effective Information Security Awareness", *Journal of Advances in Information Technology*, Vol. 3 No. 3, available at:https://doi.org/10.4304/jait.3.3.176-183.

Aloul, F. a. (2012c), "The Need for Effective Information Security Awareness", *Journal of Advances in Information Technology*, Vol. 3 No. 3, pp. 176–183.

Altshuler, Y., Aharony, N., Elovici, Y., Pentland, A. and Cebrian, M. (2011), "When Criminals Become Data (or Vice Versa) prior Scientists Stealing Reality ":,

Workshop on Information in Networks, No. June 2015, pp. 3–5.

Anderson, J.C. and Gerbing, D.W. (1988), "Structural equation modeling in practice: A review and recommended two-step approach", *Psychological Bulletin*, Vol. 103 No. 3, pp. 411–423.

Anthes, G. (2012), "HTML5 leads a web revolution", *Communications of the ACM*, Vol. 55 No. 7, p. 16.

Antonakakis, M. and Perdisci, R. (2012), "From throw-away traffic to bots: detecting the rise of DGA-based malware", *Proceedings of the 21st USENIX Security Symposium*, p. 16.

Arachchilage, N.A.G. and Love, S. (2014), "Security awareness of computer users: A phishing threat avoidance perspective", *Computers in Human Behavior*, Elsevier Ltd, Vol. 38, pp. 304–312.

Arguel, A. and Jamet, E. (2009), "Using video and static pictures to improve learning of procedural contents", *Computers in Human Behavior*, Elsevier Ltd, Vol. 25 No. 2, pp. 354–359.

B. Kim, E. (2014), "Recommendations for information security awareness training for college students", *Information Management & Computer Security*, Vol. 22 No. 1, pp. 115–126.

Bada, M. (2014), "Cyber Security Awareness Campaigns Why do they fail to change behaviour ?", *Global Cyber Security Capacity Centre: Draft Working Paper*, No. July.

Baltazar, J., Costoya, J. and Flores, R. (2009), "The real face of koobface: The largest web 2.0 botnet explained", *Trend Micro Research*, Vol. 5 No. 9, p. 10.

Bangor, A., Kortum, P.T. and Miller, J.T. (2008), "An empirical evaluation of the system usability scale", *International Journal of Human-Computer Interaction*, Vol. 24 No. 6, pp. 574–594.

Bapna, R., Gupta, A., Rice, S., Wendell, O. and Sr, H. (2017), "Trust and the Strength of Ties in Online Social Networks: An Exploratory Field Experiment", *MIS Quarterly*, Vol. 41 No. 1, pp. 115–130.

Barriball, L. and While, A. (1994), “Collecting data using a semi???structured interview: a discussion paper”, *Journal of Advanced Nursing*, Vol. 19 No. 2, pp. 328–335.

Baskerville, R.L. and Myers, M.D. (2002), “Information Systems As A Reference Discipline”, *Mis Quarterly*, Vol. 35 No. 4, pp. 859–881.

Bearden, W.O., Netemeyer, R.G., Teel, J.E., Bearden, W., Netemeyer, R.G. and Teel, J.E. (1989), “Measurement of Consumer Susceptibility to Interpersonal Influence Linked references are available on JSTOR for this article : Measurement of Consumer Susceptibility to Interpersonal Influence”, *Journal of Consumer Research*, Vol. 15 No. 4, pp. 473–481.

Betrancourt, M. (2005), “The Animation and Interactivity Principles in Multimedia Learning”, *The Cambridge Handbook of Multimedia Learning*, pp. 287–296.

Beye, M., Jeckmans, a J.P., Erkin, Z., Hartel, P.H., Lagendijk, R.I. and Tang, Q. (2010), “Literature Overview - Privacy in Online Social Networks”, *Information Security*, No. TR-CTIT-10-36, pp. 1–19.

Boshmaf, Y., Muslukhov, I., Beznosov, K. and Ripeanu, M. (2012), “Design and analysis of a social botnet”, *Computer Networks*, Vol. 57, pp. 556–578.

Braun, R. and Esswein, W. (2012), “Corporate Risks in Social Networks–Towards a Risk Management Framework”, *18th Americas Conference on Information Sysrems*, pp. 1–12.

Brooke, J., Jordan, P.W., Thomas, B., Weerdmeester, B.A. and McClelland, I.L. (1996), “SUS: A quick and dirty usability scale.”, *Redhatch Consulting Ltd*, pp. 189–194.

Bullee, J.W.H., Montoya, L., Pieters, W., Junger, M. and Hartel, P.H. (2015), “The persuasion and security awareness experiment: reducing the success of social engineering attacks”, *Journal of Experimental Criminology*, Vol. 11 No. 1, pp. 97–115.

Cao, C. and Caverlee, J. (2014), “Behavioral detection of spam URL sharing: Posting patterns versus click patterns”, *ASONAM 2014 - Proceedings of the 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis*

and Mining, No. Asonam, pp. 138–141.

Carman, A. (2014), "Study: Malicious social media attacks on the upswing - SC Magazine", *Scmagazine*, available at: http://www.scmagazine.com/social-media-managers-and-it-security-professionals-to-work-together-in-2015/article/387964/ (accessed 23 July 2015).

Cazenave, F., Quint, V. and Roisin, C. (2011), "Timesheets . js : When SMIL Meets HTML5 and CSS3 To cite this version ":, *11th ACM Symposium on Document Engineering*.

Cederholm, D. (2010), *Css3 for Web Designers*, *International Journal of Human-Computer Studies*, Vol. 64, available at:https://doi.org/10.1016/j.ijhcs.2006.06.002.

Centola, D. (2010), "The Spread of Behavior in an Online Social Network Experiment", *Science*, Vol. 329 No. 5996, pp. 1194–1197.

Chaabane, A., Ding, Y., Dey, R., Kaafar, M.A., Chaabane, A., Ding, Y., Dey, R., et al. (2014), "A Closer Look at Third-Party OSN Applications : Are They Leaking Your Personal Information ?", *In International Conference on Passive and Active Network Measurement (Pp. 235-246). Springer International Publishing.*, pp. 235–246.

Cheung, C.M.K., Chiu, P.Y. and Lee, M.K.O. (2011), "Online social networks: Why do students use facebook?", *Computers in Human Behavior*, Elsevier Ltd, Vol. 27 No. 4, pp. 1337–1343.

Chia-Ying, L. (2013), "Persuasive messages on information system acceptance - social influence theory.pdf", *Computers in Human Behavior*, Vol. 29 No. January, 2013, pp. 264–275.

Chin, W.W., Marcolin, E. and Newsted, P.R. (2003), "A partial least squares latent variable modeling approach for measuring interaction effects: results from a Monte Carlo simulation study and an electronic mail emotion/ adoption study", *Information System Research*, Vol. 14 No. 2, pp. 189–217.

Chung, N. and Han, H. (2016), "The relationship among tourists' persuasion, attachment and behavioral changes in social media", *Technological Forecasting*

and Social Change, Elsevier Inc., available at:https://doi.org/10.1016/j.techfore.2016.09.005.

Cimpanu, C. (2016), "Malware Spread via Facebook Makes 10,000 Victims in 48 Hours", *Http://news.softpedia.com/news/*, available at: http://news.softpedia.com/news/malware-spread-via-facebook-makes-10-000-victims-in-48-hours-505969.shtml (accessed 30 May 2017).

Compeau, D.R. and Higgins, C.A. (1995), "Computer Self-Efficacy : Development of a Measure and Initial Test Development of a", *MIS Quarterly*, Vol. 19 No. 2, pp. 189–211.

Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D. (2007), "A video game for cyber security training and awareness", *Computers and Security*, Vol. 26 No. 1, pp. 63–72.

Conole, G., Galley, R. and Culver, J. (2008), "Social Network Sites: Definition, History, and Scholarship", *Journal of Computer-Mediated Communication*, Vol. 13 No. 1, pp. 119–138.

Converse, T., Park, J. and Morgan, C. (2004), *PHP5 and MySQL Bible*, Wiley Publishing.

Cooligan, H. (2004), *Research Methods and Statistics in Psychology*, 4th ed. Lo., Hodder and Stoughton, available at: https://numerons.files.wordpress.com/2012/04/research-methods-and-statistics-in-psychology.pdf.

Creswell, J.W. (2007a), "Research Design: Qualitative, Quantitative and Mixed Method Aproaches", *SAGE Publications*, pp. 203–223.

Creswell, J.W. (2007b), "Chapter 3: Designing a Qualitative Study", *Qualitative Inquiry and Research Design: Choosing among Five Approaches*, pp. 35–41.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79–98.

Das, A. and Khan, H.U. (2016), "Security behaviors of smartphone users",

Information and Computer Security, Vol. 24 No. 1, pp. 116–134.

Davis, F.D. (1989), "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of", *MIS Quarterly*, Vol. 13 No. 3, p. 319–340.

Davis, F.D., Bagozzi, R.P. and Warshaw, P.R. (1989), "User Acceptance of Computer Technology : A Comparison of Two Theoretical Models Author (s): Fred D . Davis , Richard P . Bagozzi and Paul R . Warshaw Published by : INFORMS Stable URL : http://www.jstor.org/stable/2632151 REFERENCES Linked references ar", *Management Science*, Vol. 35 No. 8, pp. 982–1003.

Dawes, J. (2008), "Do data characteristics change according to the number of scale points used? An experiment using 5-point, 7-point and 10-point scales", *International Journal of Market Research*, Vol. 50 No. 1, pp. 61–77.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006), "Why Phishing Works", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 581–590.

Diffley, S. and Kearns, J. (2011), "Consumer behaviour in social networking sites: implications for marketers", *Irish Journal Of …*, pp. 47–66.

Dunlop, S., Freeman, B. and Jones, S.C. (2016), "Marketing to Youth in the Digital Age: The Promotion of Unhealthy Products and Health Promoting Behaviours on Social Media", *Media and Communication*, Vol. 4 No. 3, pp. 2183–2439.

Egelman, S., Cranor, L.F. and Hong, J. (2008), "You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings", *Proceeding of the Twenty-Sixth Annual CHI Conference on Human Factors in Computing Systems - CHI '08*, p. 1065.

Elliott, B. (2008), "Anything is possible: Managing feature creep in an innovation rich environment", *IEEE International Engineering Management Conference*, pp. 304–307.

Faghani, M.R., Matrawy, A. and Lung, C.H. (2012), "A study of Trojan propagation in online social networks", *2012 5th International Conference on New Technologies, Mobility and Security - Proceedings of NTMS 2012 Conference and Workshops*, pp. 6–10.

Faghani, M.R. and Saidi, H. (2009a), “Malware propagation in online social networks”, *2009 4th International Conference on Malicious and Unwanted Software, MALWARE 2009*, No. Grossman 2006, pp. 8–14.

Faghani, M.R. and Saidi, H. (2009b), “Malware propagation in online social networks”, *2009 4th International Conference on Malicious and Unwanted Software, MALWARE 2009*, pp. 8–14.

Fan, W. and Yeung, K.H. (2010), “Online social networksParadise of computer viruses”, *Physica A: Statistical Mechanics and Its Applications*, Elsevier B.V., Vol. 390 No. 2, pp. 189–197.

Fereday, J. and Muir-Cochrane, E. (2006), “Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development”, *International Journal of Qualitative Methods*, Vol. 5 No. 1, pp. 80–92.

Ferreira, A., Coventry, L. and Lenzini, G. (2015), “Principles of Persuasion in Social Engineering and Their Use in Phishing”, *Springer International Publishing Switzerland*, Vol. 9190, pp. 36–47.

Fischer, R.J., Halibozek, E.P., Walters, D.C., Iannone, R.B., Long, L.E., Opolot, J.S.E., Rennard, C., et al. (2013), “Introduction to Security”, *Cengage Learning*, pp. xv–xvi.

Fogg, B. (2009), “A behavior model for persuasive design”, *Proceedings of the 4th International Conference on Persuasive Technology - Persuasive ’09*, p. 1.

Fogg, B.J. (2008), “Mass Interpersonal Persuasion : An Early View of a New Phenomenon”, *Springer Berlin Heidelberg.*, No. 2008, pp. 23–34.

Fornell, C. and Larcker, D. (1981), “Evaluating structural equation models with unobservable variables and measurement error”, *Journal of Marketing Research*, Vol. 18 No. 3, pp. 39–50.

Foster, D., Blythe, M., Lawson, S. and Doughty, M. (2009), “Social networking sites as platforms to persuade behaviour change in domestic energy consumption”, *Communication*.

Frøkjær, E., Hertzum, M. and Hornbæk, K. (2000), "Measuring Usability : Are Effectiveness , Efficiency , and Satisfaction Really Correlated ?", *ACM CHI 2000 Conference on Human Factors in Computing Systems*, Vol. 2 No. 1, pp. 345–352.

Furnell, S.M. (2010), "Online identity: Giving it all away?", *Information Security Technical Report*, Vol. 15 No. 2.

Gallagher, S. (2015), "Syrian rebels lured into malware honeypot sites through 'sexy' online chats", *Arstechnica.co.uk/information-Technology/*, available at: https://arstechnica.co.uk/information-technology/2015/02/syrian-rebels-lured-into-malware-honeypot-sites-through-sexy-online-chats/ (accessed 30 May 2017).

Gao, H., Hu, J., Huang, T., Wang, J. and Chen, Y. (2011), "Security issues in online social networks", *IEEE Internet Computing*, Vol. 15 No. 4, pp. 56–63.

Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y. and Zhao, B.Y. (2010), "Detecting and characterizing social spam campaigns", *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, pp. 35–47.

Gefen, D., Straub, D.W. and Boudreau, M.-C. (2000a), "Structural Equation Modeling and Regression : Guidelines for Research Practice", *Communications of the Association for Information Systems*, Vol. 4 No. October, p. 7.

Gefen, D., Straub, D.W. and Boudreau, M.-C. (2000b), "Structural Equation Modeling and Regression : Guidelines for Research Practice", *Communications of the Association for Information Systems*, Vol. 4 No. October, p. 7.

Gliem, J.A. and Gliem, R.R. (2003), "Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales", *Midwest Research to Practice Conference in Adult, Continuing, and Community Education*, No. 1992, pp. 82–88.

Gold, S. (2010), "Social engineering today: psychology, strategies and tricks.", *Network Security*, Vol. 11 No. 14.

Gragg, D. (2001), "A Multi-Level Defense Against Social Engineering", *Information Security*, p. 18.

Gritzalis, D., Kandias, M., Stavrou, V. and Mitrou, L. (2014), "History of Information: The case of Privacy and Security in Social Media", available at: http://www.cis.aueb.gr/Publications/INFOHIST-2014 Legal Publications.pdf.

Guo, H., Cheng, H.K. and Kelley, K. (2016), "Impact of Network Structure on Malware Propagation: A Growth Curve Perspective.", *Journal of Management Information Systems*, Routledge, Vol. 33 No. 1, pp. 296–325.

Gupta, S., Singhal, A. and Kapoor, A. (2017), "A literature survey on social engineering attacks: Phishing attack", *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, pp. 537–540.

Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E. (1998), *Multivariate Data Analysis: A Global Perspective*, *Psychometrika*.

Hair, J.F., Ringle, C.M. and Sarstedt, M. (2013), "Partial Least Squares Structural Equation Modeling: Rigorous Applications, Better Results and Higher Acceptance", *Long Range Planning*, Vol. 46 No. 1–2, pp. 1–12.

Hampton, K., Goulet, L.S., Rainie, L. and Kristen, P. (2011), "Social networking sites and our lives | Pew Research Center", *Http://www.pewinternet.org*, available at: http://www.pewinternet.org/2011/06/16/social-networking-sites-and-our-lives/ (accessed 19 February 2017).

Harris, D.M. and Guten, S. (1979), "Health-Protective Behavior : An Exploratory Study", *Journal of Health and Social Behavior*, Vol. 20 No. 1, pp. 17–29.

Heartfield, R. and Loukas, G. (2015), "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks", *ACM Computing Surveys (CSUR)*, Vol. 48 No. 3, pp. 1–39.

Heinrich, C. (2011), "Secure Socket Layer (SSL)", *Encyclopedia of Cryptography and Security*, No. 1996, pp. 1135–1139.

Hevner, A.R., March, S.T., Park, J., Ram, S. and Ram, S. (2004), "Design Science in Information Systems Research", *MIS Quarterly*, Vol. 28 No. 1, pp. 75–105.

Hevner, a. R., March, S.T. and Park, J. (2004), "Design Science in Information

Systems Research", *MIS Quarterly*, Vol. 28 No. 1, pp. 75–105.

Hong, J. (2012), "The currentsState of phishing attacks", *Communications of the ACM*, Vol. 55 No. 1, pp. 74–81.

Hove, S.E. and Anda, B. (2005), "Experiences from conducting semi-structured interviews in empirical software engineering research", *International Software Metrics Symposium*, pp. 203–212.

Hu, L. and Bentler, P.M. (1999), "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives", *Structural Equation Modeling: A Multidisciplinary Journal*, Vol. 6 No. 1, pp. 1–55.

Hutter, K., Hautz, J., Dennhardt, S. and Füller, J. (2013), "The impact of user interactions in social media on brand awareness and purchase intention: The case of MINI on Facebook", *Journal of Product and Brand Management*, Vol. 22 No. 5, pp. 342–351.

Ikhalia, E. and Arreymbi, J. (2014), "Online Social Networks: A Vehicle for Malware Propagation", *13th European Conference on Cyber Warfare and Security The University of Pi Piraeus Greece 3-4 July 2014*, No. July, p. 326.

Ikhalia, E. and Serrano, A. (2015), "A Framework for Designing an Effective Security Awareness System for Online Social Network Users", *European, Mediiterranean & Middle Eastern Conference on Information Systems*, Vol. 2015, pp. 1–16.

Ikhalia, E. and Serrano, A. (2016), "Developing a New Model for the Avoidance of Malware Threats through Online Social Networks", *15th International Conference WWW/Internet 2016*.

Ikhalia, E.J. (2013), "A New Social Media Security Model (SMSM)", *International Journal of Emerging Technology and Advanced Engineering*, Vol. 3 No. 7, pp. 3–8.

Inayat, Z., Gani, A., Anuar, N.B., Anwar, S. and Khan, M.K. (2017), "Cloud-Based Intrusion Detection and Response System: Open Research Issues, and Solutions", *Arabian Journal for Science and Engineering*, Vol. 42 No. 2, pp. 399–423.

Jalote, P., Palit, A. and Kurien, P. (2004), "The Timeboxing Process Model for Iterative Software Development", *Advances in Computers*, Vol. 62 No. C, pp. 67–103.

Jin, L., Chen, Y., Wang, T., Hui, P. and Vasilakos, a V. (2013), "Understanding user behavior in online social networks: a survey", *Communications Magazine, IEEE*, Vol. 51 No. 9, pp. 144–150.

Kaiser, H.F. (1974), "An Index of Factorial Simplicity", *Psychometrika*, Vol. 39 No. 1, pp. 31–36.

Kaplan, B.B.B. and Duchon, D. (1988), "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study.", *MIS Quarterly*, Vol. 12 No. 4, pp. 571–586.

kaspersky. (2015), "Zeus Trojan Malware Threat | Zbot and Other Names | Kaspersky Lab UK", *Www.kaspersky.co.uk*, available at: https://www.kaspersky.co.uk/resource-center/threats/zeus-trojan-malware (accessed 30 May 2017).

Katsikas, S.K. (2000), "Health care management and information systems security: awareness, training or education?", *International Journal of Medical Informatics*, Vol. 60 No. 2, pp. 129–135.

Kietzmann, J.H., Hermkens, K., McCarthy, I.P. and Silvestre, B.S. (2011), "Social media? Get serious! Understanding the functional building blocks of social media", *Business Horizons*, "Kelley School of Business, Indiana University", Vol. 54 No. 3, pp. 241–251.

Kirscht, J.P., Haefner, D.P., Kegeles, S. and Rosenstock, I.M. (1966), "A National Study of Health Beliefs", *American Sociological Association*, Vol. 7 No. 4, pp. 248–254.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015), "Advanced social engineering attacks", *Journal of Information Security and Applications*, Elsevier Ltd, Vol. 22, pp. 113–122.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. (2007), "Protecting people from phishing: the design and evaluation of an embedded

training email system", *Proceedings of ACM CHI 2007 Conference on Human Factors in Computing Systems*, Vol. 1, pp. 905–914.

Labuschagne, W.A., Burke, I., Veerasamy, N. and Eloff, M.M. (2011), "Design of cyber security awareness game utilizing a social media framework", *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*, available at:https://doi.org/10.1109/ISSA.2011.6027538.

Lee, D., Hosanagar, K. and Nair, H.S. (2014), "The Effect of Social Media Marketing Content on Consumer Engagement: Evidence from Facebook.", *Working Papers (Faculty) -- Stanford Graduate School of Business*, No. Summer 2013, pp. 1–51.

Legris, P., Ingham, J. and Collerette, P. (2003), "Why do people use information technology? A critical review of the technology acceptance model", *Information & Management*, Vol. 40 No. 3, pp. 191–204.

Liang, H. and Xue, Y. (2009), "Avoidance of Information Technology Threats: A Theoretical Perspective", *MIS Quarterly*, Vol. 33 No. 1, pp. 71–90.

Liang, H. and Xue, Y. (2010), "Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective", *Journal of the Association for InformationTechnology*, Vol. 11 No. 7, pp. 394–413.

Likert, R. (1967), "The method of constructing and attitude scale", *Methods and Trchniques in Business Research*.

Lin, K.Y. and Lu, H.P. (2011a), "Why people use social networking sites: An empirical study integrating network externalities and motivation theory", *Computers in Human Behavior*, Elsevier Ltd, Vol. 27 No. 3, pp. 1152–1161.

Lin, K.Y. and Lu, H.P. (2011b), "Why people use social networking sites: An empirical study integrating network externalities and motivation theory", *Computers in Human Behavior*, Vol. 27 No. 3, pp. 1152–1161.

Luo, W., Liu, J., Liu, J. and Fan, C. (2009), "An analysis of security in social networks.", *In Dependable, Autonomic and Secure Computing 2009. DASC'09. Eighth IEEE International Conference*, pp. 648–651.

Luo, X., Brody, R., Seazzu, A. and Burd, S. (2011), "Social Engineering", *Information*

Resources Management Journal, Vol. 24 No. 3, pp. 1–8.

Makridakis, A., Athanasopoulos, E., Antonatos, S., Antoniades, D., Ioannidis, S., & Markatos, E.P. (2010), "Understanding the behavior of malicious applications in social networks", *IEEE Network*, Vol. 24 No. 5.

March, S.T. and Smith, G.F. (1995), "Design and natural science research on information technology", *Decision Support Systems*, Vol. 15 No. 4, pp. 251–266.

McClendon, D. (2012), "Perceived susceptibility of cardiovascular disease as a moderator of relationships between perceived severity and cardiovascular health promoting behaviors among female registered nurses.", *Dissertation Abstracts International: Section B: The Sciences and Engineering*, Vol. 72 No. 7–B, p. 3955.

Micro, T. (2015), "Social media malware on the rise", *Blog.trendmicro.com/*, available at: http://blog.trendmicro.com/social-media-malware-on-the-rise/ (accessed 4 June 2015).

Mingers, J. (2001), "Combining IS research methods: Towards a pluralist methodology", *Information Systems Research*, Vol. 12 No. 3, pp. 240–259.

Mislove, A., Marcon, M., Gummadi, K.P., Druschel, P. and Bhattacharjee, B. (2007), "Measurement and analysis of online social networks", *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement (IMC)*, pp. 29–42.

Mohammed, S. and Apeh, E. (2016), "A Model for Social Engineering Awareness Program for Schools", *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA) A*, pp. 392–397.

Moore, T. and Clayton, R. (2015), "Which malware lures work best? Measurements from a large instant messaging worm", *eCrime Researchers Summit, eCrime*, Vol. 2015–June No. June, available at:https://doi.org/10.1109/ECRIME.2015.7120801.

Myers, M. (1997), "Qualitative research in information systems", *Management Information Systems Quarterly*, Vol. 21 No. June, pp. 1–18.

Mylonas, A., Kastania, A. and Gritzalis, D. (2013), "Delegate the smartphone user? Security awareness in smartphone platforms", *Computers and Security*, Vol. 34, pp. 47–66.

Neal, R.W. (2013), "Facebook Virus: 'Zeus' Malware Steals Passwords And Drains Bank Accounts, Thrives On Social Network", *Http://www.ibtimes.com/facebook-Virus-Zeus-Malware-Steals-Passwords-Drains-Bank-Accounts-Thrives-Social-Network-1294881*, available at: http://www.ibtimes.com/facebook-virus-zeus-malware-steals-passwords-drains-bank-accounts-thrives-social-network-1294881 (accessed 27 July 2015).

Nelms, T., Perdisci, R., Antonakakis, M. and Ahamad, M. (2016), "Towards Measuring and Mitigating Social Engineering Software Attacks", *USENIX Security Symposium*, pp. 773–789.

Ng, B.Y., Kankanhalli, A. and Xu, Y. (Calvin). (2009), "Studying users' computer security behavior: A health belief perspective", *Decision Support Systems*, Elsevier B.V., Vol. 46 No. 4, pp. 815–825.

Nunnally, J.C. (1975), "Psychometric Theory 25 Years Ago and Now", *Educational Researcher*, Vol. 4 No. 10, pp. 7–21.

Oates, B. (2006), *Researching Information Systems and Computing*, Sage.

Odaci, H. and Çelik, Ç.B. (2016), "Does internet dependence affect young people's psycho-social status? Intrafamilial and social relations, impulse control, coping ability and body image", *Computers in Human Behavior*, Vol. 57, pp. 343–347.

Olusegun, O.J. and Ithnin, N.B. (2013), "' People Are the Answer to Security ':", *Ijcsis*, Vol. 11 No. 8, pp. 57–65.

Onwuegbuzie, A.J. and Leech, N.L. (2004), "Post Hoc Power: A Concept Whose Time Has Come", *Understanding Statistics*, Vol. 3 No. 4, pp. 201–230.

Paganini, P. (2015), "AV-TEST estimates 12 million new malware variants per monthSecurity Affairs", *Securityaffairs*, available at: http://securityaffairs.co/wordpress/32352/malware/av-test-statistics-2014.html (accessed 13 April 2017).

Pahnila, S., Siponen, M. and Mahmood, A. (2007), "Employees' behavior towards IS security policy compliance", *Proceedings of the Annual Hawaii International Conference on System Sciences*, No. April, available at:https://doi.org/10.1109/HICSS.2007.206.

Pawade, D., Lahigude, A. and Reja, D. (2015), "Review Report On Security Breaches Using Keylogger And", *International Journal of Advance Foundation and Research in Computer (IJAFRC)*, Vol. 2 No. January, pp. 55–59.

Peltier, T.R. (2005), "Implementing an Information Security Awareness Program", *Security Management Practices*, Vol. 33 No. June 2015, pp. 1–18.

Penni, J. (2017), "The future of online social networks (OSN): A measurement analysis using social media tools and application", *Telematics and Informatics*, Elsevier Ltd, Vol. 34 No. 5, pp. 498–517.

Prestaasen, B. (2011), "Improving Security Awareness and Ownership using a method based on Action Research", pp. 1–106.

Provos, N., Mcnamee, D., Mavrommatis, P., Wang, K. and Modadugu, N. (2007), "The Ghost In The Browser Analysis of Web-based Malware", *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets*, Vol. 462, p. 4.

Puhakainen, P. (2006), *A Design Theory for Information Security Awareness*, *Processing*, available at: http://en.scientificcommons.org/13922630.

Rahman, S., Huang, T.K., Madhyastha, H. V. and Faloutsos, M. (2016), "Detecting Malicious Facebook Applications", *IEEE/ACM Transactions on Networking*, Vol. 24 No. 2, pp. 773–787.

Rezgui, Y. and Marks, A. (2008), "Information security awareness in higher education: An exploratory study", *Computers & Security*, Elsevier Ltd, Vol. 27 No. 7–8, pp. 241–253.

Rietveld, T. and van Hout, R. (2017), "The paired t test and beyond: Recommendations for testing the central tendencies of two paired samples in research on speech, language and hearing pathology", *Journal of Communication Disorders*, Elsevier, Vol. 69 No. July, pp. 44–57.

Robertson, M., Pan, Y. and Yuan, B. (2010), "A social approach to security: Using social networks to help detect malicious web content", *Intelligent Systems and Knowledge Engineering (ISKE), 2010 International Conference on*, pp. 436–441.

Romera, R. (2010), "Discerning Relationships: The Mexican Botnet Connection", *Trend Micro Research*, No. September, pp. 1–34.

Rosenstock IM, Strecher VJ, B.M. (1988), "Social learning theory and the Health Belief Model.", *Health Education Quarterly.. Q.*, Vol. 15 No. 2, pp. 175–83.

Rößling, G. and Müller, M. (2009), "Social engineering: A serious underestimated problem", *Proceedings of the Conference on Integrating Technology into Computer Science Education, ITiCSE*, No. April, p. 384.

Safa, N.S., Solms, R. Von and Futcher, L. (2016), "Human aspects of information security in organisations", *Computer Fraud and Security*, Elsevier Ltd, Vol. 2016 No. 2, pp. 15–18.

Sanzgiri, A., Joyce, J. and Upadhyaya., S. (2012), "The early (tweet-ing) bird spreads the worm: An assessment of twitter for malware propagation", *Procedia Computer Science*.

Sanzgiri, A., Joyce, J. and Upadhyaya, S. (2012), "The early (tweeting) Bird spreads the worm: An assessment of twitter for malware propagation", *Procedia Computer Science*, Vol. 10, pp. 705–712.

Savalei, V. and Bentler, P.M. (2006), "Structural Equation Modeling", *Handbook of Marketing Research: Uses, Misuses, and Future Advances*, pp. 330–364.

Schaab, P., Beckers, K. and Pape, S. (2017), "Social Engineering Defence Mechanisms and Counteracting Training Strategies", *Information and Computer Security*, Vol. 25 No. 2, p. ICS-04-2017-0022.

Schnotz, W. and Lowe, R. (2003), "External and internal representations in multimedia learning", *Learning and Instruction*, Vol. 13 No. 2, pp. 117–123.

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.-J. (2009), "The impact of information richness on information security awareness training effectiveness",

Computers & Education, Elsevier Ltd, Vol. 52 No. 1, pp. 92–100.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J. (2010), "Who falls for phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions", *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10*, pp. 373–382.

Sheng, S. and Magnien, B. (2007), "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish", *In Proceedings of SOUPS 2007*, pp. 88–99.

Shrivastava, A., Sharma, M.K. and Marimuthu, P. (2018), "Internet addiction at workplace and it implication for workers life style: Exploration from Southern India", *Asian Journal of Psychiatry*, Elsevier, Vol. 32 No. November 2017, pp. 151–155.

Smith, S.D. (2016), "InfoSec Reading Room Catching Flies : A Guide to the Various Flavors of", *SANS Institute*, Vol. 1 No. 1, p. 30.

Sniehotta, F.F., Presseau, J. and Araújo-Soares, V. (2014), "Time to retire the theory of planned behaviour", *Health Psychology Review*, Taylor & Francis, Vol. 8 No. 1, pp. 1–7.

Sohrabi Safa, N., Von Solms, R. and Furnell, S. (2016), "Information security policy compliance model in organizations", *Computers and Security*, Elsevier Ltd, Vol. 56, pp. 1–13.

Solutions, S. (2017), "Paired Sample T-Test", *Statistics Solutions*, available at: http://www.statisticssolutions.com/manova-analysis-paired-sample-t-test/ (accessed 13 April 2017).

Sood, A.K. (2011), "Chain Exploitation — Social Networks Malware", *ISACA Journal*, Vol. 1, pp. 1–6.

Statista. (2016a), "Number of monthly active Facebook users worldwide as of 4th quarter 2016 (in millions)", *https://www.statista.com/statistics/264810/number-of-Monthly-Active-Facebook-Users-Worldwide/*, available at: https://www.statista.com/statistics/264810/number-of-monthly-active-

facebook-users-worldwide/ (accessed 17 April 2017).

Statista. (2016b), "Number of monthly active Twitter users worldwide from 1st quarter 2010 to 4th quarter 2016 (in millions)", *https://www.statista.com/statistics/282087/number-of-Monthly-Active-Twitter-Users/*, available at: https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/ (accessed 17 April 2017).

Stephanou, A. and Dagada, R. (2014), "the Impact of Information Security Awareness Training on Information Security Behaviour : the Case for", *Information Security*, pp. 309–330.

Stiviani, R. and Hayati, N. (2012), "Using Animation Clips To Improve The Listening Ability Of The Eighth Graders Of Smp Negeri 21 Malang", *SKRIPSI Jurusan Sastra Indonesia-Fakultas Sastra UM*, pp. 1–8.

Stretcher, V. and Rosenstock, I.M. (1997), "The Health Belief Model", *Health Behavior and Health Education: Theory, Research and Practice*, pp. 31–36.

Szewczyk, P. and Murray, B. (2008), "Malware Detection and Removal : An examination of personal anti-virus software", *Australian Digital Forensics Conference*.

Tam, K., Feizollah, A.L.I., Anuar, N.O.R.B., Salleh, R. and Cavallaro, L. (2017), "The Evolution of Android Malware and Android Analysis Techniques", *ACM Computing Surveys*, Vol. 49 No. 4, pp. 1–41.

Tavakol, M. and Dennick, R. (2011), "Making sense of Cronbach's alpha", *International Journal of Medical Education*, Vol. 2, pp. 53–55.

Thomas, K. and Nicol, D.M. (2010), "The Koobface botnet and the rise of social malware?", *Proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software, Malware 2010*, pp. 63–70.

Thomson, M.E. and Solms, R. von. (1998), "Information security awareness: educating your users effectively", *Information Management & Computer Security*, Vol. 6 No. 4, pp. 167–173.

Tidwell, C.L. (2010), “Measuring the Effect of Using Simulated Security Awareness Training and Testing on Members of Virtual Communities of Practice”, *Systemics, Cybernetics and Informatics*, Vol. 8 No. 6, pp. 85–88.

Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008), “Investigating Information Security Awareness: Research and Practice Gaps”, *Information Security Journal: A Global Perspective*, Vol. 17 No. 5–6, pp. 207–227.

Tullis, T.S. and Stetson, J.N. (2004), “A Comparison of Questionnaires for Assessing Website Usability ABSTRACT : Introduction”, *Usability Professional Association Conference*, No. June 2006, pp. 1–12.

Turner, D.W. (2010), “Qualitative interview design: A practical guide for novice investigators”, *The Qualitative Report*, Vol. 15 No. 3, pp. 754–760.

Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M.A. and Rashid, A. (2018), “Data Exfiltration: A Review of External Attack Vectors and Countermeasures”, *Journal of Network and Computer Applications*, Elsevier Ltd, Vol. 101 No. August 2017, pp. 18–54.

Vaishnavi, V. and Kuechler, B. (2004), “Design Science Research in Information Systems Overview of Design Science Research”, *Association for Information Systems*, p. 45.

Venkatesh, V. and Brown, S.A. (2001), “A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinats and Emerging Challenges”, *Management Information Systems*, Vol. 25 No. 1, pp. 71–102.

Vladlena, B., Saridakis, G., Tennakoon, H. and Ezingeard, J.N. (2015), “The role of security notices and online consumer behaviour: An empirical study of social networking users”, *International Journal of Human Computer Studies*, Elsevier, Vol. 80 No. December 2014, pp. 36–44.

Walliman, N. (2001), *Your Research Project: A Step-by-Step Guide for the First-Time Researcher*, Sage.

Wang, N., Xu, H. and Grossklags, J. (2011), “Third-Party Apps on Facebook : Privacy and the Illusion of Control”, *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*.

ACM, p. 10.

Websense. (2011), "Global Survey: Malware Attacks Up Because of Social Media; Organizations Lagging on Proper Protection - Websense News Releases", *Websense*, available at: https://community.websense.com/blogs/websense-news-releases/archive/2011/10/06/global-survey-malware-attacks-up-because-of-social-media-organizations-lagging-on-proper-protection.aspx (accessed 23 July 2015).

Williams, B., Onsman, A. and Brown, T. (1996), "Exploratory factor analysis: A five-step guide for novices", *Journal of Emergency Primary Health Care*, Vol. 19 No. May, pp. 42–50.

Woon, I.M.Y., Tan, G.W. and Low, R.T. (2005), "A protection motivation theory approach to home wireless security", *Twenty-Sixth International Conference on Information Systems*, pp. 367–380.

Workman, M. (2007), "Gaining Access with Social Engineering: An Empirical Study of the Threat", *Information Systems Security*, Vol. 16 No. 6, pp. 315–331.

Wu, M., Miller, R.C. and Garfinkel, S.L. (2006), "Do security toolbars actually prevent phishing attacks?", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '06*, p. 601.

Yan, G., Chen, G., Eidenbenz, S. and Li, N. (2007), "Malware Propagation in Online Social Networks : Nature , Dynamics , and Defense Implications Categories and Subject Descriptors", *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pp. 196–206.

Yang, C., Harkreader, R. and Gu, G. (2013), "Empirical evaluation and new design for fighting evolving twitter spammers", *IEEE Transactions on Information Forensics and Security*, Vol. 8 No. 8, pp. 1280–1293.

Yang, Z., Xue, J., Yang, X., Wang, X. and Dai, Y. (2016), "VoteTrust: Leveraging friend invitation graph to defend against social network sybils", *IEEE Transactions on Dependable and Secure Computing*, Vol. 13 No. 4, pp. 488–501.

Zaharias, P. and Poylymenakou, A. (2009), "Developing a Usability Evaluation

Method for e-Learning Applications: Beyond Functional Usability", *International Journal of Human-Computer Interaction*, Vol. 25 No. 1, pp. 75–98.

Zhang, S., Zhao, L., Lu, Y. and Yang, J. (2016), "Do you get tired of socializing? An empirical explanation of discontinuous usage behaviour in social network services", *Information & Management*, Elsevier B.V., Vol. 53 No. 7, pp. 904–914.

Zheng, X., Zeng, Z., Chen, Z., Yu, Y. and Rong, C. (2015), "Detecting spammers on social networks", *Neurocomputing*, Vol. 159, pp. 27–34.

Zimmerman, B.J. (2000), "Self-Efficacy: An Essential Motive to Learn", *Contemporary Educational Psychology*, Vol. 25 No. 1, pp. 82–91.

Zimmerman, D.W. (1997), "A note on interpretation of the paired-samples t test", *Journal of Educational and Behavioral Statistics*, Vol. 22 No. 3, pp. 349–360.

Appendix

Appendix A: Questionnaire Measurement Items

Perceived Susceptibility

	Strongly disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
It is extremely likely that my system and online social network profile will be infected by a malware attacks in the future	☐	☐	☐	☐	☐
My chances of getting malware attacks from online social networks are huge	☐	☐	☐	☐	☐
I feel malware attack from online social networks will infect my system in the future	☐	☐	☐	☐	☐
I frequently update the video player of my system when prompted, before watching videos from online social networks	☐	☐	☐	☐	☐

Perceived Severity

	Strongly disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
A malware attack from online social networks would steal my personal information from my system without my knowledge	☐	☐	☐	☐	☐
Malware attacks from online social networks would invade my privacy	☐	☐	☐	☐	☐
My personal information stolen by malware attacks from online social networks can be used to launch more attacks against other users	☐	☐	☐	☐	☐
Malware attacks from online social networks can destroy my online reputation	☐	☐	☐	☐	☐

Malware from online social networks cannot steal my banking information, expose my private chats or post messages on my behalf	☐	☐	☐	☐	☐

Perceived Threat

	Strongly disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
Malware attacks from online social networks poses a threat to me	☐	☐	☐	☐	☐
Malware attacks from online social networks poses a threat to my organisation	☐	☐	☐	☐	☐
It is risky to use my online social network account if my system is infected by malware	☐	☐	☐	☐	☐

Mass Interpersonal Persuasion

	Strongly disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
I feel I will watch an animated video about social network security if I get invitation requests from my social network friends.	☐	☐	☐	☐	☐
I feel I will watch an animated video about social network security if I get invitation requests from my social network friends I personally know.	☐	☐	☐	☐	☐
I will not watch an animated video about social network security if I get invitation requests from my social network friends.	☐	☐	☐	☐	☐

Perceived Safeguard Effectiveness

	Strongly disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
Watching a security awareness animated video about social network security would be useful in helping me detect malware attacks on online social networks	☐	☐	☐	☐	☐
Watching a security awareness animated video about social network security would enable me detect malware attacks on online social networks faster	☐	☐	☐	☐	☐
Watching a security awareness animated video about social network security would increase my social networking risk assessment ability	☐	☐	☐	☐	☐
I have anti-virus software installed on my system and do not need to watch security awareness animated video about social network security	☐	☐	☐	☐	☐

Perceived Safeguard Cost

	Strongly disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
It will take very less time to gain security awareness about social network malware attacks through animated videos	☐	☐	☐	☐	☐
It will take less cost to gain security awareness about social network malware attacks through animated videos	☐	☐	☐	☐	☐
Watching a security awareness animated video about social network malware attacks is inconvenient for me	☐	☐	☐	☐	☐

Self-Efficacy

	Strongly disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
I could successfully gain security awareness about social network malware attacks if I had never learned it before	☐	☐	☐	☐	☐
I could successfully gain security awareness about social network malware attacks if my social network connections referred a source to me	☐	☐	☐	☐	☐
I could successfully gain security awareness about social network malware attacks if I see previous cases of attacks	☐	☐	☐	☐	☐
I feel gaining security awareness about social network malware attacks does not help me in detecting malware attacks on online social networks	☐	☐	☐	☐	☐

Avoidance Motivation

	Strongly disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
I intend to obtain knowledge from a security awareness animated video to avoid malware attacks on online social networks	☐	☐	☐	☐	☐
I predict I would gain effective awareness about malware attacks on social networks through a security awareness animated video	☐	☐	☐	☐	☐
I feel I do not want to gain security awareness from an animated video to avoid malware attacks on online social networks	☐	☐	☐	☐	☐

Avoidance Behaviour

	Strongly disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
I will use the knowledge gained from a security awareness animated video to avoid malware attacks on online social networks	☐	☐	☐	☐	☐
I will update my anti-malware knowledge frequently through the security awareness video regularly	☐	☐	☐	☐	☐
Updating my anti-malware knowledge through security awareness videos is not very important to avoid malware attacks on online social networks	☐	☐	☐	☐	☐

Appendix B: Pattern Matrix and Factor Correlation Matrix

Pattern Matrix

	Factor								
	1	2	3	4	5	6	7	8	9
SAFE2	.922								
SAFE1	.915								
SAFE3	.867								
SAFE_R	.531								
MIP1		.960							
MIP2		.953							
MIP3_R		.769							
SE1			.817						
SE2			.775						

SE3			.727						
PSUS2				.892					
PSUS3				.749					
PSUS1				.682					
PSEVR1					.817				
PSEVR2					.798				
PSEVR3					.598				
SC2						1.016			
SC1						.594			
SC3_R						.553			
AB2							.905		
AB1							.831		
AB3_R							.471		
AM2								1.067	
AM1								.570	
AM3_R								.391	
PT2									.980
PT1									.620

Extraction Method: Maximum Likelihood.

Rotation Method: Promax with Kaiser Normalization.

a. Rotation converged in 6 iterations.

Factor Correlation Matrix

Factor	1	2	3	4	5	6	7	8	9
1	1.000	.346	.310	-.015	.106	-.384	.407	.378	.350
2	.346	1.000	.399	-.004	.110	-.333	.442	.435	.423
3	.310	.399	1.000	-.028	.220	-.296	.403	.354	.402
4	-.015	-.004	-.028	1.000	.086	-.011	.145	-.065	.063
5	.106	.110	.220	.086	1.000	.057	.173	.145	.200
6	-.384	-.333	-.296	-.011	.057	1.000	-.443	-.352	-.372
7	.407	.442	.403	.145	.173	-.443	1.000	.540	.436
8	.378	.435	.354	-.065	.145	-.352	.540	1.000	.388
9	.350	.423	.402	.063	.200	-.372	.436	.388	1.000

Extraction Method: Maximum Likelihood.

Rotation Method: Promax with Kaiser Normalization.

Appendix C: Qualitative Data Items and Initial Codes

N	Participants Statements	
1	"It's informative, this is very informative and erm the video, I mean sheds light on things that people need to know and it's simplified. It doesn't talk too much jargon. It iterated things I already have an idea about. I definitely will invite my friends to use this."	Informative Sheds light It's simplified No jargon Invite my friends I already have an idea about
2	"The videos are good; they kinda scare you into thinking,	Scare Awareness

	to be more aware, and I did learn the actual signs of threat. The little story really helps. I might invite my friends to watch the videos, although I expected more details".	Signs of Threat Invite my friends
3	"I thought they were good actually, the way they were created. I thought they were very informative, but in an interesting way, the message was put across very clearly, and it's very easy to understand. I kinda feel my friends would find it easy to use".	Informative Interesting way Clarity Easy to understand Easy to use
4	"I think it was very useful and it was helpful and it told you what you should look out for when going on websites and being aware about what's out there and other sites and people can send you viruses, or like malicious links. So it's important to always be aware and check erm, the actual official page. For example on Facebook, if it comes through a message from your email, you have to go on your Facebook account and actually check and erm the cartoons are a good depiction	Useful Helpful Awareness Understand easily Tell my friends about it

	of what could happen because with the scenarios you could understand easily what was going yeah. I will tell my friends about it".	
5	"It taught me a lot to be extra cautious about opening certain things. Like sometimes you don't really think erm about. Sometimes you don't really think about it, you just open it blindly like I said in most of my answering the question. I won't find any problem in with just opening links but I guess it has taught be a lot because erm just to send a message back to your friends and just ask them to clarify if you really sent the message. Just to understand the safety of everything yeah. Videos like these offer interesting insights to the sort of web pages, so I wouldn't mind watching another one again. I guess I will always keep the knowledge I gained to use in the future when opening certain pages on Facebook. I will be happy to share this information to help my friends out and fight this cause, yeah".	Awareness Extra cautious Understand safety measures Interesting insights Watch another one again Use the knowledge Happy to share this information

6	"It's an important app because you have to be aware of such risks when you are using Facebook. Yeah, mistakes could occur, you do have to be careful of the sources just so you can trust t hem. Because of risks and problems with the software and malware".	Awareness Be careful Because of risks
7	"I thought it was quite well like the way it was laid out, erm it was explained well, erm, it was engaging, and I was really listening and didn't find it boring so it was good. Erm, it was easy to use and simple. If I feel friends need to know about this, I would invite them to use it".	It was engaging It was boring Easy to use Simple Awareness Invite Friends
8	"It was very easy to understand, erm the animation was quite funny as well so it kept me wanting to listen and to find out more about cyber security. I got the questions right so it was good. I will try to invite my friends to get them aware about cyber security, because I felt like what I have just heard, I wasn't even aware that simply clicking a link from your email could be a potential danger.	Easy to Understand Funny Find out more about cyber security Kept me wanting to listen Got the questions right Invite my friends Awareness Potential danger

	So even I have learnt something, so I think especially for a lot of young people it will be good to get them on board and get them aware of these things because it could be dangerous".	
9	"Erm, I think they were sought of educational and someone that did not understand or nor how to use the internet it is useful. It was well organised, and I think that the information that was set through it would help someone that needed it. The videos were actually good, if my friends needed help, yeah I would invite them to use it. The videos were quite short and it has the information in two minutes or so, it's a good amount of time and won't bore a person and make them click next."	Educational It is useful Organised Invite them to use Videos were quite short Won't bore a person
10	"Erm, it's a very informative way of telling people the dangers of links and logging in. Erm, yeah it kind of refreshes my memory, like reading the website link to see if it's actually spelt properly. It's always informative to know that a missing letter in a	Informative Dangers of links Dangers of logging in. Trust a close friend more Invite me to use this

	link can actually prove that it's fake or real. I would trust a close friend more if they invite me to use this than a distant friend."	
11	"I think it's very useful, the real life cases ideas was very good, erm, I will share with my friends, yeah this is something we actually do all the time. Before payment we do check out websites to see if it's actually good, this is something we actually do".	Useful Real life cases Share with my friends
12	"If I was to give you an overall summary about the video, it's very informative, and regards to the video the way it explains it, it explains it very simple, which is what you need. Erm, obviously I have seen this things on Facebook before, a lot of my Facebook friends have been sending me messages about refugees to give a certain amount of money towards some kind of charity, so I have seen it before but I didn't realise it was some form of malware. So for me I just kind of need to be aware and what I need to do in terms of steps taken to make sure I am protecting	Informative Simple Awareness Protection measures Pass it to other people

	myself correctly. Now that I have received the knowledge, I would definitely pass it down to other people and make them aware people that are less tech savvy than me".	
13	"It was quite straightforward; I could understand what was going on. I know what's going on now. It's quite persuasive, I know what's going on, I understand it, it's quite clear".	Straightforward Persuasive Clarity Understandable
14	"Erm, basically, from what I just saw, it showed me the insights into how you can easily be manipulated , like getting a virus, cause if I saw something like what the person in the video saw, I would have downloaded it. But now that I know, that if you go into a third party website and they want you to download something, you just shouldn't unless you actually check it out first, otherwise you will get a virus. I have some friends that have been hacked, it's a good way of getting people to understand that there are dangers out there and you can get scammed at any point. It's a really good website to show	Awareness Safety measures I have some friends Dangers Understand Avoidance

	how you can avoid them".	
15	"Erm, I get these emails as well from Amazon and things like that, I always check like the email that it's sent from because it's usually not from Amazon.com, so that's how I usually check whether that it's a spam or not. It's scary that they can get your details "like with rose in the videos" just by clicking by clicking on a link. That's worrying, erm, is there no software that can stop these? Anyways, I think it's made me more aware of how I am. Don't just click on links sent by supposedly friends on Facebook yeah. It's a persuasive technique, I like the Dr and Patient form. I would definitely tell my friends about it, they are more careless than me".	Scary Awareness Relatable Tell my friends Persuasive
16	"Yeah, if you don't know anything about it, it could be useful. Erm just telling people about the "software" updates, I get that pop-up a lot. Yeah. I don't feel the need to use it because I am very careful, my information doesn't get shared so".	Usefulness
17	"Yeah, the app was fairly easy,	Easy to use

	access and everything was easy, watching the videos and it made me more aware of what not to click and what to click by looking for the clear signs. My friends need to see this because they need help so I will share them the link, yeah".	My friends Awareness Looking for the clear signs
18	"I think the video was quite helpful, kind of educating on malicious virus prevalent out there. I don't think many people are educated when they click on the link that it could lead to something else. I think website was quite handy, I think if you are targeting a market of younger audience then it would be quite attractive to them".	Helpful Awareness Handy Attractive
19	"Can you get hacked if you are using the app? It app is helpful. You do get to learn like not to open random links, and yeah I would like to use it again and get my friends to use it as well".	Helpful Awareness Use it again My friends to use it
20	"Okay, I did find it very useful, erm, I would actually and I am not joking I would go home and use this right now. Erm, I think for people that are not really exposed to	Useful Use it again Easy to understand Quick to understand Taught me much more

	like malware it is much easier for them to look at. And it's quick to understand, erm, even though I know a little bit about it, it has actually taught me much more and it was easy to understand, I was able to find new videos. Each video gave me something new to learn from".	