Online Social Network Security Awareness: Mass Interpersonal Persuasion using a Facebook App

Ehinome Ikhalia, Alan Serrano, David Bell and Panos Louvieris

Brunel University London

Abstract

Purpose

Online social network (OSN) users have a high propensity to malware threats due to the trust and persuasive factors that underpin OSN models. The escalation of social engineering malware encourages a growing demand for end-user security awareness measures. This paper takes the theoretical cybersecurity awareness model TTAT-MIP and tests its feasibility via a Facebook App, namely Social Network Criminal (SNC).

Design/methodology/approach

The research employs a mixed methods approach to evaluate the SNC app. A Systems Usability Scale (SUS) measures the usability of SNC. Paired samples T-Tests were administered to forty participants to measure security awareness - before and after the intervention. Finally, twenty semi-structured interviews were deployed to obtain qualitative data about the usefulness of the App itself.

Findings

Results validate the effectiveness of OSN apps utilising a TTAT-MIP model – specifically the mass interpersonal persuasion (MIP) attributes. Using TTAT-MIP as a guidance, practitioners can develop security awareness systems that better leverage the intra-relationship model of Online Social Networks (OSNs).

Research limitations/implications

The primary limitation of this study is the experimental settings. Although the results testing the TTAT-MIP Facebook App are promising, these were set under experimental conditions.

Practical implications

SNC enable persuasive security behaviour amongst employees and avoid potential malware threats. SNC support consistent security awareness practices by the regular identification of new threats which may inspire the creation of new security awareness videos.

Social Implications

The structure of OSNs is making it easier for malicious users to carry out their activities without the possibility of detection. By building a security awareness program using the TTAT-MIP model, organisations can proactively manage security awareness.

Originality/value

Many security systems are cumbersome, inconsistent and non-specific. The outcome of this research provides organizations and security practitioners with a framework for designing and developing proactive and tailored security-awareness systems.

Keywords: Online Social Networks, Malware, Mass Interpersonal Persuasion, Threat Avoidance Theory, SUS, Social Engineering.

1 Introduction

Although social engineering may have different meanings, in the context of cybersecurity and therefore in the context of this paper, social engineering is defined as a malicious user's 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). The key objective of the malicious user, also known as "an attacker" is to illegally obtain information that allows unauthorised access to one or more systems.

Social engineering is an approach increasingly adopted by attackers as it is often easier to gain illegal access to systems when compared to technology enabled strategies. For example, it is easier and cheaper to mislead a staff member of an organisation into giving away their password than carrying out a brute-force attack to acquire it (Gupta et al., 2017). Social engineering usually starts with collecting contextual information on potential targets. This activity is typically obtained using a 'dumpster diving' technique: gathering information through company phone books, memos, company policy manuals, organizational charts, and phone calls. The advent of online social networks (OSNs), however, has introduced new opportunities for attackers to execute their illegal/malicious actions (Ferreira et al., 2015; Gragg, 2001). Attackers are now exploiting OSNs such as Facebook to collect preliminary background information on potential victims and to explore both human and technology-based social engineering. Such exploitation is for the purpose of deploying malicious software (commonly referred as malware) designed to steal sensitive data from the systems of unsuspecting OSN users (Nelms et al., 2016). The characteristics of OSNs combined with users' behaviour make them a particular target of social engineering attacks (Diffley and Kearns, 2011; Faghani and Saidi, 2009; Hanna et al., 2011; Lin and Lu, 2011; Yan et al., 2007).

Fogg (2008) offered insights as to why online social platforms lead to the evolution and change in user behaviour at scale. Fogg (2008) defined this phenomenon as Mass Interpersonal Persuasion (MIP). MIP suggests that OSN users tend to get involved in trends that then engages their 'friends' and 'friends' of 'friends'. It is a unique success determinant of OSNs and it is the biggest factor that influences users of online social networks to perform certain behaviours at such a scale. MIP includes six components: persuasive experience, automated structure, social distribution, rapid cycle, huge social graph and measured impact.

It is clear that the characteristics of OSNs support the psychological aspects of social engineering. For example, social engineering thrives on trust-based relationships and the forgery of relationships between an attacker and potential victims to manipulate them to perform illegal actions (Yang et al., 2016). Similarly, OSNs grows on relationships built between users, and frequently this characteristic has been abused for malicious intentions. An attacker can clone the profile of a legitimate OSN user's connection and then attempt to forge a relationship with the potential target and gradually build trust. Such trust-based relationships can be used to persuade a potential victim into downloading malware on their computing devices. The Zeus virus is an example of such attacks. Kaspersky (2015) reported a Trojan horse malware – Zeus, initially discovered in 2007, had 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 (Riccardi et al., 2013).

The escalation of social engineering malware threats has increased the growing demand for end-user security awareness covering associated risks and effective mitigation measures (Parsons et al., 2014). There is research that argues that security awareness systems are efficient measures to mitigate social engineering malware attacks (Aloul, 2012; Arachchilage and Love, 2014; Olusegun and Ithnin, 2013; Thomson and Solms, 1998). Despite this there are indications that OSN are still vulnerable to social engineering attacks. The authors of this paper argue that most existing systems do not consider the nature and characteristics of the technology platform through which malware attacks occur. OSN platforms present multi-vectors for sophisticated malware attacks which make user detection and avoidance a herculean task.

In this paper, we introduce a Web-based Facebook animated video application, "Social network criminal" (SNC) that has been designed and developed based on a theoretical model previously proposed and statistically tested namely TTAT-MIP (Ikhalia and Serrano, 2016). The motivation for developing SNC is to practically validate the TTAT-MIP model and to create security awareness that improves the threat avoidance behaviour of OSN users. The rest of the paper is structured as follows. The theoretical model from which this application is based is presented in section 2. Section 3 describes the working functionality of SNC, linking it with the theoretical model. Section 4 describes the methodology adopted to validate the Facebook application, whilst section 5 presents the data collection, analysis and results of the studies undertaken. Section 6 presents the overall discussion and Section 7 concludes the paper with areas for further research.

2 Rationale: The theoretical model TTAT-MIP

The Facebook application used in this paper has been designed and developed based on an extended version of the technology threat avoidance theory using mass interpersonal persuasion approach, namely TTAT-MIP (see Figure 1). For the TTAT-MIP model, a survey questionnaire was used to modify the technology threat avoidance theory (TTAT) adding mass interpersonal persuasion (MIP). We analysed 285 samples by structural equation modelling (SEM) approach, particularly Covariance-based SEM.

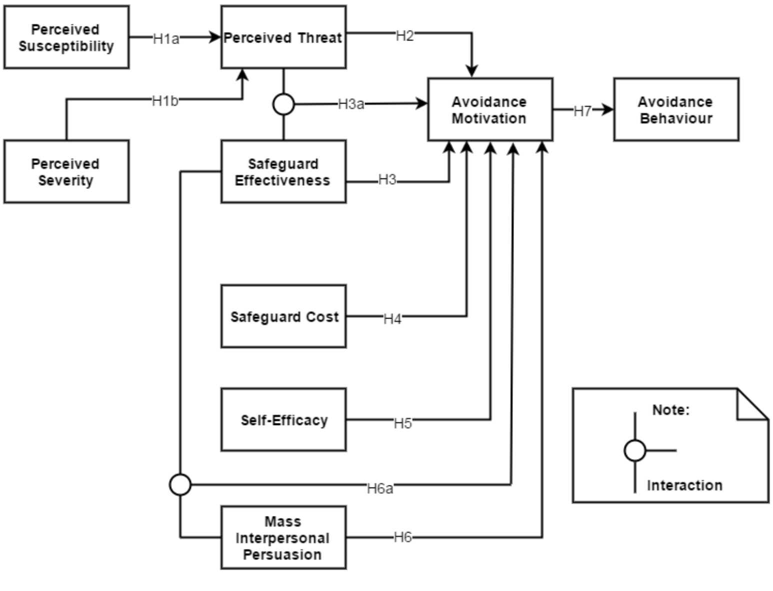


Figure 1 The TTAT-MIP model

This paper aims to practically operationalize the TTAT-MIP model using a Facebook App (a.k.a. Social network criminal - SNC). The intention is to add knowledge to the quantitative evaluation presented in Ikhalia and Serrano (2016) by using qualitative methods during the validation of the Facebook App. In order to understand the rationale of the model, a brief description is presented in the following paragraph. Detailed information about the creation of this model together with its quantitative validation can be found in Ikhalia and Serrano (2016) and Ikhalia (2017).

The malware threat avoidance behaviour of OSN users is determined by their 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”. Threat perception is developed by perceived susceptibility and perceived severity. Perceived susceptibility is 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.

> *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.*

Avoidance motivation is defined 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.

> *H3: Safeguard effectiveness positively affects avoidance motivation.*

Safeguard effectiveness negatively moderates the relationship between perceived threat and 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 safeguard measure

> *H4: Safeguard cost negatively affects avoidance motivation*

Self-efficacy is defined as the confidence in applying a safeguarding measure to avoid a malware threat.

> *H5: Self efficacy positively affects avoidance motivation*

To empirically measure MIP, we intend to focus on the success determinants of MIP which are: Persuasive experience, social distribution and a large social graph.

> *H6: MIP positively affects avoidance motivation*

Furthermore, we argue that MIP positively moderates the relationship between safeguard effectiveness and avoidance motivation.

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

Finally*,* avoidance motivation has a positive effect on the threat avoidance behaviour of OSN users

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

Findings suggest that OSN users develop a threat perception when they perceive the negative consequences of a malware attack would be severe. To motivate online social network users to avoid malware, they need to be convinced that the threats exist and are avoidable. Furthermore, when tackled with a threat, users are motivated to avoid the threat if they perceive the effectiveness of the safeguarding measure (safeguard effectiveness), the convenience of using it (safeguard cost), their self-confidence in using it (self-efficacy) and the mass interpersonal persuasion (MIP) of the safeguard (Liang & Xue 2010; Ikhalia & Serrano 2016). Results 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). These findings suggest that to help OSN users to be aware of the threats posed by social networks environments and avoid them; interested parties should include techniques of persuasion from users' interpersonal connections. The following section describes in detail how the TTAT-MIP model is operationalised through the Facebook App.

3 Working Functionality of Social Network Criminal (SCN)

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. The choice of using video animation for presenting information was based on evidence from the literature which shows the broad adoption of videos as a significant factor for influencing user engagement on OSN settings (Cheng et al., 2008; Dunlop et al., 2016; Kaplan and Haenlein, 2010). In addition, videos receive less criticism by users, thus, allowing them to focus on the message being delivered (Rosenkrans, 2009; Soika et al., 2010). Next there is a description of the main functionality of the App.

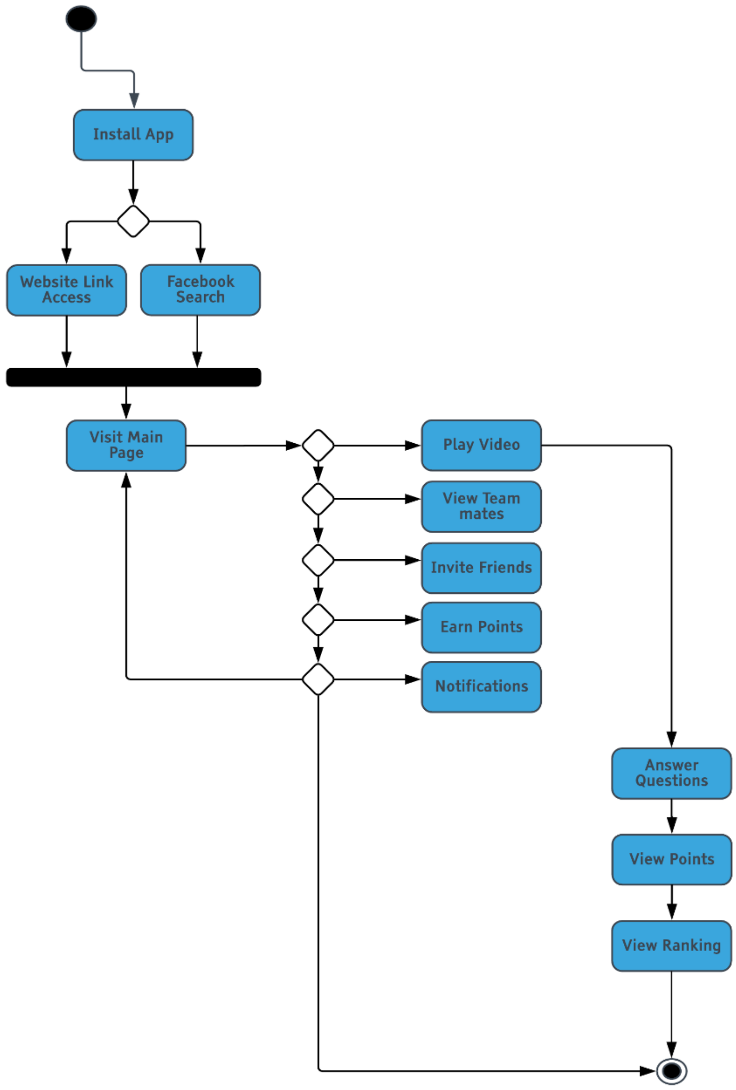
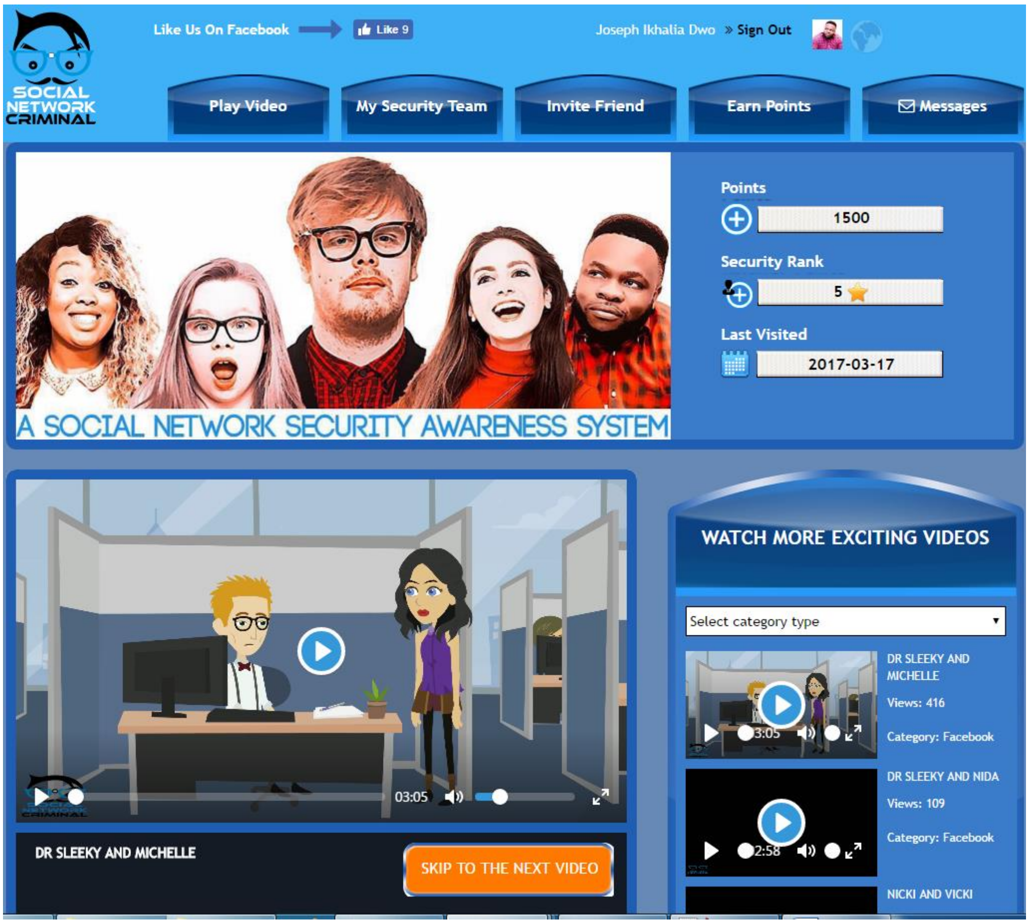


Figure 2 Basic Activity Diagram of SNC Deployment and Use

After the app has been installed, access is possible via a web link or by searching Facebook (you can access a view of the App here https://www.socialnetworkcriminal.com/). A main page then presents the user with a number of options (see figure 3). Functionality is available to enable connection to friends (via invites and competition) as well a video viewing with subsequent quiz questions.



Points: 1500

Security Rank: 5 ★

Last Visited: 2017-03-17

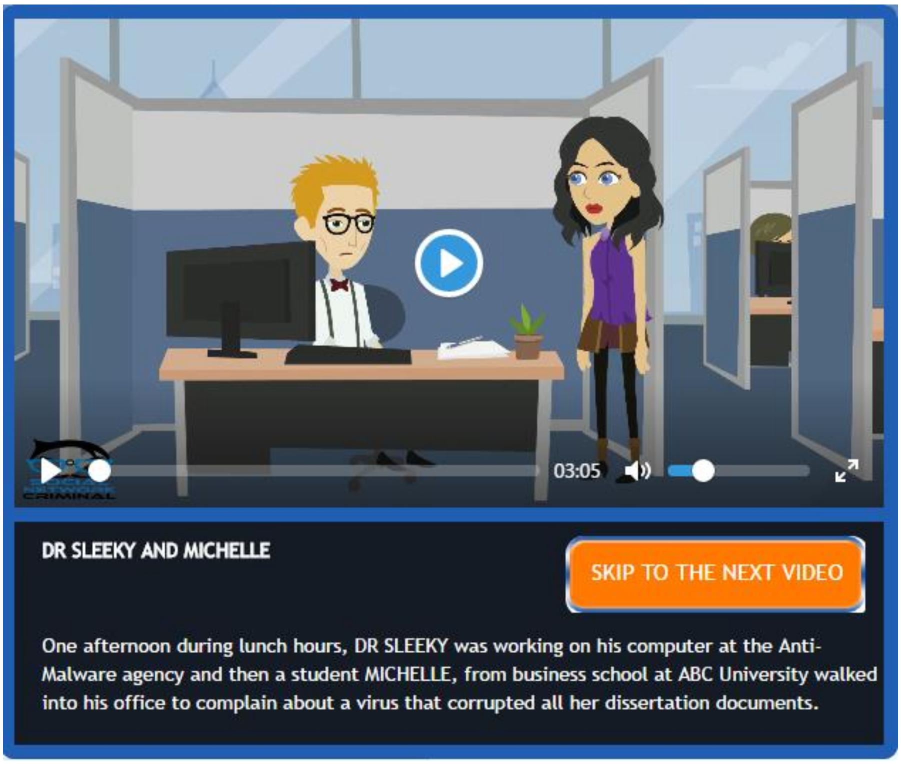
DR SLEEKY AND MICHELLE
Views: 416
Category: Facebook

DR SLEEKY AND NIDA
Views: 109
Category: Facebook

Figure 3: Homepage of SNC

3.1 Play Video

This feature allows users to observe scripted animation videos based on previous cases of social network malware attacks and the different measures needed to avoid such attacks. We inform the user about the “threat” and its severity (Perceive Thread in the TTAT-MIP model in Figure 1) as well as the safeguard measures to avoid them. Figure 4 is a screenshot of an example of a video in SNC.



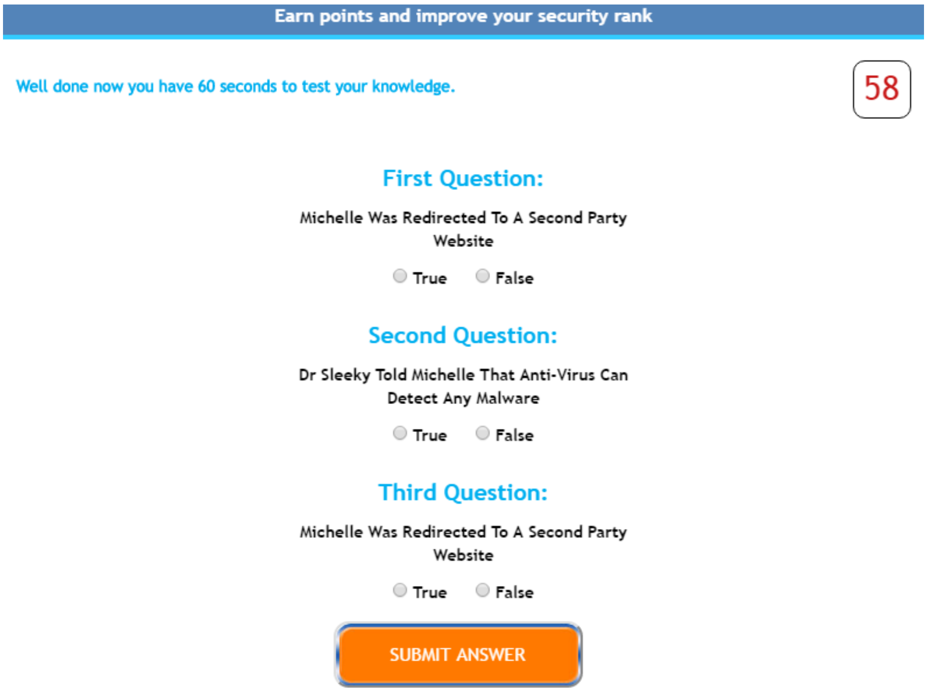
DR SLEEKY AND MICHELLE

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 4: A Video Scene on SNC

3.2 Quiz

This feature is also used to increase the level of the perceived threat, as depicted in the TTAT-MIP model. After a user completes a video, a pop-up quiz with a 60 seconds countdown 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 content. The quiz was designed to make it impossible for users to provide accurate answers without sufficient engagement. 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 5 is an example of such quizzes.


Earn points and improve your security rank

Well done now you have 60 seconds to test your knowledge.

58

First Question:

Michelle Was Redirected To A Second Party Website

○ True ○ False

Second Question:

Dr Sleeky Told Michelle That Anti-Virus Can Detect Any Malware

○ True ○ False

Third Question:

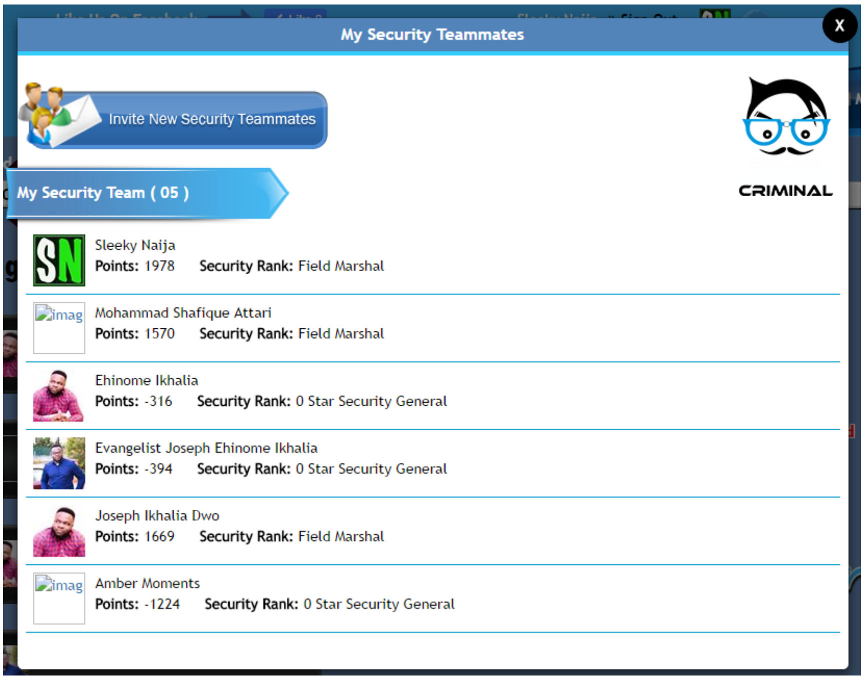
Michelle Was Redirected To A Second Party Website

○ True ○ False

Figure 5: Quiz Sample

3.3 My Security Team

This feature allows users to send invitations to be part of their security team to their Facebook friends. This feature enhances the persuasiveness of SNC by allowing teammates to observe their security rankings and possibly stir up competition amongst teammates. As TTAT-MIP suggests, OSN users are motivated to avoid malware threats when persuaded by their friends, in this case the persuasion is made through competitiveness. By allowing them to build a network of security teammates, SNC exemplifies the Mass Interpersonal Persuasion construct within TTAP-MIP. Figure 6 is shows an example of how users can motivate their networks.


My Security Teammates

X

Invite New Security Teammates

CRIMINAL

My Security Team (05)

Sleeky Naija
Points: 1978 Security Rank: Field Marshal

Mohammad Shafique Attari
Points: 1570 Security Rank: Field Marshal

Ehinome Ikhalia
Points: -316 Security Rank: 0 Star Security General

Evangelist Joseph Ehinome Ikhalia
Points: -394 Security Rank: 0 Star Security General

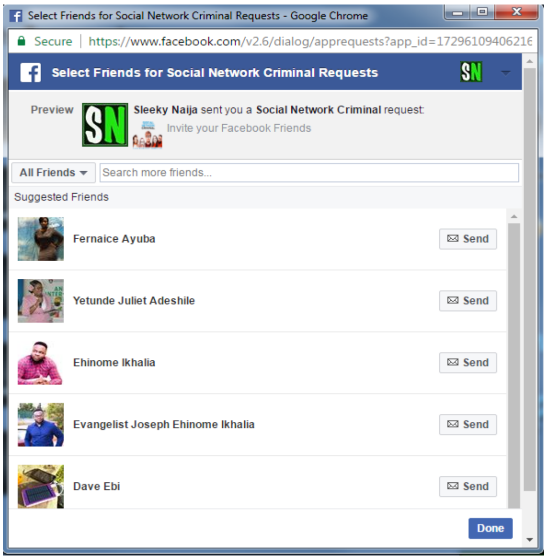
Joseph Ikhalia Dwo
Points: 1669 Security Rank: Field Marshal

Amber Moments
Points: -1224 Security Rank: 0 Star Security General

Figure 6 Security Teammates of a user on SNC

3.4 *Invite Friend:*

Similar to other Facebook applications, this marketing feature allows SNC users to notify their friends of the existence of the app. Users can inform their friends multiple times at various intervals. Based on TTAT-MIP, users are more likely to use SNC when persuaded by their friends. As such, the “Invite Friend” feature allows inter-personal persuasion to occur and consequently a change in threat avoidance behaviour. An example of how friends can be invited to participate on SCN is shown in Figure 7.


Select Friends for Social Network Criminal Requests - Google Chrome

Secure | https://www.facebook.com/v2.6/dialog/apprequests?app_id=172961094062l6

Select Friends for Social Network Criminal Requests

Preview **Sleeky Naija** sent you a **Social Network Criminal** request:
Invite your Facebook Friends

All Friends ▾ Search more friends...

Suggested Friends

Fernaice Ayuba ✉ Send

Yetunde Juliet Adeshile ✉ Send

Ehinome Ikhalia ✉ Send

Evangelist Joseph Ehinome Ikhalia ✉ Send

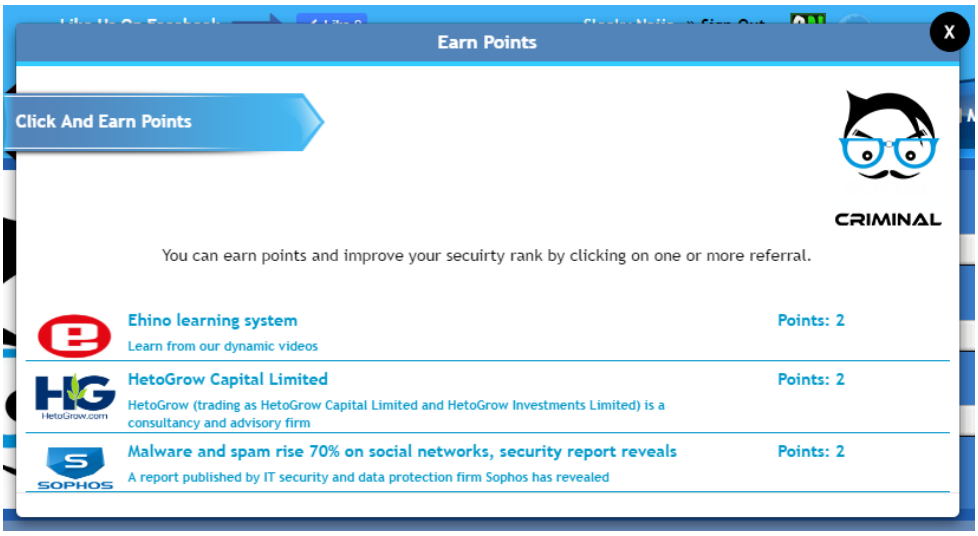
Dave Ebi ✉ Send

Done

Figure 7 Informing friends about SNC

3.5 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. The concept of "Earning Points" is a psychological persuasion factor that motivates users for their knowledge about the existence of a threat. It relates strongly with the mass interpersonal persuasion construct of TTAT-MIP, as it allows security teammates on SNC to observe the progress of their security awareness which tends to persuade members with low-security points to learn more and attain higher points. Figure 8 shows how this can be undertaken.



You can earn points and improve your secuirty rank by clicking on one or more referral.

Ehino learning system — Points: 2
Learn from our dynamic videos

HetoGrow Capital Limited — Points: 2
HetoGrow (trading as HetoGrow Capital Limited and HetoGrow Investments Limited) is a consultancy and advisory firm

Malware and spam rise 70% on social networks, security report reveals — Points: 2
A report published by IT security and data protection firm Sophos has revealed

Figure 8: Earning Points on SNC

4 Evaluation Methodology

The research employs mixed methods (quantitative and qualitative) to evaluate the SNC app: surveys, lab experiments and semi-structured interviews. The methods were used as follows:

- Systems Usability Scale to measure the usability of SNC (usefulness and user satisfaction)
- Paired Samples T-Test administered to 40 participants to measure the improvement of their security awareness, before and after intervention.
- Semi-structured interviews to 20 participants to obtain qualitative data about the usefulness of the App.

4.1 Systems Usability Scale (SUS)

The first method measures usability of SNC (usefulness and user satisfaction) and was carried out using a systems usability scale (SUS) survey questionnaire. SUS has been empirically validated by Bangor et al., (2008) as a useful technique within the usability community for efficiently and quickly collecting user's subjective assessment of a system's usability. A closed questionnaire design was used to assist participants in understanding the questions clearly through alternatives provided and also to provide a basis for comparison. Likert scales of 1 to 5 were used in this study as they are known to be effective (Gliem and Gliem, 2003). 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 higher degrees of reliability and validity while ensuring that participants provide accurate answers due to its highly structured measures. The results of SUS are provided in section 5.1. Details about SUS questionnaire design are presented Appendix 1.

4.2 Paired Samples T-Test

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.

In the laboratory experiment phase of SNC, the participants were required to undertake an online test to access their risk assessment abilities concerning malware threats on online social networks. Subsequently, they were allowed to engage with SNC by using its security awareness tools (videos animation clips). The participants were required to complete a second online test and their scores were statistically analysed and compared with the initial scores using a paired samples t-test technique.

4.3 Semi-structured interviews

A hybrid thematic analysis approach (inductive and deductive) was used to extrapolate insights from the data gathered from semi-structured interviews - allowing participants to provide verbal feedback about their opinion on receiving security awareness through SNC (Turner, 2010). Semi-structured interviews are widely employed for conducting qualitative research. Semi-structured interviews are particularly suited to this task as they allow the researcher/interviewer to ask follow-up questions in order to gain further information or clarity about a topic of interest. For example, during the interviews in the second study, users were asked to briefly describe their opinion about SNC. Some participants used phrases such as "I found it persuasive or interesting". Consequently, the interviewer probed them on what they meant by "persuasive" or "interesting". Hove and Anda (2005) argue that investigations related to issues in software development are usually qualitative and relevant measures are gathered through semi-structured interviews. They argue that semi-structured interviews involve high costs and quality which are often relative to the how the interviews are conducted.

4.4 Participants

The study was carried out with 40 participants from a random sample of students in a top UK University. Forty 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 with SNC. They were invited to a computer laboratory at the 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 study demographics is presented in Table 1.

Table 1: 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

4.5 Study Procedure

Each participant was briefed on the nature of the experiment, its phases and signed a consent form required by the ethics committee of the University. 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 carried out using a Microsoft Windows desktop computer and participants were presented with ten scenarios of OSN malware threats (uploaded on surveymonkey.com). The online social network scenarios were designed based on previously reported incidents of OSN malware attacks (Faghani and Saidi, 2009; Gao et al., 2010, 2011). The participants gave their assessment of ten scenarios each before and 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 and the participants were shown ten more OSN activity scenarios to evaluate. The pre- and post-tests scores of each participant were recorded to observe whether or not their OSN security behaviour improved. Finally, the participants gave verbal feedback when asked to express their opinion about receiving security awareness through SNC.

5 Results

5.1 System Usability Scale (SUS) Results

SPSS software package (IBM SPSS Statistics 20) was used for the data analysis of the system usability scale (SUS). The Cronbach's alpha value to measure the internal consistency of how closely related the set of items are as a group (Gliem and Gliem, 2003) was calculated. Previous research argues that a given alpha greater than 0.70 is statistically adequate (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 scoring 82.9 out of 100 (Brooke et al., 1996). The score was obtained using the same standard procedures recommended in the literature (see Appendix 2 for more details on the SUS score from each participant and the mean and standard deviations).

SUS was created to assess a single study within a scale of 0 to 100 where higher scores indicate better usability (Bangor et al., 2008). Therefore, a score of 82.9 reflects a relatively high score. To complement this information, the score obtained of 82.9 can be compared to the mean SUS score of a study undertaken by Bangor et al. (2008). In this research 2,324 surveys have been completed over the course of 206 studies resulting in a a mean SUS score for all surveys of 70.14 (s = 21.71) with a median of 75 and a range from 0 to 100. In this context it can be said that the SUS score of SNC (82.9) is above the median and thus it can be considered as a high score. In addition to this, the SUS score was re-affirmed as the participants' mentioned that they find SNC intuitive and easy to use during the interviews (see section 5.4 for more details).

5.2 Paired Samples t-Test Results: Testing user's awareness

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 (Rietveld and van Hout, 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, the 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).

> Alternative Hypothesis (*H₁*): Using SNC can significantly improve the security behaviour of social network users.
>
> Null Hypothesis (*H₀*): Using SNC does not significantly improve the security behaviour of social network users.

The findings show that the participants average mean test scores were significantly improved after using SNC. This is evidenced by the p-value (p = 0.001). 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 standard 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).

5.2.1 The validity of the Paired Samples t-Tests

A normality test was conducted to assess 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 = 0.200). 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 9 and Figure 10 show the histogram of differences in marks and a reasonable probability (QQ) plot respectively.

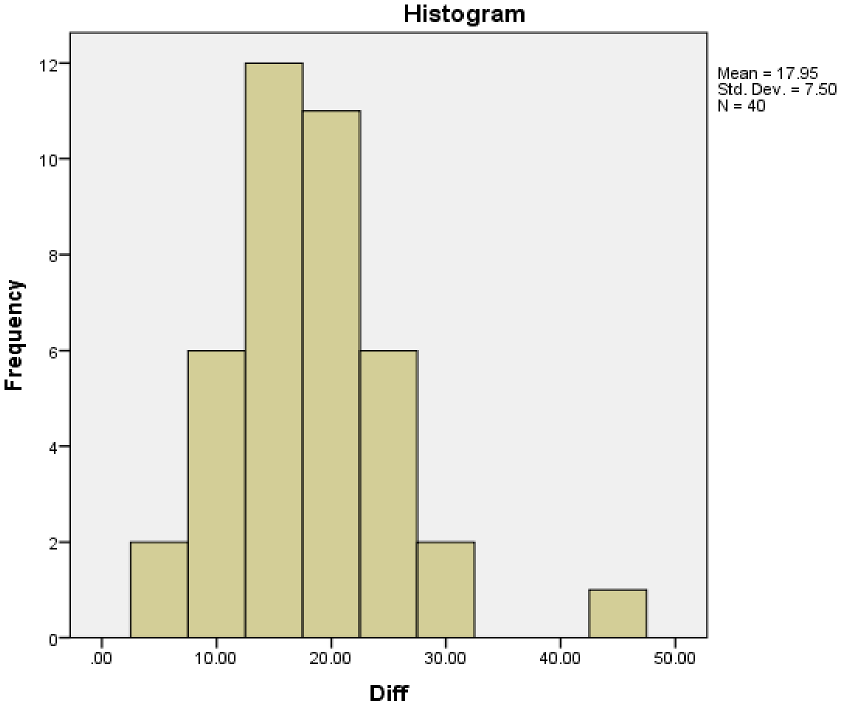


Figure 9 Difference in pre- and post-scores

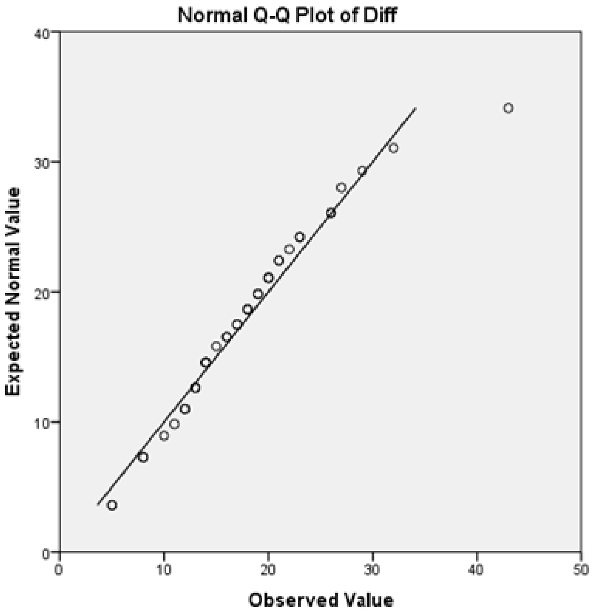


Figure 10 : Normal Probability QQ plot of the Difference Scores

5.3 Semi-Structured Interviews

Semi-structured interviews allowed participants to express their viewpoints about the SNC app. 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 were recorded. Subsequently, 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 of 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.

5.3.1 Semi-Structured Interviews: Steps for Data Analysis

A hybrid of inductive and deductive thematic analysis approach was employed to analyse the qualitative data (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 potential new factors that may have influenced SNC other than the factors inherent within TTAT-MIP. The following process was followed to conduct the analysis.

Step 1 - Familiarisation with the data: After transcribing the data, it was carefully read and re-read.

Step 2 - Initial code generation: Features of the data were coded systematically and based on the theoretical model – TTAT-MIP.

Step 3 - Searching for themes: Initial codes were collated into initial representative themes as seen in Figure 11.

Step 4 - Reviewing themes: Themes were reviewed, and their interrelationships were accessed. Thereafter, strongly related themes were combined to represent a single theme as seen in Figure 12.

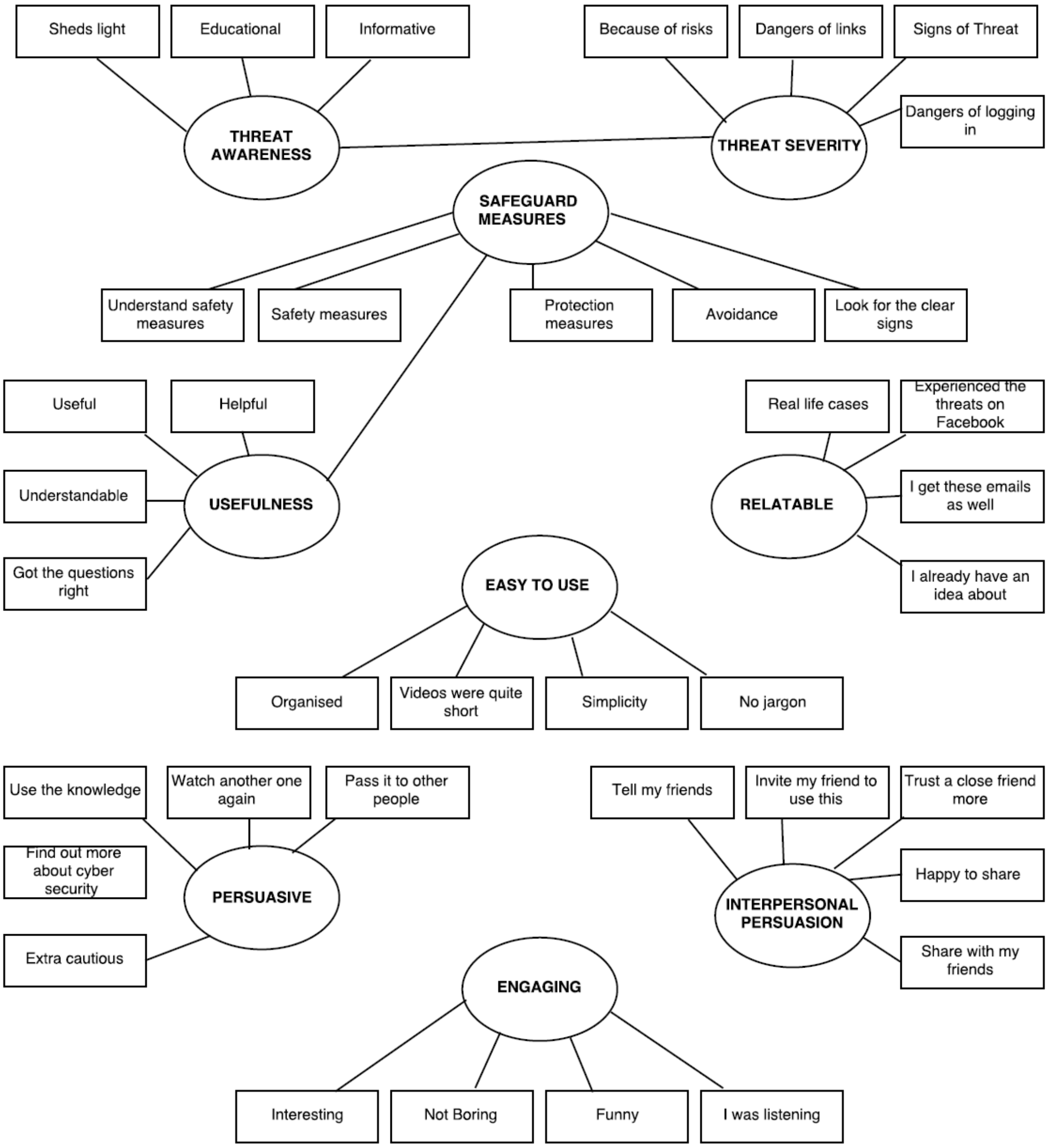


Figure 11 Initial Thematic Map, Showing 9 Main Themes

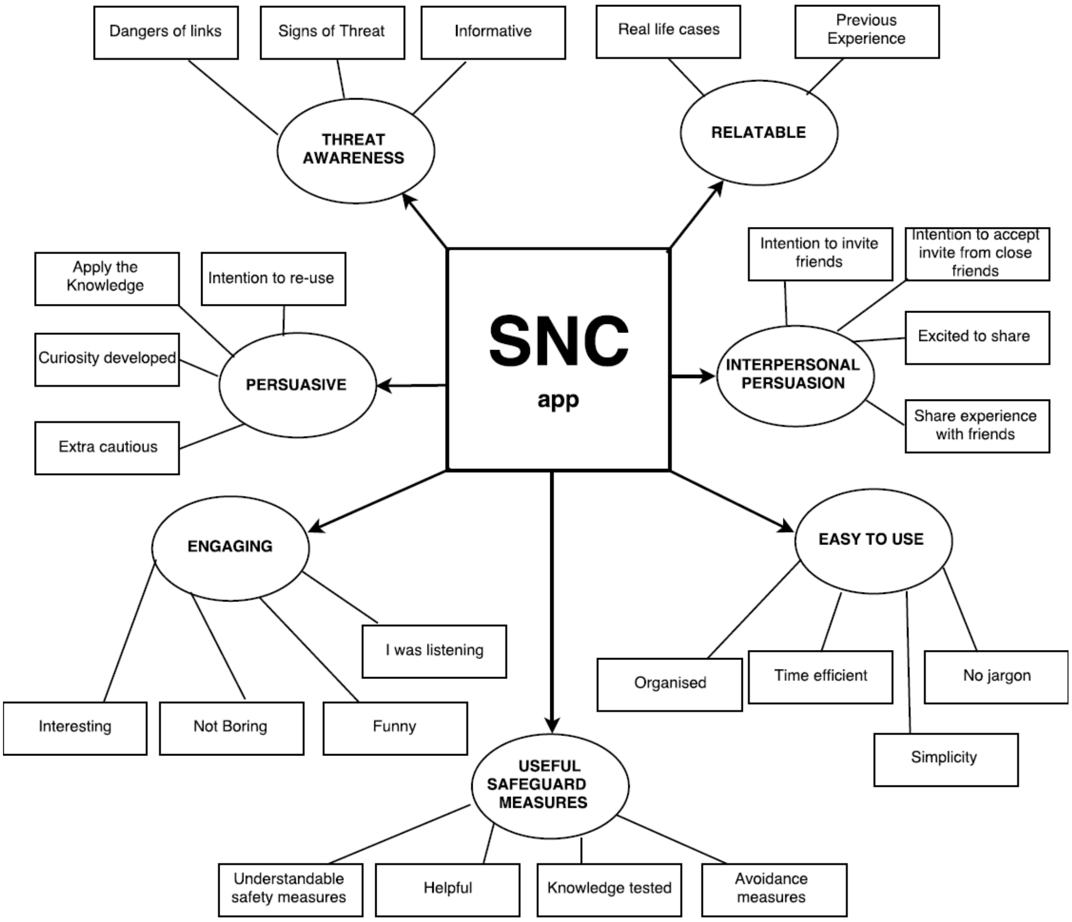


Figure 12 Final Thematic Map, Showing 7 Main Themes

5.4 Semi-Structured Interviews Results

Twenty participants gave verbal feedback on their viewpoints about SNC and their responses supported the results of the paired samples t-tests and the SUS study. For confidentially the identification of the participants is made through numbering: Participant 1, participant 2, etc.

The participants acknowledged that SNC raised their awareness about malware threats in an engaging manner. They appraised the storytelling technique used by SNC and found it relatable and easy to understand. They mentioned that they feel persuaded to apply the knowledge gained to avoid OSN malware threats in the future. Furthermore, the results suggest SNC had an interpersonal persuasive effect on the participants. Most of the participants expressed their willingness to share the SNC experience with their OSN friends. Overall, the key findings from the thematic analysis suggests that SNC 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. These are discussed in more detailed next.

5.4.1 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. Supporting statements from participant 6 are:

“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?”

Previous studies argue that malware threat awareness has not received adequate attention. Most organisations predominantly focus on refining the capabilities of their firewalls and anti-malware software which are solely unable to circumvent malware threats (Ferreira et al., 2015; Shaw et al., 2009; Stephanou and Dagada, 2014; Workman, 2007). More often, the consequence of unawareness leads to exploitation of the biggest weakness in the cybersecurity landscape – the social engineering of humans. The videos on SNC demonstrate the proficiency to make users aware of provoking their thought processes. Supporting statements from participant 5 are:

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

Motivating OSN users to think about malware threats increases consciousness of every single interaction they make online. Additionally, threat awareness has a significant theoretical foundation. Ikhalia et al., (2017) argue that a key construct of TTAT-MIP which influences threat avoidance motivation is – perceived threat. Perceived severity strongly affects perceived threat. The result of the semi-structured interviews validates this construct because most of the participants admitted their vulnerability having identified the dangers of carelessly downloading software through malicious links on OSNs. Participant 4 comments:

“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."

The findings suggest a need to stress the immense dangers of OSN malware threats may have a significant influence on the depth of users’ security awareness. In other contexts, however, this finding may not apply; for example, it is a public debate that smoking addicts simply do not quit smoking because of its associated health hazards. Other predisposing factors could influence their decision to quit smoking.

In the context of OSN malware threats, users need more than mere warnings such as *“be careful of what you click”*; they need to be informed on the short and long-term negative consequences of clicking a malware link. By intensifying security awareness on the psycho-socio and economic severity of OSN malware threats, users’ threat avoidance capabilities could reach unprecedented depths.

5.4.2 Relatability

Relatability describes the quality or state of being relatable. Unpredictably, some participants acknowledged this quality after watching the videos on SNC. For example, Participant 3 commented:

“It iterated things I already have an idea about”

A key noteworthy point in the above statement is – “iterated”. We argue that iterating an already known concept makes it relatively easy for OSN users to retain their security awareness and consequently their security behaviour. According to Ikhalia and Serrano, (2015), one of the limitations of existing security awareness systems is – the lack of contextual knowledge. Contextualised awareness implies that information on threat avoidance need to be delivered to users relative to the technology setting through which they are being exploited. In the case of SNC, we employed a storytelling technique to accomplish this task. As earlier mentioned, SNC adopted previous cases of OSN malware attacks and presented them to users in the form of animation videos. Such a technique was positively appraised by most participants as it made the security awareness information somewhat relatable to their on-going OSN experience. Supporting statements from Participant 1 are:

“I think it’s very useful, the real-life cases idea was very good”

“The little story really helps”

From the participants’ statements, it is 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, this study avoided disseminating security awareness information in an abstract manner. The value of relatability could be drawn from its ability to stimulate the interest of OSN users. According to 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 (Hutter et al., 2013; Lin and Lu, 2011). As a result, a pleasant setting is created for the promotion of the idea/product/service. The relatable quality of SNC is a useful tactic as everyday events (real-life cases of OSN malware threats) are used to attach emotions to the security awareness videos.

5.4.3 Persuasive

Persuasion describes the extent to which SNC influenced the participants to change their security behaviour. The study identified sub-themes such as: (1) Application of the Knowledge; (2) intention to reuse; (3) curiosity developed; and (4) extra cautious. All these sub-themes provide substantial evidence to support a fundamental construct within TTAT-MIP: Avoidance behaviour. Further explanation of each of these sub-themes is found next.

Application of 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. Supporting statements from Participant 2 are:

“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 participants acknowledged their intention to use SNC in gaining more awareness about OSN malware threats. For example, Participant 8 comments:

“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 cybersecurity. Supporting statements from Participant 7 are:

"It kept me wanting to listen and to find out more about cybersecurity"

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

Extra cautious. The participants admitted that through SNC, they learnt the need to be extra careful when carrying out their online social networking activities. Supporting statements from Participant 10 are:

"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 provide evidence that SNC was able to persuade the participants into making verbal declarations to reuse the app, apply the knowledge acquired, seek further knowledge within cybersecurity and become extra cautious while on OSNs. Based on the underlying theoretical model (TTAP-MIP) there is substantial evidence that OSN users' avoidance motivation could influence their actual avoidance behaviour. In the context of this study, avoidance behaviour depicts whether OSN users would develop the intention to seek awareness using SNC and regularly update their knowledge as well. Nonetheless, the persuasive nature of SNC is found to be well-matched with the TTAT-MIP model.

5.4.4 Interpersonal Persuasion

Almost every participant in this study showed a tendency to share their security awareness experience using SNC with their friends. Interpersonal persuasion defines how willing the participants are to invite their OSN friends to use SNC for security awareness. The current study expected SNC would stimulate interpersonal persuasion as the SNC theoretical model TTAT-MIP suggests. Supporting statements from Participant 12 are:

"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 (Fogg, 2008). One of the significant values that interpersonal persuasion brings to SNC 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 states 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 SNC because many OSN users are more inclined to use products/services recommended by their friends. Supporting statements from Participant 13 are:

"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 SNC. Therefore, SNC has been developed with technological features to facilitate interpersonal persuasion at scale.

With hindsight, SNC has the features for users to observe the level of their friends' security awareness; it then becomes relatively seamless for OSN users to estimate the potential vulnerability of their friends which may stimulate a revolutionary security culture shift. In this context Participant 15 comments:

"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 of 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.

5.4.5 Engaging

The findings show that the participants perceived SNC 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. Supporting statements from Participant 16 are:

"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 is evident that the manner in which security awareness was conveyed to OSN users through SNC, attracted their attention substantially. In the systematic literature review conducted by Ikhalia and Serrano (2015), one of the factors identified for designing effective security awareness for OSN users is – end-user engagement.

5.4.6 Ease-of-use

There is substantial evidence to support the ease-of-use of SNC. In the context of this study, ease-of-use describes the degree at which SNC can be seamlessly used. As previously mentioned, the functionalities 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. Supporting statements from Participant 17 are:

“I mean it 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 with the typical cybersecurity setting. We ensured that considerable efforts were invested in simplifying the security awareness information to make it appealing to all classes of users regardless of their computing background. Supporting statements from Participant 18 are:

“The message was put across very clearly."

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

Additionally, the participants positively appraised the short time constraints of SNC’s security awareness videos. They mentioned how straightforward the videos were organised without being boring. Supporting statements from Participant 19 are;

“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”

In line with the fundamental theoretical model TTAT-MIP, ease-of-use is found to support a key independent construct - safeguard costs. Safeguard costs is the time and effort needed to use a safety measure to avoid a malware threat on OSNs.

5.4.7 Useful Safeguard Measures

The findings also show that the participants perceived the safeguard measures of SNC as useful. Safeguard measures describe the steps taken to avoid a malware threat. Supporting statements from Participant 20 are:

“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”

Similarly, the construct – safeguard effectiveness included in TTAT-MIP - provides support for this finding. Arguably, OSN users are inclined to consider the perceived effectiveness of a safeguard measure before using it.

6 Discussion of the Results

The results of the experimental design provide evidence supporting SNC as having a significant effect on users' threat avoidance behaviour. The SUS score showed a significantly high usability level of 82.9 which suggests that the SNC app is not only effective at improving users' behaviour, OSN users found the system useful as well. According to results from a thematic analysis of participant feedback, SNC was found to be persuasive, interpersonal persuasive, engaging, easy to use, relatable, informative and generally useful.

Reflecting on the TTAT-MIP factors that influence the threat avoidance motivation of OSN users, safeguard cost relates to the ‘ease of use' element and perceived threat relates to the informative element identified from results of the semi-structured interview. SNC is seen to be informative due to the relatively good level of awareness it provided participants' during the experimental validation.

Interpersonal persuasion was an essential element identified. Users mentioned how SNC enhanced their persuasion to invite their OSN connections, particularly the vulnerable ones to improve their threat avoidance skills. The interpersonal persuasive element can be linked to 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 from the SUS study and paired sample t-test respectively. This means that the TTAT-MIP model was tested both theoretically through Structural Equation Modelling, and practically through SCN adding further credibility to TTAT-MIP.

7 Conclusion and Further Work

Online social networks (OSNs) are designed to improve social relationships amongst users. These users share different kinds of information such as lifestyles, careers, interests, activities, and other significant information. 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 considerable risk to user privacy and security.

The structure of OSNs is helping malicious users to carry out their activities without the possibility of detection. Baskerville & Rowe (2012) argue that as functionality increases in IT systems, security threats facing users increases proportionately. There is a need, therefore, for a more proactive measure to undercut these threats facing 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 research identified that the success of a system for OSN security awareness must consider factors such as: Persuasion, interpersonal persuasion, relatability, and ease-of-use. Additionally, such a system should also be overtly useful and engaging while making OSN users aware of the specific threats and avoidance measures to ensure that their digital assets and identities are kept secure. From the participants' statements, it is reasonably suggestive to attribute the perceived helpfulness of 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.

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, all providing substantial evidence to support a fundamental construct within TTAT-MIP – avoidance behaviour.

The evaluation of the SNC in this study has potential implications for 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 knowledge. The IT group can identify the current and potential security concerns. During Security awareness training the IT group can simulate malware attack incidents based on relatable events as suggested from the practical evaluation of SNC, which could compel employees to think before performing any online activity and keep them a step ahead of malware attackers.

Security awareness is not only for lower and middle management, but it is also considered for senior management staff. Constructing a security awareness program using TTAT-MIP supports 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.

Future research may involve exploring a field experiment or applied research to investigate the impact of SNC in real-world settings without any form of control. Research efforts should be invested to study the scalability and adaptability of SNC in other social network platforms. The outcome of such research may contribute significantly to the field of behavioural science which may effectively elucidate the degree to which people avoid malware threats when influenced by their online connections.

8 References

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

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.

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.

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.

Cheng, X., Dale, C. and Liu, J. (2008), “Statistics and social network of YouTube videos”, *IEEE International Workshop on Quality of Service, IWQoS*, pp. 229–238.

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

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.

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

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.

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

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.

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.

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

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.

Hanna, R., Rohm, A. and Crittenden, V.L. (2011), "We're all connected: The power of the social media ecosystem", *Business Horizons*, "Kelley School of Business, Indiana University", Vol. 54 No. 3, pp. 265–273.

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.

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. (2017), *A Malware Threat Avoidance Model for Online Social Network Users*, Brunel University.

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., Serrano, A. and Arreymbi, J. (2018), "Deploying Social Network Security Awareness Through Mass Interpersonal Persuasion (MIP)", *International Conference on Cyber Warfare and Security*.

Ikhalia, E., Serrano, A., Bell, D. and Arreymbi, J. (2017), "Developing and Implementing TTAT-MIP for the Avoidance of Malware Threats through Online Social Networks", *IADIS International Journal on WWW/Internet*, Vol. 15 No. 1, pp. p31-46.

Kaplan, A.M. and Haenlein, M. (2010), "Users of the world, unite! The challenges and opportunities of Social Media", *Business Horizons*, Vol. 53 No. 1, pp. 59–68.

kaspersky. (2015), "Zeus Trojan Malware Threat | Zbot and Other Names | Kaspersky Lab UK", *Www.Kaspersky.Co.Uk*.

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

Lin, K.Y. and Lu, H.P. (2011), “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.

Luo, X., Brody, R., Seazzu, A. and Burd, S. (2011), “Social Engineering”, *Information Resources Management Journal*, Vol. 24 No. 3, pp. 1–8.

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

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

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), “Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)”, *Computers and Security*, Elsevier Ltd, Vol. 42, pp. 165–176.

Riccardi, M., Di Pietro, R., Palanques, M. and Vila, J.A. (2013), “Titans’ revenge: Detecting Zeus via its own flaws”, *Computer Networks*, Vol. 57 No. 2, pp. 422–435.

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.

Rosenkrans, G. (2009), “The Creativeness and Effectiveness of Online Interactive Rich Media AdvertisingRosenkrans, G. (2009). The Creativeness and Effectiveness of Online Interactive Rich Media Advertising. Journal of Interactive Advertising, 9(2), 18–31. http://doi.org/10.1016/”, *Journal of Interactive Advertising*, Vol. 9 No. 2, pp. 18–31.

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.

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. 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.

Soika, K., Reiska, P. and Mikser, R. (2010), “The importance of animation as a visual method in learning chemistry”, *Concept Maps: Making Learning Meaningful*, Vol. 3 No. 10, p. 9.

Solutions, S. (2017), “Paired Sample T-Test”, *Statistics Solutions*.

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.

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.

Turner, D.W. (2010), “Qualitative interview design: A practical guide for novice investigators”, *The Qualitative Report*, Vol. 15 No. 3, pp. 754–760.

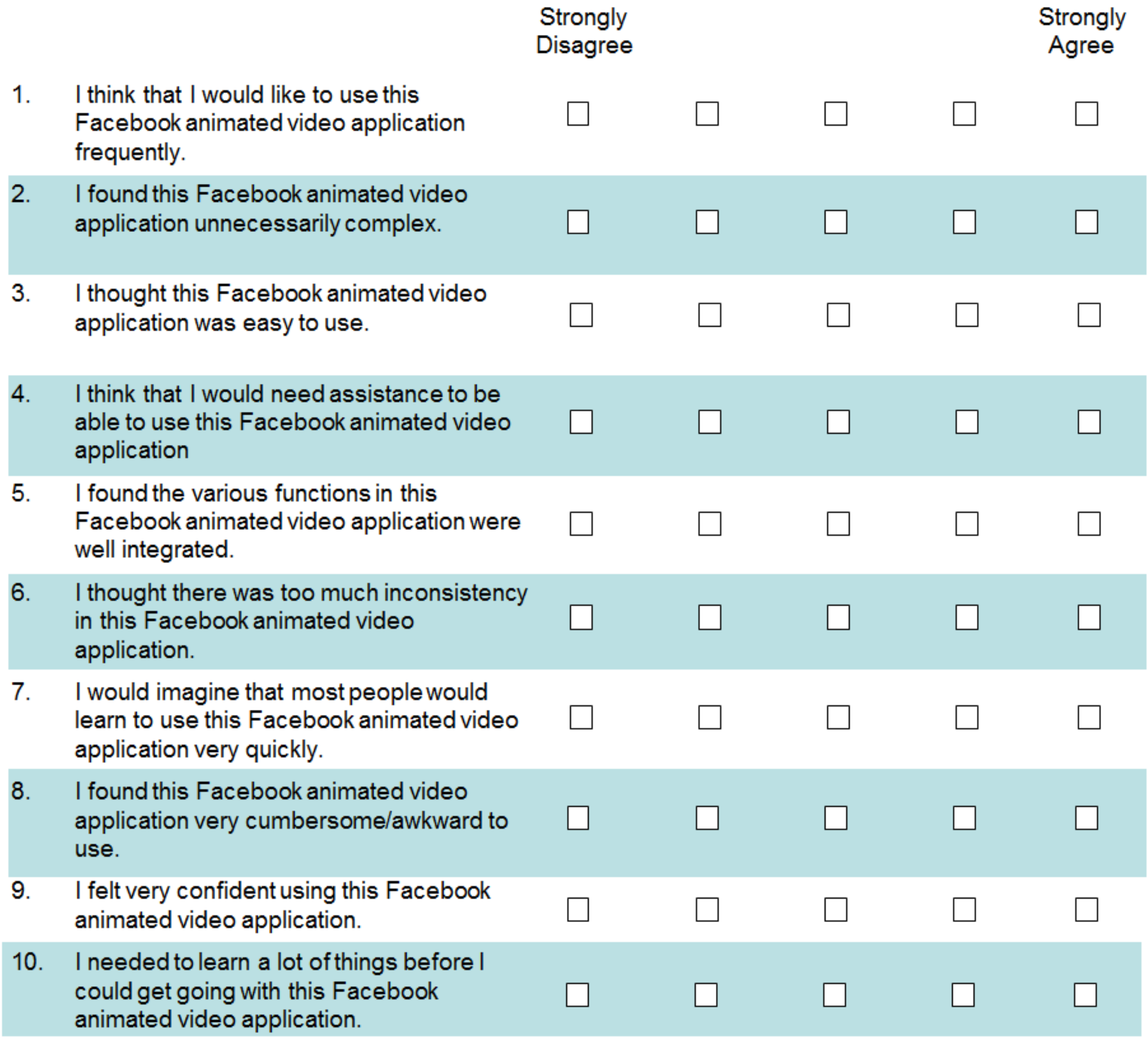
Venkatesh, V. and Brown, S.A. (2001), “A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinats and Emerging Challenges”, *Management Information Systems*, Vol. 25 No. 1, pp. 71–102.

Workman, M. (2007), “Gaining Access with Social Engineering: An Empirical Study of the Threat”, *Information Systems Security*, Vol. 16 No. 6, pp. 315–331.

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, 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.

Appendix 1 SUS Questionnaire Items



		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.	□	□	□	□	□

Appendix 2 Average Score for each SUS Question

Appendix 2: 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