Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full length article

Phishing threat avoidance behaviour: An empirical investigation

Nalin Asanka Gamagedara Arachchilage [a, *], Steve Love [b], Konstantin Beznosov [c]

[a] Australian Centre for Cyber Security, University of New South Wales (UNSW Canberra), Australian Defence Force Academy, Australia
[b] Digital Design Studio, The Glasgow School of Art, United Kingdom
[c] University of British Columbia, Vancouver, Canada

ARTICLE INFO

Article history:
Received 31 July 2015
Received in revised form
9 February 2016
Accepted 15 February 2016
Available online xxx

Keywords:
Usable security
Security awareness
Phishing threats
Security education
Mobile learning
Game based learning

ABSTRACT

Phishing is an online identity theft that aims to steal sensitive information such as username, password and online banking details from its victims. Phishing education needs to be considered as a means to combat this threat. This paper reports on a design and development of a mobile game prototype as an educational tool helping computer users to protect themselves against phishing attacks. The elements of a game design framework for avoiding phishing attacks were used to address the game design issues. Our mobile game design aimed to enhance the users' avoidance behaviour through motivation to protect themselves against phishing threats. A think-aloud study was conducted, along with a pre- and post-test, to assess the game design framework though the developed mobile game prototype. The study results showed a significant improvement of participants' phishing avoidance behaviour in their post-test assessment. Furthermore, the study findings suggest that participants' threat perception, safeguard effectiveness, self-efficacy, perceived severity and perceived susceptibility elements positively impact threat avoidance behaviour, whereas safeguard cost had a negative impact on it.

1. Introduction

Internet technology provides the backbone for modern living enabling ordinary people to shop, socialize, communicate, network and also be entertained via their personal computers and mobile devices such as smartphones. As people's reliance on the Internet grows, so the possibility of hacking and other security breaches increases regularly (Liang & Xue, 2010). Computer users play a major role in helping to make cyberspace a safer place for everyone (Arachchilage, Namiluko, & Martin, 2013). This paper focuses on how the human aspect of security can be influenced to avoid cyber-threats in the computer use.

Cyber-threats commonly include computer viruses and other types of malicious software (malware), unsolicited e-mail (spam), eavesdropping software (spyware), orchestrated campaigns aiming to make computer resources unavailable to the intended users (distributed denial-of-service (DDoS) attacks), social engineering, and online identity theft (phishing). The motivations behind these attacks tend to be either for financial or social gain (Kirlappos & Sasse, 2012; Ng & Rahim, 2005; Woon, Tan, & Low, 2005; Workman Bommer, & Straub, 2008). For example, a DDoS attack could target a bank in order to overwhelm its online banking server and the attacker can exhort money before “giving” the server back to the bank.

One such a cyber-threat that is particularly dangerous to computer users is phishing (Arachchilage, 2015; Arachchilage & Love, 2013, 2014; Arachchilage, Tarhini, & Love, 2015; Hong, 2012; Kirlappos & Sasse, 2012; Kumaraguru, Rhee, Acquisti, et al., 2007; Kumaraguru, Rhee, Sheng, et al., 2007; Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2007). Phishing, however, is a form of *semantic attack* and sometimes referred to as online identity theft, which aims to steal sensitive information such as username, password and online banking details from its victims. In phishing attacks, victims get directed by phishing emails to visit fake replicas (often, for example, purporting to be from the user's bank) of legitimate websites. Phishing attacks are getting more sophisticated day by day, as attackers learn new techniques and change their strategies accordingly (Kirlappos & Sasse, 2012; Hong, 2012; Kumaraguru, Rhee, Sheng, et al., 2007; Kumaraguru, Rhee, Acquisti, et al., 2007; Kumaraguru, Sheng, et al., 2007).

According to APWG Phishing Activity Trends Report (APWG, 2014), more than 75% of phishing attacks target retail services, online payment systems as well as financial institutions. Aaron and Rasmussen (2015) revealed through the Global Phishing Survey

[*] Corresponding author.
E-mail addresses: nalin.asanka@adfa.edu.au (N.A.G. Arachchilage), s.love@gsa.ac.uk (S. Love), beznosov@ece.ubc.ca (K. Beznosov).

http://dx.doi.org/10.1016/j.chb.2016.02.065
0747-5632/© 2016 Elsevier Ltd. All rights reserved.

study, more than 82% of phishing attacks target e-Commerce, banks as well as money transfer industries. Phishing attacks are not mitigated as quickly. The average uptime for phishing attacks in the second half of 2014 was 29 h and 51 min (Aaron & Rasmussen, 2015).

Automated anti-phishing tools have been developed and used to alert users of potentially fraudulent emails and websites. For example, Calling ID Toolbar, Cloudmark Anti-Fraud Toolbar, EarthLink Toolbar, Firefox 2, eBay Toolbar and Netcraft Anti-Phishing Toolbar. However, these tools are not entirely reliable in detecting phishing attacks (Kirlappos & Sasse, 2012; Li, Berki, Helenius, & Ovaska, 2014; Moghimi & Varjani, 2016; Purkait, 2012; Sheng et al., 2007). Even the best anti-phishing tools could miss over 20% of phishing websites (Zhang, Egelman, Cranor, & Hong, 2007). Ye and Sean (2002) and Dhamija and Tygar (2005) have developed a prototype called “trusted paths” (i.e. between the Web browser and its human user) for the Mozilla web browser that is designed to help users verify that their browser has made a secure connection to a trusted website. Authors revealed that the existence of a trusted path from the browser to user does not guarantee that the browser will tell the user true and useful things which aid for their decision-making. As reported, the trusted path should also provide required information to the user to make a trust decision. They also stressed that the web history offers many examples where the reality of a browsing session did not match the user's mental model. Therefore, these systems are still insufficient to combat phishing threats (Arachchilage & Cole, 2011; Arachchilage & Love, 2014; Kirlappos & Sasse, 2012; Purkait, 2012; Sanchez & Duan, 2012; Sheng et al., 2007).

Security experts and phishing attackers are in a rat race today. On the one hand, security experts with the help of application developers will continue to improve phishing and spam detection tools. Nevertheless, the “human” is the weakest link in information security (Arachchilage & Love, 2014; CNN, 2005; Purkait, 2012). On the other hand, attackers continue learning new techniques and changing their strategies according to human frailties, to make phishing attacks successful (Kumaraguru, Rhee, Sheng, et al., 2007; Kumaraguru, Sheng, et al., 2007). This is why researchers consider user education as a means of preventing phishing (Arachchilage & Love, 2014; Downs, Holbrook, & Cranor, 2007; Kirlappos & Sasse, 2012; Kumaraguru, Rhee, Acquisti, et al., 2007; Kumaraguru, Rhee, Sheng, et al., 2007; Kumaraguru, Sheng, et al., 2007; Purkait, 2012; Sanchez & Duan, 2012; Richmond, 2006; Robila & Ragucci, 2006; Sheng et al., 2007).

It has been shown that both academic institutions and government organisations have made a significant effort to provide end user education to enable public understanding of security (Kirlappos & Sasse, 2012). The Anti-Phishing Work Group (APWG, 2016) is a non-profit organisation working to provide anti-phishing educational interventions to enhance the public understanding of security. The US Computer Emergency Readiness Team (US-CERT, 2016) also offers free advice on its website about common security breaches for computer users who have a lack of computer literacy. While a great deal of effort has been dedicated to resolving the phishing threat problem by prevention and detection of phishing emails, URLs and web sites, little research has been done in the area of educating users to protect themselves from phishing attacks (Kirlappos & Sasse, 2012). Therefore, research needs more focus on anti-phishing education to protect users from phishing threats.

The aim of the study reported in this paper was to investigate how one can develop a mobile game that, through motivation, enhances users' avoidance behaviour in order to protect themselves against phishing attacks. Therefore, it asks the following research questions: how does one identify which issues the game needs to address? Once the salient issues are identified, the second question is, what principles should be used to address these issues. The elements of a game design framework by Arachchilage and Love (2013) were used to address these mobile game design issues and presenting information in the game design context. A game prototype was designed and developed for the mobile Android platform using MIT App Inventor Emulator (MIT App Inventor, 2012). Then a think-aloud study was employed to understand the participants' phishing threat avoidance behaviour on the game design framework, after their engagement with the mobile game prototype. Furthermore, pre- and post-tests were used to determine whether or not anti-phishing education takes place after the game play activity.

To summarise, this research evaluated a game design framework introduced by Arachchilage and Love (2013). The game was designed and developed as an educational tool to teach computer users how to thwart phishing attacks. The study results showed a significant improvement of participants' phishing avoidance behaviour and suggested that participants' threat perception, safeguard effectiveness, self-efficacy, perceived severity and perceived susceptibility elements positively impact threat avoidance behaviour, whereas safeguard cost had a negative impact on it.

The reminder of this paper is structured in the following manner. Section 2 discusses the related work. Section 3 describes the game design issues and how we developed the mobile game prototype as an educational tool helping computer users to protect themselves against phishing attacks. In section 4, we discuss the methodology and research designed employed in this research. Section 5 presents the main findings reported in this paper. Section 6 presents a discussion of our findings with the previous research work. Finally, the section 7 provides conclusions and opens up opportunities for future work that may extend the research work reported in this paper.

2. Related work

Previous research has indicated that technology alone is insufficient to address critical IT security challenges. To date, there has been little work published on the human aspect of people performing security checks and protecting themselves from various attacks which are imperative to cope up with cyber-threats such as phishing attacks (Alsharnouby, Alaca, & Chiasson, 2015; Anderson & Agarwal, 2006; Arachchilage & Cole, 2011; Arachchilage & Love, 2014; Aytes & Terry, 2004; Ion, Reeder, & Consolvo, 2015; Liang & Xue, 2009; Liang & Xue, 2010; Ng & Rahim, 2005; Susan, Catherine and Ritu, 2006; Woon et al., 2005; Workman et al., 2008). Many discussions related to information security have ended with conclusions similar to the one by (Gorling, 2006): “*if we could only remove the end-user from the system we would be able to make it secure*”. Where it is impossible to completely eliminate the end-user from the computer system (for example, in home computer use), some argue that the best possible approach for computer security is to educate the end-users in security prevention (Kirlappos & Sasse, 2012; Mitnick & Simon, 2002; Schneier, 2000). Previous research has discovered well designed end-user security education can be effective (Le Compte, Elizondo, & Watson, 2015; Kumaraguru, Rhee, Acquisti, et al., 2007; Kumaraguru, Rhee, Sheng, et al., 2007; Kumaraguru, Sheng, et al., 2007; Sheng et al., 2007). This could be web-based training materials, contextual training and embedded training to enhance users' ability to avoid phishing threats. One objective of the current work described in this paper is to find effective ways to educate people on how to identify and avoid phishing attacks.

Kirlappos and Sasse (2012) claimed that security education should consider the drivers of end user behaviour rather than warning users of dangers. Therefore, well-designed security education should develop threat perception where users are aware that such a threat is present in the cyberspace. It should also encourage users to enhance avoidance behaviour through motivation to protect them from malicious IT threats.

So, how does one educate computer users in order to prevent them from becoming victims of phishing threats? The study reported in this paper designs and develops a mobile game as a tool for educating computer users about phishing attacks. This concept is grounded on the notion that computer games not only can provide education (Le Compte et al., 2015; Raybourn & Waern, 2004; Walls, 2012; Wang, Øfsdahl, & Mørch-Storstein, 2009), but also offer a better natural learning environment, which motivates the user to keep engaging with it (Amory & Seagram, 2003; Boyinbode & Ng'ambi, 2015; Prensky, 2001; Walls, 2012). Additionally, game-based education attracts and retains the user until the end of the game by providing immediate feedback.

Sheng et al. (2007) developed a game to evaluate participants' ability to identify fraudulent web sites before and after spending 15 min engaged in one of their three anti-phishing training activities: playing the game; reading an anti-phishing tutorial they created based on the game; or reading existing online training materials. They found that participants who played the game were better able to identify phishing websites after engaging 15 min of training compared to participants in other conditions. However, they also reported 31 percent of users could not still differentiate between good websites and bad ones (Sheng et al., 2007). Our mobile game developed in this research aimed to enhance the users' avoidance behaviour through motivation to protect themselves against phishing threats.

The most significant feature of a mobile environment is "*mobility*" itself such as mobility of the user, mobility of the device and mobility of the service (Parsons, Ryu, & Cranshaw, 2006). It enables users to be in contact while they are outside the reach of traditional communicational spaces (Boyinbode & Ng'ambi, 2015). For example, a person can play a game on his mobile device while travelling on the bus or train, or waiting in a queue.

Some innovators strongly argue that desktop computers will disappear from the society while new handheld devices and their interfaces will turn into ubiquitous, pervasive, invisible and be embedded in the surrounding environment (Shneiderman, 1987). They also believe that those devices will be context-aware, attentive and perceptive, sensing users' desires and providing feedback through ambient displays that glow, hum, change shape or blow air. Furthermore, some researchers and technology experts predict advanced mobile devices that are wearable, or even implemented under the human skin (Shneiderman, 1987). For example, individual implanted wireless sensors that can be used to track users entering premises (Shneiderman, 1987).

There is a trend in games technology targeting handheld devices (Denk, Weber, & Belfin, 2007; Klopfer, 2008). For example, touch-based interfaces introduced on iPhone/iPod, changed computer based educational games to the emerging mobile-based platform. Those touch-based interfaces enable the player to interact with digital objects within the gaming environment much easier than navigating through the keyboard. As a consequence of those emerging mobile technology, iPhone and Android devices, now low-cost app stores are awash with games.

Sheng, Holbrook, Kumaraguru, Cranor, and Downs (2010) have conducted a role-play survey with over 1000 online survey respondents to study who falls for phishing attacks. Their study showed that participants of age range between 18 and 25 are more susceptible to phishing attacks than other age groups. The studies reported in our paper, included participants from a diverse group of staff and students at Brunel University and the University of Bedfordshire, UK, including people who were concerned with computer security. Our research aimed to design and develop a mobile game prototype as an educational tool to teach computer users how protect themselves against phishing attacks.

3. Game design issues

The main focus of the proposed game design is to educate computer users to thwart phishing attacks. To answer our research question (how does one identify which issues the game needs to address?), we used the issues drawn from phishing threat avoidance in order to explore the principles needed for structuring the design of the game in the context of computer use. A game design framework introduced by Arachchilage and Love (2013), examined individuals' phishing threat avoidance behaviour by using game-based anti-phishing education. We incorporated several elements of their framework into our design. The hypotheses (H) are described as follows:

Consistent with the game design framework (Fig. 1), the user's phishing threat avoidance behaviour is determined by avoidance motivation, which, in turn, is affected by perceived threat. Perceived threat is influenced by perceived severity and susceptibility as well as their combination (interaction effect). Users' avoidance motivation is also determined by the three constructs such as safeguard effectiveness, safeguard cost and self-efficacy.

Whilst the game design framework identifies the issues that the game design needs to address, it should also indicate how to structure this information and present it in a game context. To this end, we aimed to develop threat perceptions, making individuals more motivated to avoid phishing attacks and use safeguarding measures.

3.1. What to teach?

Possible phishing attacks can be identified in several ways, such as by carefully looking at the website address, so called Universal Resource Locator (URL), signs (i.e., VeriSign, https, Extended Validation (EV) certificates), content and jargon of the web page, the lock icon(s) on the browser chrome, the context of the email message and the general warning messages displayed on the website (Downs et al., 2007; Wu, Miller, & Garfinkel, 2005; Shekokar, Shah, Mahajan, & Rachh, 2015). Previous research has identified that existing anti-phishing techniques based on URLs are not robust enough for phishing detection by users (Garera, Provos, Chew, & Rubin, 2007; Purkait, 2012; Sheng et al., 2007). Alsharnouby et al. (2015) evaluated whether improved browser security indicators and increased awareness of phishing have led to users' improved ability to detect against phishing attacks. They employed an eye-tracking device to obtain objective quantitative data on which visual cues draw users' attention as they determine the legitimacy of websites. Though many participants reported paying attention to the URL, the study revealed they either tried to recall familiar URLs or used heuristics such as assessing the simplicity of the URL (Alsharnouby et al., 2015).

Garera et al. (2007) strongly argued that it is often possible to differentiate phishing websites from legitimate ones by carefully looking at the URL without having any knowledge of the content of the corresponding website, sings and symbols such as "VeriSign" signs or "Padlock" icons. Therefore, we argue that teaching people not to fall for phishing through URLs is important and well-designed anti-phishing education based on URLs can contribute to stopping users falling for phishing attacks.

The objective of the anti-phishing mobile game design prototype reported in this paper is to teach users how to identify phishing URLs. As such, the game design should develop an

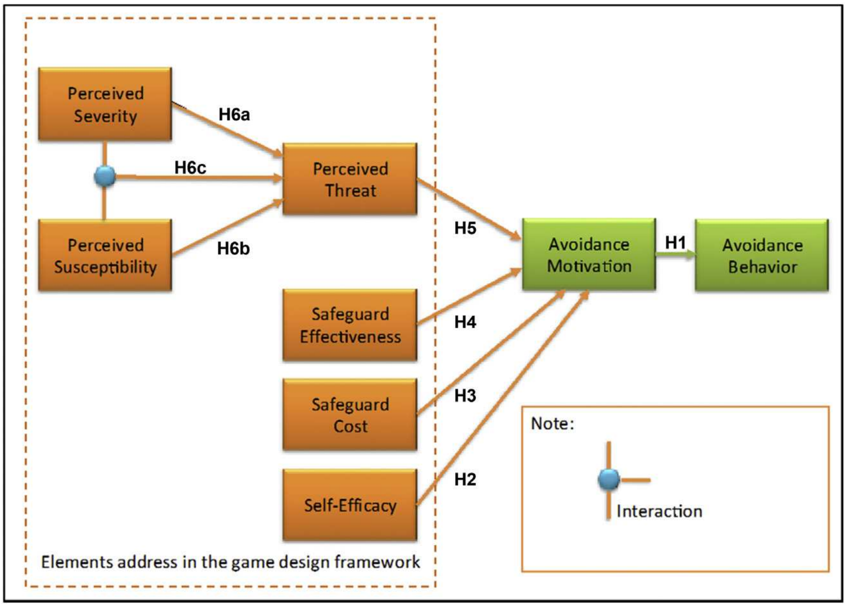


Fig. 1. A game design framework for avoiding phishing attacks (Arachchilage & Love, 2013) H1. Avoidance motivation positively affects the avoidance behaviour. H2. Self-efficacy positively affects avoidance motivation. H3. Safeguard Cost negatively affects avoidance motivation. H4. Safeguard Effectiveness positively affects avoidance motivation. H5. Perceived Threat positively affects avoidance motivation. H6a. Perceived Severity positively affects avoidance motivation. H6b. Perceived Susceptibility positively affects avoidance motivation. H6c. The combination of Perceived Severity and Perceived Severity positively affects avoidance motivation.

awareness of identifying the features of URLs. For example, legitimate websites usually do not have numbers at the beginning of their URLs such as http://81.153.192.106/.www.hsbc.co.uk.

3.2. Story and mechanism

The game is based on a scenario of a character of a small fish and ‘his’ teacher who lives in a big pond. The main character of the game is the small fish, who wants to eat worms to become a big fish. The game player role-plays as a small fish. However, he should be careful of phishers those who try to trick him with fake worms. This represents phishing attacks by developing threat perception. Each worm is associated with a website address (URL), which appears in a dialogue box. We employed the approach of URL classification used in Sheng et al. (2007) and Dhamija, Tygar, and Hearst (2006) studies. In our study, a total of 10 URLs were designed to randomly display five good worms and five bad worms. The list of URLs is shown in Table 1. The small fish's job is to eat all the real worms associated with legitimate website addresses, and reject fake worms associated with fake website addresses, before its time is up. This scenario is for developing the severity and susceptibility of the phishing threat in the game design.

The other character is the small fish's teacher, who is a mature and experienced fish in the pond. If the worm associated with the URL is suspicious and if it finds it difficult to identify the website, the small fish can go to ‘his’ teacher and request help. The teacher helps him by giving some tips on how to identify bad worms. For example, “website addresses that have numbers in the front are generally scams” or “a company name followed by a hyphen in a URL is generally a scam”. Whenever the small fish requests help from the teacher, the user's score will be reduced by a certain amount (in this case by 100 s) as a payback for safeguard measure. This design choice attempts to address the safeguard effectiveness and the cost of paying for the safeguard in the game design. The consequences of the player's actions are shown in Table 2.

The proposed game design randomly generates a worm associated with a URL each time. The URL could be either phishing or legitimate. When the user plays the game from the beginning to the

Table 1
List of URLs displayed in the game.

Game focus	Real or phishing	Examples	“Tips/Training messages” from big fish
Appropriate URL	*Real*	*http://www.nationwide.co.uk/default.htm*	“URLs with well-known domain and correctly spelt are legitimate”
IP address URL	*Phishing*	*http://147.46.236.55/PayPal/login.html*	“Don't trust URLs with all numbers in the front”
Miss spelt URL	*Phishing*	*www.paypa1.com*	“Don't trust URLs with misspelled known websites”
Appropriate URL	*Real*	*www.smile.co.uk/*	“URLs with well-known domain and correctly spelt are legitimate”
Sub domain URL	*Phishing*	*www.argos.co.uk.myshop.com*	“Don't trust URLs with large host names that contained a part of a well-known web addresses”
Similar and deceptive domains	*Phishing*	*http://www.msn-verify.com/*	“Company name followed by a hyphen usually means, it's a scam website”
Appropriate URL	*Real*	*http://www.halifax.co.uk/aboutonline/home.asp*	“URLs with well-known domain and correctly spelt are legitimate”
Similar and deceptive domains	*Phishing*	*www.ebay-security.com*	“Companies don't use security related keywords in their domains”
Miss spelt URL	*Phishing*	*www.online.ll0ydstsb.co.uk*	“Don't trust URLs with misspelled known websites”
Appropriate URL	*Real*	*https://ibank.barclays.co.uk/*	“URL with ‘https://’ usually a legitimate website”

Table 2
Scoring scheme and consequences of the player's action.

	Good worm (associate with legitimate URL)	Bad worm (associate with phishing URL)
Player eats	Correct, gain 10 points (each attempt = 1 point)	False negative, (each attempt loses 100 s out of 600 s)
Player reject	False positive, (each attempt loses 100 s out of 600 s)	Correct, gain 10 points (each attempt = 1 point)

end, the complexity of the URLs presented is dramatically increased. The user is presented with a worm associated with a different URL each time throughout the game. This helps the user to gain conceptual knowledge on how to identify URLs. Therefore, the game design aims at the development of the self-efficacy in preventing oneself from phishing attacks.

The proposed game design is based on a story and presented to the player using digital objects; attractive digital objects were integrated into the game such as sounds and graphics in order to engage the user within the gaming environment. This included sound effects to provide feedback on underwater background music and the player's actions on the selection of either a good or bad worm. For example, a light water bubbling sound played in the background throughout the game to create the feeling that the user (i.e., the small fish) lives in the pond.

3.3. *Mobile game prototype*

To explore the viability of using a game for preventing phishing attacks, a working prototype model was developed for a mobile telephone using MIT App Inventor Emulator (Fig. 2).

The player is given instructions before starting the game. Then the main menu of the mobile game prototype appears, along with underwater background and the corresponding sound effects. A light water bubbling sound is played in the background throughout the game to make the user feel that they are in the pond. A URL is displayed with each worm; where the worms are randomly generated.

If the worm associated with URL is legitimate, then the user is expected to tap on the worm in order to increase their score. However, if the user fails to identify the legitimate URL, then remaining lives will be reduced by one point. On the other hand, if the worm associated with the URL is phishing, then the user is also expected to tap on the "AVOID" button to reject the URL, in order to increase the score. If the user fails to do this, then remaining lives will be reduced by one point. If the worm associated with the URL is suspicious and if it is difficult to identify, the user can tap on the big fish (in this case, teacher fish) to request help. Then some relevant tips will be displayed just below the URL. For example, "website addresses associate that have numbers in the front are generally scams." Whenever the user taps on the big fish, the time left is reduced by 100 points (in this case 100 s). Finally, the user gains 10 points if all given URLs were correctly identified within 5 lives and 600 s.

4. Methodology and research design

Our study employed a usability study of the game prototype as the first step to assess the subjective satisfaction of mobile game prototype interface. This is based on the notion that learning based on mobile game takes place if participants are satisfied with the overall game prototype. Then a think aloud experiment conducted along with a pre- and post-test as the second step of the research study to assess the game design framework introduced by Arachchilage and Love (2013) through the developed mobile game prototype.

4.1. *Data collection*

This study employed both qualitative and quantitative data collection approaches. A quantitative data collection was employed to collect data about the usability of the mobile game prototype. To this end, we employed System Usability Scale (SUS), which is used to measure users' subjective satisfaction of mobile game interface usability (Brooke, 1996). Tullis and Stetson (2004), as well as Finstad (2006) suggest sample sizes of at least 12–14 participants

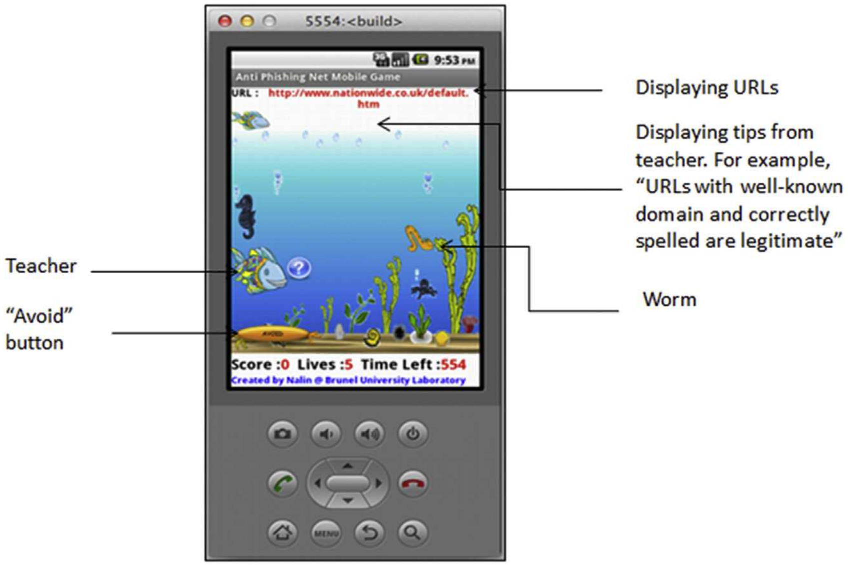

5554:<build>
9:53 PM
Anti Phishing Net Mobile Game
URL : http://www.nationwide.co.uk/default.htm
Score :0 Lives :5 Time Left :554
Created by Nalin @ Brunel University Laboratory
Displaying URLs
Displaying tips from teacher. For example, "URLs with well-known domain and correctly spelled are legitimate"
Worm
Teacher
"Avoid" button
AVOID
MENU

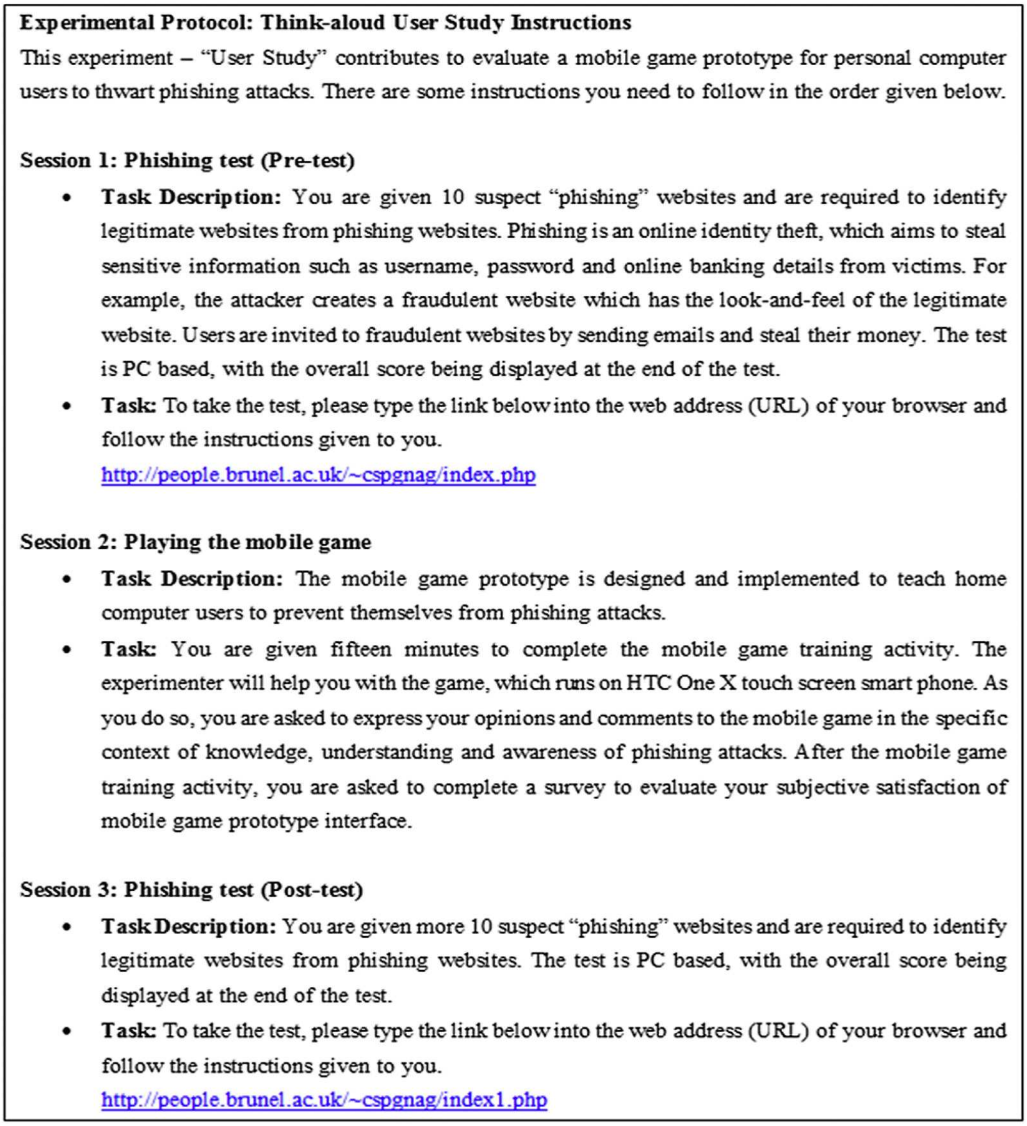
Fig. 2. The mobile game prototype on MIT App Inventor Emulator.

are needed to get reasonably reliable results for the conditions of the study. SUS uses a five-point Likert scale with anchors for strongly agree and strongly disagree. However, Finstad (2006) found that a significant amount of non-native English speakers failed to understand word "cumbersome" in SUS's item 8: "I found the system to be very cumbersome to use" (Finstad, 2006; Lewis & Sauro, 2009). Since our study included participants with multinational background, the word "cumbersome" was replaced with "awkward", per suggestion from Finstad (2006). The set of questionnaire items reproduced SUS for measuring the users' subjective satisfaction of our mobile game prototype interface is shown in Appendix A (Brooke, 1996).

Along with the pre- and post-test, a think-aloud protocol was employed to collect data about the user impact on the elements of the game design framework after their engagement with the mobile game prototype. The corresponding instructions are provided in Fig. 3.

4.2. *Pilot study*

In the pilot study, we recruited eight first-year undergraduate students from the Department of Computer Science and Technology at the University of Bedfordshire, UK. The pilot study revealed that the mobile game was effective in teaching participants to look at URL on their browser's address bar, when assessing a website's legitimacy. Participants scored 49 percent in the pre-test and 78 percent in the post-test of identifying phishing or legitimate websites after playing the mobile game. There was a considerable improvement of participants' results (29 per cent) in the post-test during the pilot study. All the participants stated that their decisions were based on looking at the address bar, when evaluating the websites in the post-test. Furthermore, they stated that they made only very few attempts to look at the address bar when evaluating the websites in the pre-test. Therefore many participants used incorrect strategies to determine website legitimacy. For example, one of the common strategies consisted of checking whether or not the website was designed professionally. However, this may not be a useful strategy, as many phishing websites are exact replica of legitimate websites (Sheng et al., 2007). The attacker can easily mimic any professional website from the source code of the particular page provided by the browser. Moreover, they highlighted that the mobile game was somewhat effective in



Experimental Protocol: Think-aloud User Study Instructions

This experiment – "User Study" contributes to evaluate a mobile game prototype for personal computer users to thwart phishing attacks. There are some instructions you need to follow in the order given below.

Session 1: Phishing test (Pre-test)

- **Task Description:** You are given 10 suspect "phishing" websites and are required to identify legitimate websites from phishing websites. Phishing is an online identity theft, which aims to steal sensitive information such as username, password and online banking details from victims. For example, the attacker creates a fraudulent website which has the look-and-feel of the legitimate website. Users are invited to fraudulent websites by sending emails and steal their money. The test is PC based, with the overall score being displayed at the end of the test.
- **Task:** To take the test, please type the link below into the web address (URL) of your browser and follow the instructions given to you.
  http://people.brunel.ac.uk/~cspgnag/index.php

Session 2: Playing the mobile game

- **Task Description:** The mobile game prototype is designed and implemented to teach home computer users to prevent themselves from phishing attacks.
- **Task:** You are given fifteen minutes to complete the mobile game training activity. The experimenter will help you with the game, which runs on HTC One X touch screen smart phone. As you do so, you are asked to express your opinions and comments to the mobile game in the specific context of knowledge, understanding and awareness of phishing attacks. After the mobile game training activity, you are asked to complete a survey to evaluate your subjective satisfaction of mobile game prototype interface.

Session 3: Phishing test (Post-test)

- **Task Description:** You are given more 10 suspect "phishing" websites and are required to identify legitimate websites from phishing websites. The test is PC based, with the overall score being displayed at the end of the test.
- **Task:** To take the test, please type the link below into the web address (URL) of your browser and follow the instructions given to you.
  http://people.brunel.ac.uk/~cspgnag/index1.php

Fig. 3. Think-aloud protocol instructions.

learning different URL patterns to differentiate phishing URLs from legitimate ones.

The pilot study findings suggest that the participants learnt most of the URL-related concepts that we aimed to teach using the mobile game. For example, most participants seemed to understand that URLs beginning with numbers are usually a sign of scam. However, the study also found that some participants applied the lessons learnt from the mobile game incorrectly. They misapplied the rule about URLs that have all numbers in the front are usually scams. For example, *www2.fdic.gov* as a phishing website, because the URL contained the number 2 after the "*www*". This is because the mobile game prototype did not include a URL with the number after the *www* such as *www2* or *www4*. However, participants were tested on their ability to identify the above type of URLs in the post-test. Therefore, we included URL '*www2.fdic.gov*' in our mobile game prototype before launching the main study.

4.3. Main study

4.3.1. Participants

The think-aloud study along with a pre- and post-test was run with 20 participants to observe their understanding, knowledge, and awareness of phishing attacks through the mobile game prototype. Participants were recruited from the Brunel University, UK, who were 3rd year computer science undergraduate students. They were invited to participate by sending email to their university email addresses and posting Facebook message asking for their help. Participants were invited to the computer laboratory at Brunel University. The permission was taken from the ethics committee at Brunel University before conducting the think-aloud study.

Participants' ages ranged from 18 to 25, with a gender split of 65 percent male and 35 percent female. The majority had more than 20 h per week of Internet experience. All of them had the experience of Internet shopping at least once. Furthermore, all participants had the experience of using a smart phone for more than a year. Each participant took part in the think-aloud study on a fully voluntary basis. A summary of participants' demographics is shown in Table 3.

4.3.2. Procedure

The data was collected using the think-aloud procedure along with a pre- and post-test. The think-aloud study was conducted in-person with each participant taking approximately one hour. First, each individual participant was given an explanation of the nature of the think-aloud experimental study and asked to sign a consent form. They were informed that the think-aloud experiment was about testing the participant's understanding of phishing threat awareness through the mobile game prototype. They were also told that they were free to withdraw from the experiment study at any time and without having to give a reason for withdrawing. To begin the experiment, participants (on an individual basis) were asked whether or not they knew what the term *'phishing attack'* meant. Those who gave a positive response were asked to give a short verbal description to confirm their understanding, whilst negative responders were read a brief definition of what a phishing attack was and given a short verbal description. Then participants were asked to follow think-aloud user study instructions given in the experimental protocol shown in Fig. 3. They were also informed that they could ask any questions to clarify anything related to the experiment that they were unsure about. The pre- and post-tests were based on an Apple MacBook Pro computer where the participants received their score at the end of each test.

Table 3
Participants demographics in the main study.

Characteristics	Total
Sample Size	20
Gender	
Male	13
Female	7
Age (18–25)	20
Experience using mobile device	
Mobile phone	0
Smart phone	20
Average hours per week on the internet	
0–5	0
6–10	0
11–15	0
16–20	0
20+	20

In the pre-test, participants were presented with ten websites and asked to differentiate phishing websites from legitimate ones. After evaluating 10 websites, participants were given 15 min to complete the training activity using our mobile game installed on an HTC One X smartphone with a touch screen. After engaging for 15 min with the mobile game prototype, the participants were asked to complete a survey. The SUS questionnaire items of the survey used to measure the users' subjective satisfaction of the mobile game prototype interface shown in Table 3 (Brooke, 1996). The SUS scoring approach will be discussed in more detail in section 5.4. Then, the participants were shown ten more websites in the post-test. The score was recorded during the pre- and post-tests, to observe participants' understanding and awareness of phishing threat through the given mobile game prototype. More than half of the websites were phishing, whilst the rest were legitimate ones from popular brands. For the purpose of this experiment, recently being attacked phishing websites were taken from PhishTank.com (PhishTank, 2013) from November 1 to November 28, 2013. All phishing website URLs were captured within seven hours of being reported. The participants talked about their opinions and experience of phishing threat awareness through the mobile game prototype during the study. Moreover, they talked about their opinions in terms of avoidance behaviour, motivation, threat perception, threat severity and susceptibility, cost, knowledge and the effectiveness of mobile game prototype to protect themselves from phishing threats.

5. Results

5.1. SUS study results

The purpose of SUS study was to evaluate the general usability of the mobile game prototype. Therefore, it employed the SUS scoring approach introduced by Brooke (1996). The SUS produces a single number representing a composite measure of the general usability of a software application (in our case mobile game prototype application). To obtain the SUS score of the mobile game prototype, initially the sum of score contributions from each item was calculated. Each item's score contribution ranges from 0 to 4. For items 1, 3, 5, 7 and 9 the score contribution is the scale position minus 1. For items 2, 4, 6, 8 and 10, the score contribution is 5 minus the scale position. Finally, multiply the sum of the scores by 2.5 to obtain the overall value of mobile game prototype usability. The SUS scores range from 0 to 100. Therefore, to accomplish this study, the user satisfaction with the mobile game prototype deployed on a HTC One X touch screen smart phone was measured using the SUS. The scores are summarized in Table 4.

In general, the participants' subjective satisfaction of the mobile game prototype application was significantly high with 84 percent (83.62 out of 100) (Brooke, 1996). Participants also noted that they

Table 4
The user satisfaction of the mobile game prototype application.

No	Statement	Average score	Standard deviation
1	I think that I would like to use this mobile game frequently	3.95	0.759
2	I found the mobile game unnecessarily complex	1.50	0.607
3	I thought the mobile game was easy to use	4.55	0.510
4	I think that I would need the support of a technical person to be able to use this mobile game	1.70	0.865
5	I found the various functions in this mobile game were well integrated	4.20	0.696
6	I thought there was too much inconsistency in this mobile game	1.65	0.671
7	I would imagine that most people would learn to use the mobile game very quickly	4.45	0.686
8	I found the mobile game very awkward to use	1.60	0.503
9	I felt very confident using the mobile game	4.35	0.587
10	I needed to learn a lot of things before I could get going with this mobile game	1.60	0.754
	Average Overall Satisfaction Score (Ranges from 0–100)	**83.62**	

Total Score = 33.45.
SUS Score = 33.45 × 2.5 = 83.62.

found the mobile game prototype to be very usable and felt that they could learn it very quickly. This is mainly because the game player had to follow three functionalities, which are easy to remember when interacting with the mobile game. First, tap on the worm icon to eat if the worm was associated with a legitimate website address. Second, tap on the "AVOID" button if the worm was associated with a fake website address. Third, tap on the "big fish" image icon (the small fish's teacher) to request help if the worm associated with the website address is suspicious and difficult to identity. Therefore, a minimum number of functionalities can help completing the game easily. This might have enhanced the participants' subjective satisfaction of mobile game interface usability. Moreover, participants demonstrated they had a higher confidence after their engagement with the mobile game prototype. Participants were also able to learn the game quickly (within 5 min) and they stated they are quite interested in using the mobile game frequently.

In summary, the survey results suggest that the participants' subjective satisfaction of the mobile game prototype was significantly high. Therefore, the study continued with the analysis of think-aloud data. The results of think-aloud study revealed that how the participants' phishing threat avoidance behaviour impact on the game design framework after their engagement with the mobile game prototype. Furthermore, pre- and post-tests revealed whether or not the anti-phishing education took place through the mobile game prototype.

5.2. Results of the think-aloud study

The data analysis of the think-aloud study was conducted in two phases, which were based on Norgaard and Hornbaek's (2006) study. First, the study segmented the recordings through the application of keywords to each segment. The keywords were taken from the elements of the game design framework introduced by Arachchilage and Love (2013). The audio recordings were mainly segmented into eight keywords: avoidance behaviour, avoidance motivation, perceived threat, safeguard effectiveness, safeguard cost, perceived severity, perceived susceptibility and self-efficacy. Second, the study attempted to analyse and form a coherent interpretation of segments that shared keywords. Therefore, the study findings were organized into eight areas. Table 5 summarises these key areas and main findings within each of them.

5.3. Summary of results

The current study empirically evaluated the game design framework introduced by Arachchilage and Love (2013) through a prototype of an educational mobile game. A think-aloud study was conducted, along with a pre- and post-test, to assess the game design framework. The study used 20 participants with each one participating for approximately one-hour.

Initially, we evaluated the participants' subjective satisfaction of the mobile game prototype using SUS scoring approach introduced by Brooke (1996). The score was significantly high, 83.62 out of 100 (Brooke, 1996). The research study employed ***Paired-samples t-test*** to compare the means scores for the participants' pre- and post-tests (Pallant, 2007). Participants, who played the mobile game, scored 56% in the pre-test and 84% in the post-test. There was a statistically significant increase in the post-test ((Pre-test: M = 56.00, SD = 17.911 and Post-test: M = 84.00, SD = 13.139), $t(19) = -7.97$, $p < 0.005$ (two-tailed)).

There is a significant improvement of 28% of the participants' phishing avoidance behaviour in the post-test ($p < 0.005$ (two-tailed)). Eighteen participants scored above 80%, whilst five of them scored full marks (100%) in the post-test. All participants scored above 50 percent in their post-test. The individual participant's score during their engagement with the mobile game prototype is shown in Fig. 4. It has been seen that a considerable improvement of overall participants' phishing avoidance behaviour through the mobile game prototype. Therefore, we conclude that the mobile game prototype was somewhat effective in teaching participants to look at URLs in their browser's address bar when assessing the website legitimacy.

In addition, during think-aloud study, all participants shared their opinions about phishing threat awareness after using the mobile game. All of them indicated that the mobile game was somewhat effective in enhancing their avoidance behaviour through motivation to protect themselves against phishing attacks. Furthermore, we captured their reflection on the elements of the game design framework introduced by Arachchilage and Love (2013) after their engagement with the mobile game prototype. The study revealed that perceived threat, safeguard effectiveness, perceived susceptibility, perceived severity and self-efficacy positively impact while safeguard cost negatively impact avoidance behaviour through motivation to protect themselves against phishing threats.

6. Discussion

This study empirically investigated the game design framework introduced by Arachchilage and Love (2013) through a mobile game prototype for computer users to thwart phishing attacks. It is useful to stress the participants' impact on the framework after their engagement with the game play activity. It has been seen that participants' avoidance behaviour has increased by 28 percent in the post-test, after playing the game. One participant stated: "*You*

Table 5
Overview of results — N refers to the number of sessions in which a finding was made (out of 20 sessions in total).

Area of attention	Main findings	N	Example of quotes
Avoidance behaviour	I play the mobile game to avoid phishing attacks OR Updating knowledge through the mobile game is very useful to avoid phishing attacks	20	"The game was useful and I liked to play the game to avoid phishing" "I like to play the game to learn about phishing rather than reading books, articles or papers" "You can see my avoidance behaviour has increased by looking at the score of pre and post-test"
Avoidance motivation	I'm interested in playing the mobile game to avoid phishing attacks OR I feel that gaining mobile game based education to avoid phishing attacks is somewhat useful	20	"Wow! This game is useful and a fantastic idea" "This game is really interesting, I think I love to play it again and again" "Wow This game is great! Can I download it from the Internet?" "Yes, this game is important, because at the end of the day it's our money, we do not want to lose it" "I like to play the game a little longer" "I would recommend this game to my family, peers and friends" "Yes, this is a simple game anybody can play" "I will be the first one who will buy this game, tell me when everything is done"
Perceived threat	Phishing attacks pose a threat to my computer OR A phishing attack is a danger to my computer	20	"Yes, I feel phishing is a huge threat, because at the end of the day attackers steal our money" "I feel phishing threat is harmful to my computer" "Yes, I feel phishing threat is dangerous to my computer"
Perceived severity	A phishing attack would steal my personal information from my computer without my knowledge OR Phishing attack would invade my privacy	20	"Phishing attacks would steal my banking details" "Phishing attacks would steal my username, passwords, credit or debit card details" "Phishing attackers can use my personal details for crimes"
Perceived susceptibility	It is extremely likely that my computer will be infected by a phishing attack in the future OR My chances of getting phishing attacks are great.	20	"Yes, I now feel that my computer also may be infected by a phishing attack in the future" "It is very easily that I can fall for phishing" "Hmm, there is a high probability that my computer also will be infected by a phishing attack"
Safeguard effectiveness	The mobile game based education would be useful for detecting phishing attack OR The mobile game based education increased my knowledge of phishing attacks	20	"Yes, the game really helps me to identify good websites from bad ones" "This mobile game is useful and fantastic for learning" "This mobile game teaches how to avoid phishing threat" "Actually, I liked the way how the game teaches" "Yes, I learnt a lot about detecting phishing attacks through the game" "I don't think that I would not be able to get this much of knowledge by reading a book or article about phishing"
Safeguard cost	It will take less time to gain phishing education through the mobile game OR It will cost less money to gain anti-phishing education through the mobile game, if downloaded for free.	18	"The game is simple" "The game does not take long time to play" "I like to download the game for free" "I don't mind to pay for this game"
Self-efficacy	I gained knowledge about phishing attacks through the mobile game OR I feel gaining anti-phishing knowledge through the mobile game does really helped me for detecting phishing attacks	20	"Yes, this game improved my knowledge about phishing" "In the past, I really didn't check the URLs, now I know it is very important" "Yes, this game taught me how to identify phishing URLs" "I didn't know the meaning of 'https://' is secure version of http before playing the game." "Yes, I think that the game was really good in teaching different patterns of URLs" "I did not know by looking at the URL I can decide the legitimacy of the website before playing the game" "Now I know how to identify the difference between the good and bad website"

can see my phishing knowledge has increased by looking at the score of pre- and post-tests". These results support the findings of Arachchilage and Love's (2013). The proposed game design framework was evaluated through an empirical investigation, which showed that users' avoidance behaviour is important in combatting phishing. The framework explained a considerable amount of variance in participants' avoidance behaviour, which is 15% (Arachchilage & Love, 2013). In addition, the results of our study support the findings of Liang and Xue's (2010). Their model explained a considerable amount of variance in users' avoidance behaviour (21%) (Liang & Xue, 2010). Their findings showed actual avoidance behaviour is significant to avoid spyware attacks using given anti-spyware software as a safeguarding measure. Therefore, results of our study described that participants had a great impact on the avoidance behaviour element of the game design framework after their engagement with the mobile game prototype.

All participants were convinced that the mobile game is somewhat effective in enhancing their avoidance behaviour through motivation to protect themselves from phishing threats. Their common argument was that books, papers, articles and lecture notes are boring. Those materials cannot provide fun with immediate feedback, whereas this type of mobile game based education can actually provide both. This would have motivated them to play the game to learn about phishing threats. One participant responded that: "*I will now go and read more about phishing threats*". This statement describes how much the participant was motivated to

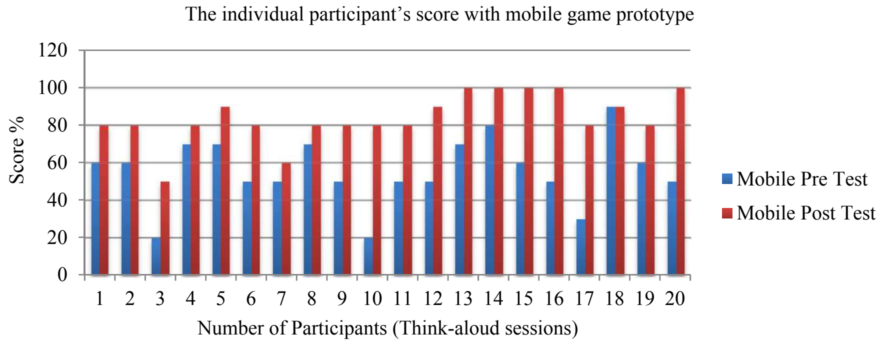


Fig. 4. The individual participant's score during their engagement with the mobile game prototype.

learn about phishing threats after playing the game. All participants said that this mobile game is really interesting and that they would love to play it again and again. Therefore, the current study conveys a simple, yet powerful message that the mobile game prototype enhances personal computer users' motivation to avoid phishing attacks. The game design framework introduced by Arachchilage and Love (2013) revealed that users' avoidance motivation is important for combatting phishing threat and also avoidance behaviour is determined by avoidance motivation. In addition, the current study also backs up the findings of Liang and Xue's (2010) theoretical model. The research model explained a considerable amount of variance in users' avoidance motivation (56%). Their findings showed that users' IT threat avoidance behaviour is determined by avoidance motivation. Fundamentally, avoidance motivation can be represented by the behavioural intention to use the safeguard measure. As stressed by cognitive theorists (Ajzen, 1991; Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975; Venkatesh, Morris, Davis, & Davis, 2003), behavioural intention is a strong predictor of actual behaviour. Therefore, the current study results showed that the participants' engagement with the mobile game prototype has a significant impact on the avoidance motivation element of the game design framework.

All twenty participants said that they felt that such phishing threats exist in the cyberspace after playing the game and they believed that an attack might occur at any time to their personal computer system. The threat perception enhanced their motivation to avoid phishing threat. One participant stated: “*I feel phishing is a huge threat after playing the game, because at the end of the day attackers may steal our sensitive information such as username, password and credit/debit card information if we are unaware of phishing threats*”. Furthermore, the same participant mentioned that the risk of being phished is relatively high due to the pervasiveness of Internet technology. Participants rated the danger to be very high, in case that a real phishing attack occurs. A few participants discussed the fact that attackers could not only disclose their sensitive information but also use that information for crimes which is even more dangerous. One participant stated: “*I think phishing attacks not only steal my money, but attackers can also use my personal information for crimes*”. Therefore, it seemed like severity and susceptibility of phishing attacks have developed through the mobile game prototype where participants perceived phishing as a dangerous threat. This findings support the findings of Liang and Xue's (2010) theoretical model. They argued that computer users have to be convinced and feel that such malicious IT threats exist in the cyberspace and are avoidable. Users' failure to feel the threat perception causes them to not act to avoid it. Their data analysis results found that the model is able to explain a respectable amount of variance in threat perception (33 percent). However, this figure is slightly lower than the finding of the game design framework introduced by Arachchilage and Love (2013), which is 36 percent. The current study findings therefore demonstrated the threat perception that users need to be aware of the likelihood and severity of being attacked by phishing threats. One participant stated: “*Now I must be really careful of when I do online transactions*”. The study revealed that users perceived that such a threat is existent in the cyberspace: they also sensed that there is likelihood and that it could be severe if the threat actually occurred. Workman et al. (2008) reveal that perceived susceptibility and severity both have an effect on user IT security behaviour. Therefore, the current study findings demonstrate that participants' engagement with the mobile game prototype has a significant impact on the perceived threat, perceived severity and susceptibility elements of the game design framework.

All twenty participants believed that the mobile game prototype is an effective safeguarding measure to thwart phishing threat. One participant stated: “*Now only I realised the worth of looking at the URL to identify good website from bad ones. I never knew that the attacker can mimic URLs to launch a phishing attack before playing the game.*” All participants mentioned that the mobile game prototype is an effective approach that motivated them to learn about phishing threats. Therefore, they believed the mobile game is an effective way of educating people to combat phishing. Moreover, participants stressed that the mobile game was somewhat effective in gaining knowledge with fun. It can be argued that if the mobile game prototype is effective, then it influences participants to enhance their avoidance motivation to thwart phishing attacks. Our findings support the findings of Liang and Xue's (2010). They empirically demonstrated that safeguard effectiveness can motivate users to avoid malicious IT threats. Previous studies on information security have consistently emphasized that safeguard effectiveness motivates users to perform computer security practices (Anderson & Agarwal, 2006; Ng, Kankanhalli, & Xu, 2009; Woon et al., 2005). In addition, the game design framework introduced by Arachchilage and Love (2013), empirically proved that the safeguard effectiveness element should be addressed in the game design framework for personal computer users to thwart phishing threat. Therefore, results of our study suggest that the participants had great impact on the safeguard effectiveness element of the game design framework, after their engagement with the mobile game prototype.

All participants in the think-aloud study stated that the game is simple and it does not take too long to play. They mentioned that they would only like to download the game online if it were freely available. One participant stated: “*If the game is too expensive and takes too long to play, I don't buy it then.*” However, a couple of participants showed their interest of purchasing the mobile game online. One participant stated: “*I like to buy the game online. I'm a bit more suspicious if a useful game is online for free download. Because it can be a virus attack sometimes.*” The other participant said: “*I do not hesitate to pay for useful things. I really liked the game. Therefore, I would pay for it*”. Participants' motivation to play the game is determined by the cost that they have to pay to download the game and the time it takes to play the game (Liang & Xue, 2010). When the game is freely available online and does not take too long to play, participants showed their motivation to play the game to avoid phishing threat. It explained that avoidance motivation is determined by safeguard cost that describes time and money efforts to play the mobile game. The current study findings backed up the findings of Liang and Xue's (2010) theoretical model. It empirically investigated that safeguard cost had a negative impact on users' avoidance behaviour through motivation to protect themselves from phishing attacks. Previous IT security research also revealed that costs associated with network security significantly reduce the likelihood that individuals enable their home wireless network security (Woon et al., 2005). In addition, the current study results support the findings of the game design framework introduced by Arachchilage and Love (2013). It empirically investigated that safeguard cost had a negative impact on users' avoidance behaviour through motivation to protect themselves from phishing attacks. Therefore, the current study indicated that the participants had a great impact on the safeguard cost element of the game design framework after their engagement with the mobile game prototype.

All participants believed that the mobile game prototype was somewhat effective in teaching how to identify good URLs from bad ones. The evidence was obvious from the score of pre- and post-tests. In the pre-test, participants scored 56% while after playing the game in the post-test they scored 84%. The score has increased by 28 percent in the post-test. The overall score of post-tests supported the opinions and statements observed in the think-aloud study. Therefore, the findings demonstrated that learning has taken place through the mobile game prototype, which reflected on the score of participants' post-test. All participants agreed saying things like, “*I learnt a lot of new things about phishing through the mobile game which I had not known*”. They also believed that the mobile game prototype was somewhat effective in teaching participants to identify good URLs from bad ones. The study argued that effective learning about phishing threats through the mobile game prototype, motivated participants to avoid phishing attacks. The current study findings supported the findings of the game design framework introduced by Arachchilage and Love (2014). Their findings indicate that participants' self-efficacy had positively impacted their motivation to thwart phishing attacks. Findings from our study also confirm the findings of Liang and Xue's (2010). They empirically investigated participants' self-efficacy and showed that it had positively impacted their motivation to thwart spyware attacks. Previous research has also showed that users are more motivated to perform IT security related performance as the level of their self-efficacy increases (Ng et al., 2009; Woon et al., 2005; Workman et al., 2008). Therefore, results of our study provide evidence to incorporate participants' self-efficacy into the game design framework for computer users to thwart phishing threats.

In summary, this study found that the mobile game prototype enhanced the user avoidance behaviour through increasing their motivation to protect themselves from phishing attacks after the game play activity. Furthermore, the results provide support to assess the game design framework introduced by Arachchilage and Love (2013) through the mobile game prototype. Findings from out study suggest that perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, perceived threat, and perceived susceptibility elements have a significant impact on avoidance behaviour through motivation to thwart phishing attacks, as addressed in the game design framework.

7. Conclusion and future work

This research evaluated a game design framework introduced by Arachchilage and Love (2013). The game was designed and developed as an educational tool to teach computer users how to protect themselves against phishing attacks. It addressed two questions: The first question is how can one identify which issues the game needs to address? What principals should guide to structure this information? We used a game design framework in order to address those issues and present information in the game design context. The objective of our anti-phishing mobile game design was to teach users how to distinguish legitimate URLs from phishing ones. The mobile game prototype was designed and developed for Android platform using MIT App Inventor Emulator. The research reported in this paper discussed the participants' impact on the game after their engagement with the game play activity. We employed SUS, as the first step to assess the subjective satisfaction of mobile game prototype interface. Then, a think-aloud study was conducted along with a pre- and post-test in order to evaluate the game design framework (Arachchilage & Love, 2013).

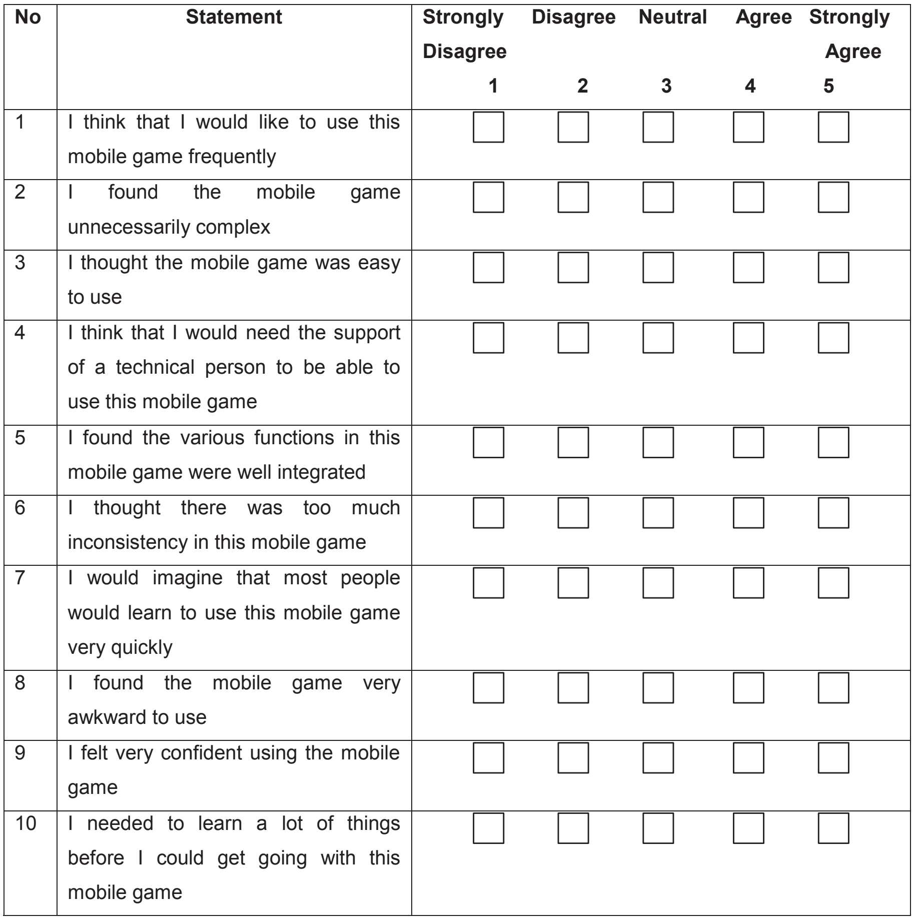
Our results are encouraging. In the pre-test, participants' success rate was 56%, whilst scoring 84% in their post-test. The study findings showed that learning has taken place through the mobile game prototype. Participants' avoidance behaviour has also increased by 28 percent, which is reasonably high. Therefore, the mobile game prototype was able to teach participants to protect themselves from phishing attacks. Furthermore, we found that the mobile game prototype enhanced user avoidance behaviour by motivating them to protect themselves from phishing attacks. Finally, the study results suggest that perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, perceived severity and perceived susceptibility elements have a significant impact on avoidance behaviour through motivation to thwart phishing attacks as addressed in the game design framework (Arachchilage & Love, 2013).

However, only five participants were able to achieve 100% score in differentiating legitimate websites from phishing websites, by looking at URLs in the post-study. There are several explanations for these results. The mobile game functioned properly, however, was still a prototype. It is useful to develop a proper mobile game, rather than a prototype with some attractive graphics with visual objects, including more complex URLs and then test on a different sample to confirm our findings. In addition, limited display size of the mobile phone might have caused a problem for participants especially those with visual impairment.

In this research, we selected phishing attacks as the IT threat, and designed a mobile game prototype to protect computer users from phishing. Future research can be conducted with different threat sources such as viruses, malware, botnets and spyware to examine whether the findings of this study will change or the framework will need to be adapted.

The main objective of our anti-phishing mobile game prototype was to teach users how to identify phishing URLs, which is one of many ways of identifying a phishing attack. Future research can be conducted on designing a game to teach the other areas, such as signs and content of the web page, the lock icons and jargons of the webpage, the context of the email message and the general warning messages displayed on the website.

Appendix A. SUS questionnaire items used in this study.



No	Statement	Strongly Disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
1	I think that I would like to use this mobile game frequently	□	□	□	□	□
2	I found the mobile game unnecessarily complex	□	□	□	□	□
3	I thought the mobile game was easy to use	□	□	□	□	□
4	I think that I would need the support of a technical person to be able to use this mobile game	□	□	□	□	□
5	I found the various functions in this mobile game were well integrated	□	□	□	□	□
6	I thought there was too much inconsistency in this mobile game	□	□	□	□	□
7	I would imagine that most people would learn to use this mobile game very quickly	□	□	□	□	□
8	I found the mobile game very awkward to use	□	□	□	□	□
9	I felt very confident using the mobile game	□	□	□	□	□
10	I needed to learn a lot of things before I could get going with this mobile game	□	□	□	□	□

References

Aaron, G., & Rasmussen, R. (2015). *Global phishing survey 2H2014: Trends and domain name use*. Retrieved from: http://internetidentity.com/wp-content/uploads/2015/05/APWG_Global_Phishing_Report_2H_2014.pdf Accessed 05.02.16.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior & Decision Processes, 50*, 179–211.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting behavior*. Englewood Cliffs, NJ: Prentice Hall.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: user strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82*, 69–82.

Amory, A., & Seagram, R. (2003). Educational game models: conceptualization and evaluation. *South African Journal of Higher Education, 17*(2), 206–217.

Anderson, C. L., & Agarwal, R. (2006). Practicing safe computing: message framing, self-view, and home computer user security behaviour intentions. In *International conference on information systems, Milwaukee, WI* (pp. 1543–1561).

Anti Phishing Working Group (APWG). (2014). *Phishing activity trends report, 2nd quarter 2014*. Retrieved from: http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf Accessed 05.02.16.

APWG. (2016). *Anti-phishing working group*. Available at: http://www.antiphishing.org/ Accessed 05.02.16.

Arachchilage, N. A. G. (2015). User-centred security: a game design to thwart phishing attacks. In *International conference: Redefining the R&D needs for Australian cyber security on November 16, 2015*. Canberra, Australia: University of New South Wales at the Australian Defence Force Academy. arXiv preprint arXiv:1511.03459.

Arachchilage, N. A. G., & Cole, M. (2011). *Design a mobile game for home computer users to prevent from "phishing attacks", Information Society (i-Society), 27-29 June 2011* (pp. 485–489). Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5978543&isnumber=59784 Accessed 22.12.11.

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior, 29*(3), 706–714.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: a phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304–312.

Arachchilage, N. A. G., Namiluko, C., & Martin, A. (2013, December). A taxonomy for securely sharing information among others in a trust domain. In *Internet technology and secured transactions (ICITST), 2013 8th international conference for (pp. 296–304)*. IEEE.

Arachchilage, N. A. G., Tarhini, A., & Love, S. (2015). Designing a mobile game to thwarts malicious IT threats: a phishing threat avoidance perspective. *International Journal for Infonomics (IJI), 8*(3/4). Infonomics. arXiv preprint arXiv:1511.07093.

Aytes, K., & Terry, C. (2004). Computer security and risky computing practices: a rational choice perspective. *Journal of Organizational and End User Computing, 16*(2), 22–40.

Boyinbode, O., & Ng'ambi, D. (2015). MOBILect: an interactive mobile lecturing tool for fostering deep learning. *International Journal of Mobile Learning and Organisation, 9*(2), 182–200.

Brooke, J. (1996). SUS-A quick and dirty usability scale. *Usability Evaluation in Industry, 189*, 194.

CNN. com. (2005). *A convicted hacker debunks some myths*. Available at: http://www.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/index.html Accessed 04.04.11.

Denk, M., Weber, M., & Belfin, R. (2007). Mobile learning challenges and potentials. *International Journal of Mobile Learning and Organisation, 1*, 122–139.

Dhamija, R., & Tygar, J. D. (2005). The battle against phishing: dynamic security skins. In *Proceedings of the 2005 symposium on usable privacy and security, Pittsburgh, Pennsylvania, July 06-08, 2005, SOUPS '05, 93* pp. 77–88). New York, NY: ACM Press. Availbale at: http://doi.acm.org/10.1145/1073001.1073009 Accessed 20.3.11.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In CHI '06 (Ed.), *Proceedings of the SIGCHI conference on human factors in computing systems, Montréal, Québec, Canada, April 22-27, 2006* (pp. 581–590). New York, NY: ACM Press. Available at: http://doi.acm.org/10.1145/1124772.1124861 Accessed 15.05.11.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioural response to phishing risk. In *Proceedings of the anti-phishing working groups - 2nd annual eCrime researchers summit, 37–44, October 2007, Pittsburgh, Pennsylvania*. Available at: http://dx.doi.org/10.1145/1299015.1299019 Accessed 25.03.11.

Finstad, K. (2006). The system usability scale and non-native English speakers. *Usability Studies, 4*(1), 185–188.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007). A framework for detection and measurement of phishing attacks. In *Proceedings of the 2007 ACM workshop on Recurring malcode, Alexandria, Virginia, USA, November 2007*.

Gorling, S. (2006). The myth of user education. In *Proceedings of the 16th virus bulletin international conference*. Royal Institute of Technology, Department of Industrial Economics and Management (INDEK).

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74–81. Available at: http://cacm.acm.org/magazines/2012/1/144811-the-state-of-phishing-attacks/fulltext Accessed 30.07.15.

Ion, I., Reeder, R., & Consolvo, S. (2015, July). "... no one can hack my mind": comparing expert and non-expert security practices. In *Symposium on usable privacy and security (SOUPS)*.

Kirlappos, I., & Sasse, M. A. (2012). Security education against phishing: a modest proposal for a major rethink. *Security & Privacy, IEEE, 10*, 24–32. March-April 2012, Available at: http://dx.doi.org/10.1109/MSP.2011.179 Accessed 25.09.12.

Klopfer, E. (2008). *Augmented learning: Research and design of mobile educational games*. The MIT Press.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007c). Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI conference on human factors in computing systems, San Jose, California, USA, April - May 2007*.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., et al. (2007a). Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. In *APWG eCrime Researchers Summit, 4–5October 2007, Pittsburgh, PA, USA*.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007b). *Teaching Johnny not to fall for phish*. Tech. rep. Cranegie Mellon University. Available at: http://www.cylab.cmu.edu/files/cmucylab07003.pdf Accessed 12.06.11.

Le Compte, A., Elizondo, D., & Watson, T. (2015, May). A renewed approach to serious games for cyber security. In *Cyber conflict: Architectures in cyberspace (CyCon), 2015 7th international conference on (pp. 203–216)*. IEEE.

Lewis, J. R., & Sauro, J. (2009). The factor structure of the system usability scale. In *Proceedings of the 1st international conference on human centered design: Held as part of HCI international 2009, San Diego, CA, 19–24 July 2009*. Available at: http://dx.doi.org/10.1007/978-3-642-02806-9_12 Accessed 08.07.12.

Li, L., Berki, E., Helenius, M., & Ovaska, S. (2014). Towards a contingency approach with whitelist-and blacklist-based anti-phishing applications: what do usability tests indicate? *Behaviour & Information Technology, 33*(11), 1136–1147.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly, 33*(1), 71–90.

Liang, H., & Xue, Y. (2010). Understanding security behaviours in personal computer usage: a threat avoidance perspective. *Association for Information Systems, 11*(7), 394–413.

MIT App Inventor. (2012). *Learn about app inventor*. Available at: http://beta.appinventor.mit.edu/learn/ Accessed 12.03.12.

Mitnick, K., & Simon, W. L. (2002). *The art of deception – Controlling the human elements of security*.

Moghimi, M., & Varjani, A. Y. (2016). *New rule-based phishing detection method. Expert systems with applications*.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: a health belief perspective. *Decision Support System, 46*(4), 815–825.

Ng, B. Y., & Rahim, M. A. (2005). A socio-behavioral study of home computer users intention to practice security. In *The ninth Pacific Asia conference on information systems, Bangkok, Thailand, 2005*.

Nørgaard, M., & Hornbæk, K. (2006). What do usability evaluators do in practice?: an explorative study of think-aloud testing. In *Proceedings of the 6th conference on designing interactive systems, University Park, PA, USA, 26–28 June 2006*. Available at: http://dx.doi.org/10.1145/1142405.1142439 Accessed 18.08.12.

Pallant, J. (2007). *A step by step guide to data analysis using SPSS for windows (Version15), SPSS survival manual*. Buckingham: Open University Press.

Parsons, D., Ryu, H., & Cranshaw, M. (2006). A study of design requirements for mobile learning environments. In *Proceedings of the sixth IEEE international conference on advanced learning technologies* (pp. 96–100).

PhishTank, 2013. Avalable at: http://www.phishtank.com/, Accessed 28.11.13.

Prensky, M. (2001). *Digital game-based learning revolution*. New York: Digital Game-Based Learning.

Purkait, S. (2012). Phishing counter measures and their effectiveness–literature review. *Information Management & Computer Security, 20*, 382–420.

Raybourn, E. M., & Waern, A. (2004). Social learning through gaming. In *Proceedings of CHI 2004, Vienna, Austria* (pp. 1733–1734).

Richmond, R. (2006). *Hackers set up attacks on home PCs, financial firms: Study, September 2006*. Available at: http://www.marketwatch.com/News/Story/Story.aspx?dist=newsfinder&siteid=google&guid=%7B92615073-95B6-452EA3B9569BEACF91E8%7D&keyword= Accessed 27.03.11.

Robila, S. A., & Ragucci, J. W. (2006). Don't be a phish: steps in user education. In *Proceedings of the 11th annual SIGCSE conference on innovation and technology in computer science education, 26 – 28 June 2006, Bologna, Italy*. Available at: http://dx.doi.org/10.1145/1140124.1140187 Accessed 29.03.11.

Sanchez, F., & Duan, Z. (2012). A sender-centric approach to detecting phishing emails. In *Presented at the ASE/IEEE international conference on cyber security*. Available at: http://www.cs.fsu.edu/research/reports/TR-121106.pdf Accessed 03.12.12.

Schneier, B. (2000). *Semantic attacks; the third wave of network attacks, crypto-gram newsletter, October 2000*. Available at: http://www.schneier.com/crypto-gram-0010.html Accessed 02.04.11.

Shekokar, N. M., Shah, C., Mahajan, M., & Rachh, S. (2015). An ideal approach for detection and prevention of phishing attacks. *Procedia Computer Science, 49*, 82–91.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In *28th international conference on Human factors in computing systems, 10-15 April, 2010, Atlanta, Georgia, USA*.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., et al. (2007). Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security, Pittsburgh, Pennsylvania, July 2007*.

Shneiderman, B. (1987). *Designing the user interface: Supplemental materials*. College Park, MD: University of Maryland at College Park.

Susan, H., Catherine, A., & Ritu, A. (2006). Practicing safe computing. In *Proceedings message freaming, self-view and home computer user security behaviour intentions, ICIS 2006, 93*. Available at: http://aisel.aisnet.org/icis2006/93 Accessed 15.03.11.

Tullis, T. S., & Stetson, J. N. (2004). A comparison of questionnaires for assessing website usability. In *Usability professionals association (UPA) 2004 conference, Minneapolis, USA, 7–11 June 2004*.

US-CERT. (2016). *The US computer emergency readiness team*. Available at: https://www.us-cert.gov/ Accessed 05.06.16.

Venkatesh, V., Morris, V. M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly, 27*(3), 425–478.

Walls, R. (2012). *Using computer games to teach social studies*. Uppsala University. Doctoral dissertation.

Wang, A. I., Øfsdahl, T., & Mørch-Storstein, O. K. (2009). *Collaborative learning through games–characteristics, model, and taxonomy*.

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. In *International conference on information systems, Las Vegas, NV* (pp. 367–380).

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799–2816.

Wu, M., Miller, R., & Garfinkel, S. (2005). Do security toolbars actually prevent phishing attacks?. In *Proceedings of the SIGCHI conference on human factors in computing systems, Montreal, Quebec, Canada, 22–27April 2006*.

Ye, Z., & Sean, S. (2002). In *Trusted paths for browsers, Proceedings of the 11th USENIX security symposium* (pp. 263–279). Berkeley, CA, USA: USENIX Association.

Zhang, Y., Egelman, S., Cranor, L. F., & Hong, J. (2007). Phinding phish - Evaluating anti-phishing tools. In *Proceedings of the 14th annual network & distributed system security symposium, February 28-March 2, 2007*. Available at: http://lorrie.cranor.org/pubs/toolbars.html Accessed 04.06.11.