Computers in Human Behavior 60 (2016) 185–197

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/

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, Earth-Link 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