Computers in Human Behavior 38 (2014) 304–312

Contents lists available at ScienceDirect

Computers in Human Behavior

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

Security awareness of computer users: A phishing threat avoidance perspective

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

[a] Cyber Security Centre, Department of Computer Science, Oxford University, Wolfson Building, Parks Road, Oxford OX1 3QD, United Kingdom
[b] School of Information Systems, Computing and Mathematics, Brunel University, Uxbridge, Middlesex UB8 3PH, United Kingdom

ARTICLE INFO

Article history:
Available online 8 July 2014

Keywords:
Usable security
Phishing threats
Security awareness
Security education
Procedural knowledge
Conceptual knowledge

ABSTRACT

Phishing is an online identity theft, which aims to steal confidential information such as username, password and online banking details from its victims. To prevent this, anti-phishing education needs to be considered. Therefore, the research reported in this paper examines whether conceptual knowledge or procedural knowledge has a positive effect on computer users' self-efficacy to thwart phishing threats. In order to accomplish this, a theoretical model based on Liang and Xue's (2010) Technology Threat Avoidance Theory (TTAT) has been proposed and evaluated. Data was collected from 161 regular computer users to elicit their feedback through an online questionnaire. The study findings revealed that the interaction effect of conceptual and procedural knowledge positively impacts on computer users' self-efficacy, which enhances their phishing threat avoidance behaviour. It can therefore be argued that well-designed end-user security education contributes to thwart phishing threats.

1. Introduction

The message "security is vital" is a phrase that all computer users should know. Computer users play a most important role in helping to make cyberspace a safer place for everyone due to the Internet technology growth. Internet technology is so pervasive today that it provides the backbone for modern living enabling ordinary people to shop, socialise and be entertained all thorough their own computers. As people's reliance on the Internet grows, so the possibility of hacking and other security breaches increases regularly (Liang & Xue, 2010).

Security exploits can include cyber-threats such as a set of computer programs which can disturb the normal behaviour of computer systems (viruses), malicious software (malware), unsolicited e-mail (spam), monitoring software (spyware), attempting to make computer resources unavailable to its intended users (Distributed Denial-of-Service or DDoS attack), the art of human hacking (social engineering) and online identity theft (phishing). These cyber-attacks are prepared to target either financial or social gain (Ng, Kankanhalli, & Xu, 2009; Woon, Tan, & Low, 2005; Workman, Bommer, & Straub, 2008). For example, a DDoS attack can target a financial organisation in order to break down their email server and the attacker can exhort a lump sum of money to give the email server back to the organisation.

On the other hand, perhaps, some people are on a mission of fun and accomplishment rather than financial or social gain. For example, a teenager can hack their friend's Facebook account to have fun or show off their capabilities. The BBC has reported that one in four young Britons attempts to access the Facebook accounts of their friends just for fun (BBC News, 2010a–c).

In addition, as organisations have become increasingly 'virtual' there has been a technological shift from work to the domestic environment (Arachchilage & Love, 2013; O'Brien et al., 1999). Employees are free to work at home or bring unfinished work home due to the pervasiveness of Internet technology. This increases the opportunity for individual users to open the backdoor to hackers. Unlike employees in organisations, these computer users at home are unlikely to have a sufficient IT infrastructure to protect themselves from cyber-threats, or may not have proper standard or strict IT security policies in place. For example, most computer users are not IT professionals and lack a high degree of computer literacy to set up a secure personal computing system (Doswell, 2008). Further examples of people's lack of security awareness include; browsing unsafe websites, downloading suspicious software, sharing passwords among family and peers and using unprotected home wireless networks (Liang & Xue, 2010).

Previous research has indicated that computer users are still the weakest link in the field of information security (Arachchilage &

* Corresponding author. Tel.: +44 0 7400 421001.
E-mail addresses: Nalin.Asanka@cs.ox.ac.uk (N.A.G. Arachchilage), Steve.Love@brunel.ac.uk (S. Love).

http://dx.doi.org/10.1016/j.chb.2014.05.046
0747-5632/

Love, 2013; CNN.com, 2005; Long, 2013; Pike, 2011). This can be seen by the way people regularly disclose personal information to the general public online through social media outlets such as Facebook, Twitter, Hi5, Orkut, Skype and professional social networking sites like LinkedIn.

Therefore, the research reported in this paper focuses on a cyber-attack, which is particularly dangerous to computer users; phishing (Dhamija, Tygar, & Hearst, 2006). Phishing, however, is a social engineering crime, a so-called *semantic attack* and well known as online identity theft (Arachchilage & Love, 2013). Phishing aims to steal confidential information such as username, password and online banking details from its victims. In phishing, victims normally get invited by scam emails to visit fraudulent websites. The attacker creates a fraudulent website, which has the look-and-feel of a legitimate website. Unsuspecting users are invited by sending scam emails to access to the fraudulent website and steal their money. Google has reported that 9500 websites are blacklisted daily (Goodin, 2012). Nevertheless, phishing attacks get more sophisticated day by day as and when attackers learn new techniques and change their strategies accordingly (Iacovos & Sasse, 2012; Kumaraguru et al., 2007a,b). Therefore, phishing has become a severe cyber-security problem today.

Sheng, Holbrook, Kumaraguru, Cranor, and Downs (2010) have conducted a role-play survey with 1001 online survey respondents to investigate who fall for phishing attacks. The study revealed that women are more susceptible than men to phishing and participants between the ages of 18 and 25 are more susceptible to phishing than other age groups. Participants in the study came from a diverse group of staff and students, including people who were concerned about computer security.

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 (Iacovos & Sasse, 2012). The Anti-Phishing Work Group (APWG) is a non-profit organisation working to provide anti-phishing education to enhance the public understanding of security. The US Computer Emergency Readiness Team also offers free advice on its website about common security breaches for computer users who have a lack of computer literacy (United State Computer Emergency Readiness Team, 2013). 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 (Arachchilage & Love, 2013; Iacovos & Sasse, 2012; Long, 2013; Purkait, 2012).

Therefore, the aim of the research reported here, is to investigate whether conceptual knowledge or procedural knowledge has a positive effect on computer users' self-efficacy in relation to thwarting phishing attacks.

2. Theoretical background

Automated anti-phishing tools have been developed to alert users of potentially fraudulent emails and websites. For example, Firefox 2, Calling ID Toolbar, EarthLink Toolbar, Cloudmark Anti-Fraud Toolbar, eBay Toolbar and Netcraft Anti-Phishing Toolbar. However, these tools are not totally reliable in detecting phishing attacks (Dhamija et al., 2006; Iacovos & Sasse, 2012; Li, Berki, Helenius, & Ovaska, 2014; Purkait, 2012; Sheng et al., 2007). Even the best anti-phishing tools omitted 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" for the Mozilla web browser that is designed to help users verify that their browser has made a secure connection to a trusted website. However, none of these systems are yet sufficient to combat phishing threats (Arachchilage & Cole, 2011; Arachchilage & Love, 2013; Iacovos & 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 programmers will continue to improve phishing and spam detection tools. However, the "human in the loop" is the weakest link in computer security (Arachchilage & Love, 2013; CNN.com, 2005; Long, 2013; Purkait, 2012). Dhamija et al. (2006) conducted a laboratory-based experiment showing twenty-two participants to twenty websites, asking them to determine which ones were legitimate. They found out that participants made mistakes on the test 40% of the time. Furthermore, they noted that 23% of their participants ignored all cues in the web browser address bar and status bar as well as all security indicators. A considerable amount of literature work has been reported that this is one of major reasons why people fall for phishing attacks (Downs, Holbrook, & Cranor, 2007; Kumaraguru et al., 2007a,b; Sheng et al., 2007; Wu, Miller, & Garfinkel, 2006). Unfortunately, most computer users have a lack of security awareness due to the deficiency of education, awareness, professionalism and training (Hui, 2007). Therefore, to thwart this, anti-phishing education needs to be considered (Downs et al., 2007; Kumaraguru et al., 2007a; Richmond, 2006; Robila & Ragucci, 2006,b; Arachchilage & Love, 2013; Iacovos & Sasse, 2012; Long, 2013; Purkait, 2012; Sanchez & Duan, 2012; Sheng et al., 2007).

Previous research has indicated that technology alone is inadequate to solve critical IT security problems. So far, there has been little work on the human aspect of performing security and preventing users from cyber-attacks which are imperative to cope up with cyber-threats such as phishing attacks (Anderson & Agarwal, 2006; Aytes & Terry, 2004; Liang & Xue, 2009; Ng and Rahim, 2005; Arachchilage & Love, 2013; Iacovos & Sasse, 2012; Purkait, 2012; Susan, Catherine, & Ritu, 2006; Woon et al., 2005; Workman et al., 2008). Many security experts' discussions have finished with the conclusion of "if we could only remove the user from the system, we would be able to make it secure" (Arachchilage & Love, 2013; Gorling, 2006). Where it is impossible to entirely eliminate the end-user from the system, for example in-home use, the best possible approach for computer security is to educate the end-user in security prevention (Arachchilage & Love, 2013; Mitnick & Simon, 2002; Schneier, 2000). Previous research has revealed that well-designed user security education can be effective (Kumaraguru et al., 2007a,b; Sheng et al., 2007). This could be web-based training materials, contextual training and embedded training to improve users' ability to thwart phishing attacks. However, the possibility of innocent people being phished increases regularly and their susceptibility to phishing attacks still remains at a higher level (Arachchilage & Love, 2013; Iacovos & Sasse, 2012; Purkait, 2012). Therefore, the research work reported in this paper attempts to investigate why computer users are susceptible for phishing attacks. Furthermore, the current study examines whether conceptual knowledge or procedural knowledge influences computer users self-efficacy to thwart phishing attacks.

3. Theoretical model

As previously stated, the premise behind this study is to examine why computer users are susceptible for phishing attacks. Therefore, a theoretical model has been developed to assess whether conceptual or procedural knowledge influences on computer users' self-efficacy to thwart phishing attacks. The proposed theoretical model was based on a theoretical model derived from Technology Threat Avoidance Theory (TTAT), which describes individual IT users' behaviour of avoiding the threat of malicious information technologies such as phishing attacks (Liang & Xue,