Computers in Human Behavior 29 (2013) 706–714

Contents lists available at SciVerse ScienceDirect

Computers in Human Behavior

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

# A game design framework for avoiding phishing attacks

Nalin Asanka Gamagedara Arachchilage *, Steve Love

*School of Information Systems, Computing and Mathematics, Brunel University, Uxbridge, Middlesex UB8 3PH, United Kingdom*

ARTICLE INFO

*Article history:*

*Keywords:*
Game design
Game based learning
Phishing threat
Security awareness
Usable security
Human–computer interaction and design

ABSTRACT

Game based education is becoming more and more popular. This is because game based education provides an opportunity for learning in a natural environment. Phishing is an online identity theft, which attempts to steal sensitive information such as username, password, and online banking details from its victims. To prevent this, phishing awareness needs to be considered. This research aims to develop a game design framework, which enhances user avoidance behaviour through motivation to protect users from phishing attacks. In order to do this, a theoretical model derived from Technology Thread Avoidance Theory (TTAT) was developed and used in the game design framework (Liang & Xue, 2010). A survey study was undertaken with 150 regular computer users to elicit feedback through a questionnaire. The study findings revealed that perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, perceived severity, and perceived susceptibility elements should be addressed in the game design framework for computer users to avoid phishing attacks. Furthermore, we argue that this game design framework can be used not only for preventing phishing attacks but also for preventing other malicious IT attacks such as viruses, malware, botnets and spyware.



## 1. Introduction

Security exploits can include malicious IT threats such as 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 attacks are prepared to target either financial or social gain (Purkait, 2012; Aggarwaly, Rajadesingan, & Kumaraguru, 2012; Ng, Kankanhalli, & Xu, 2009; Workman, Bommer, & Straub, 2008 and Woon, Tan, & Low, 2005). For example, a DDoS attack could target a bank in order to break down their e-mail server and the attacker can exhort a lump sum of money to give the e-mail server back to the bank.

One such IT threat that is particularly dangerous to computer users is phishing. This is a type of semantic attack (Purkait, 2012; Aggarwaly et al., 2012; Downs, Holbrook, & Cranor, 2007 and Schneier, 2000) in which attackers try to fool and steal money from legitimate Internet users sending e-mails rather than exploiting bugs in computer software. The attacker creates a fraudulent web site which has the look-and-feel of the legitimate website. Then users are invited by sending e-mails to access to a fraudulent website and steal their money. Phishing attacks get more sophisticated regularly as and when attackers learn new techniques and change their strategies accordingly (Purkait, 2012; Aggarwaly et al., 2012 and Kumaraguru et al., 2007). The most popular approach is e-mail (James, 2005 and Richmond, 2006). Phishing e-mails employ a variety of tactics to trick people into disclosing their confidential information such as usernames, passwords, national insurance numbers and credit/debit card numbers. For example, asking people to take part in a survey or urging people to verify their bank account information in which they must provide their bank details to be compensated. The increasing sophistication of these techniques makes it a challenge to protect individual users against phishing attacks (Purkait, 2012 and Drake, Oliver, & Koontz, 2006).

Personal computer users are susceptible to phishing attacks due to the rapid growth of internet technology (Purkait, 2012; Aggarwaly et al., 2012 and Ponnurangam et al., 2007). This is because users can have lack of security awareness and sensitive trust decisions that they make during online activities such as online banking transactions or bill payments. Therefore, personal computer users make a significant contribution in helping to make cyberspace a safer place for everyone. Internet technology is so ubiquitous today that it provides the backbone for modern living enabling ordinary people to socialize, shop, and be entertained all through their personal computers. As people's reliance on Internet grows, the possibility of hacking, attacking and other security breaches increases rapidly (Liang & Xue, 2009). Therefore, the message "security is important" should be reached to all personal computer users.

* Corresponding author.
*E-mail addresses:* Nalin.Asanka@brunel.ac.uk (N.A.G. Arachchilage), Steve.Love@brunel.ac.uk (S. Love).

0747-5632/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.chb.2012.12.018

Automated computer systems can be used to identify some fraudulent e-mails and websites (Sanchez & Duan, 2012; Purkait, 2012 and Workman et al., 2008). Dhamija and Tygar (2005) and Ye and Sean (2002) have developed a prototype called "trusted paths" for the Mozilla web browser that was designed to help users verify that their browser has made a secure connection to a trusted website. Nevertheless, these systems are not totally reliable in detecting phishing attacks (Purkait, 2012; Sanchez & Duan, 2012 and Sheng et al., 2007). Previous research has revealed that available anti-phishing tools such as CallingID Toolbar, Cloudmark Anti-Fraud Toolbar, EarthLink Toolbar, Firefox 2, eBay Toolbar and Netcraft Anti-Phishing Toolbar are deficient for combating phishing threats (Purkait, 2012 and Robila & Ragucci, 2006). Even the best toolbars neglect over 20% of phishing websites (Zhang, Egelman, Cranor, & Hong, 2007). On the one hand, software application designers and developers will continue to improve phishing and spam detection. However, human is the weakest link in information security (Purkait, 2012 and CNN.com, 2005). On the other hand, human factor risks can mitigate by educating users on how to combat phishing threats (Purkait, 2012; Aggarwaly et al., 2012; Brody, Mulig, & Kimball, 2007 and Robila & Ragucci, 2006).

Phishing education needs to be considered to protect individual users against phishing threats. Previous studies have reported end-user education as a frequently recommended approach to countering phishing attacks (Allen, 2006; Hiner, 2002; Purkait, 2012; Timko, 2008 and Kumaraguru et al., 2007). So, how to educate computer users to combat phishing threat?

The design of games is a double-edged sword. When its power is properly harnessed to serve good purposes, it has tremendous potential to improve human performance. However, when it is exploited for violation purposes, it can pose huge threats to individuals and society. Therefore, the design of educational games is not an easy task and there are no all-purpose solutions (Walls, 2012 and Moreno-Ger, Burgos, Sierra, & Fernández-Manjón, 2008). The notion that game based education offers the opportunity to embed learning in a natural environment has repeatedly emerged in the research literature (Arachchilage & Cole, 2011; Walls, 2012; Moreno-Ger et al., 2008 and Sheng et al., 2007).

This research study is the first step in the development of a game design framework to enhance user avoidance behaviour through motivation to thwart phishing attacks. The aim of this study is to investigate what key elements should be addressed in the game design framework to avoid phishing attacks.

The objectives are as follows:

- Identify the key elements that should be addressed in the game design framework to avoid phishing attacks.
- Evaluate the game design framework using phishing attack (malicious IT threat) and game based anti-phishing education (safeguarding measure).
- Formulate a game design framework to thwart phishing attacks.

## 2. Theoretical Background

The premise behind this study is to develop a game design framework, which enhances user avoidance behaviour through motivation to protect them against phishing attacks. A theoretical model derived from Technology Threat Avoidance Theory (TTAT) was used to develop the game design framework, which is shown in Fig. 1 (Liang & Xue, 2010). The TTAT describes individual IT users' behaviour of avoiding the threat of malicious information technologies such as phishing attacks (Liang & Xue, 2009). The model examines how individuals avoid malicious IT threats by using a given safeguarding measure. The safeguarding measure does not necessarily have to be an IT source such as anti-phishing tools; rather it could be behaviour such as anti-phishing education (Liang & Xue, 2010).

Consistent with TTAT (Liang & Xue, 2009), users' IT 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. Perceived threat is also influenced by the interaction of perceived severity and susceptibility. User's avoidance motivation is also determined by three constructs such as safeguard effectiveness, safeguard cost, and self-efficacy.

Safeguard effectiveness is described as the individual assessment of a safeguarding measure regarding how effectively it can be applied to avoid the malicious IT threat (Liang & Xue, 2010). For example, the individual assessment regarding how effectively anti-phishing education can be applied to avoid a phishing attack. Safeguard cost is a payback for safeguard effectiveness. This refers to the physical and cognitive efforts such as time, money, inconvenience and comprehension required using the safeguard measure (Liang & Xue, 2009). Self-efficacy is defined as individuals' confidence in taking the safeguard measure. This is an important determinant of avoidance motivation. Previous research has revealed that individuals are more motivated to perform IT security related behaviours as the level of their self-efficacy increases (Kaiser, in press; Ng et al., 2009; Woon et al., 2005). In addition, the research model posits that avoidance motivation is influenced by an interaction between perceived threat and safeguard effectiveness.

The TTAT identifies the issues that the game design framework needs to address. The proposed game design framework attempts to develop threat perceptions such that individuals will be more motivated to avoid phishing attacks and use safeguarding measures. A key aspect of this is that they realise the effectiveness of safeguarding measures, lower safeguard costs, and increase self-efficacy.

Sheng et al. have conducted a role-play survey with 1001 online survey respondents to study who falls for phishing attacks (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). 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 are included from a diverse group of staff and student, including people who were concerned about computer security. The study described in this paper was targeted towards to examine participants' phishing threat avoidance behaviour by using anti-phishing education. Therefore, the survey was only administered to participants' ages ranged from 18 to 25 those who had not already completed the questionnaire before.

## 3. Pilot study

A pilot study is a rehearsal, which is conducted before the main study takes place (Compeau & Higgins, 1995; Milne, Orbell, & Sheeran, 2002; Sonderegger & Sauer, 2010). It helps the researcher to determine whether or not the study is appropriate in terms of validity. If any problems are encountered during the pilot study, adjustments are made before the main study. A quantitative analysis, based on Likert style questionnaire, approach was adopted to evaluate the game design framework described in this paper.

### 3.1. Questionnaire design

The questionnaire was constructed based on Liang and Xue's theoretical model and relevant research literature (Liang & Xue, 2009; Liang & Xue, 2010; Rosenstock, 1974; Saleeby, 2000; Smith, Milberg, & Burke, 1996; Champion & Scott, 1997; Compeau & Higgins, 1995; Davis, 1989 and Davis, Bagozzi, & Warshaw, 1983).

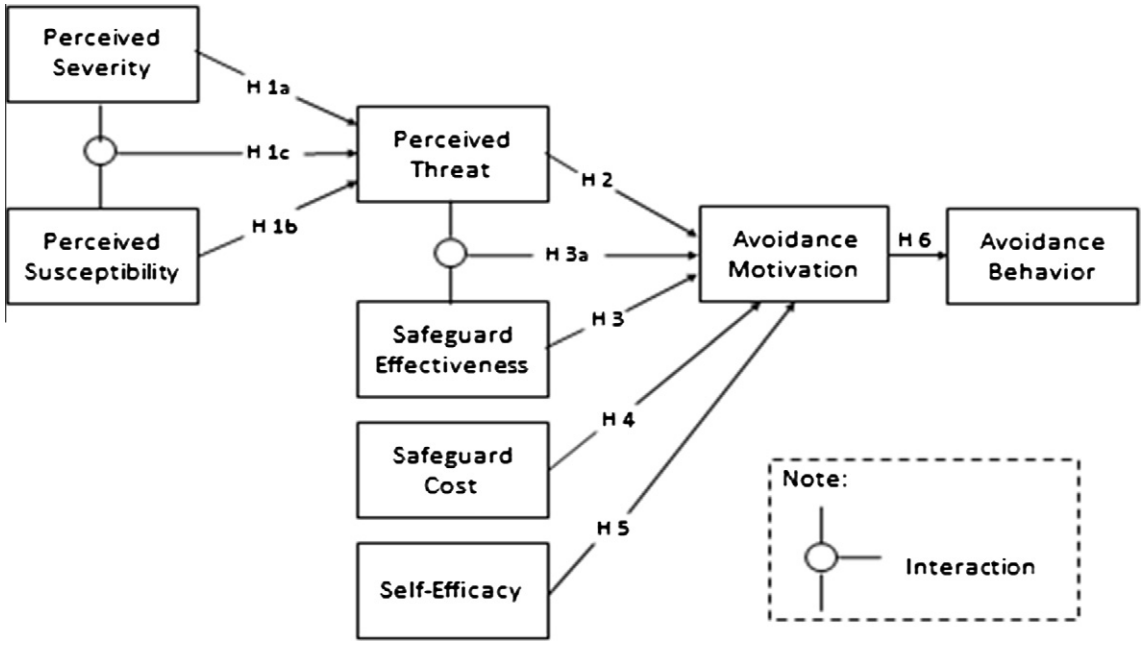


**Fig. 1.** Research model derived from TTAT (Liang & Xue, 2010).

Perceived threat was measured on the basis of substantive meaning (Rosenstock, 1974). The questionnaire items related to this aspect assessed respondents' perception of the likely harm, danger, peril or damage that phishing attack imposes. Perceived susceptibility was developed based on health behaviour research (Saleeby, 2000); and was used to evaluate the likelihood and possibility of the occurrence of a phishing attack.

TTAT speculates that computer users' well-being includes two dimensions: computer performance and information privacy. However, Liang and Xue argue that a malicious IT attack could damage both dimensions (Liang & Xue, 2009). Therefore, severity perception of computer users should relate to the two dimensions. Perceived severity was measured by the number of items based on the privacy literature in IS (Smith, Milberg, & Burke, 1996) and practitioner research that report the negative impact of phishing attacks (Brody et al., 2007; Dhamija, Tygar, & Hearst, 2006; Downs, Holbrook, & Cranor, 2006; Downs et al., 2007; Grinter et al., 2006; Jagatic, Johnson, Jakobsson, & Menczer, 2007; Miller & Garfinkel, 2005 and Schneier, 2000). The items developed in their research were based on users' concerns about both loss of personal and confidential information and degraded computer performance related to processing speed, Internet connection, and software applications.

The items of safeguard effectiveness were developed based on relevant health behaviour research (Downs et al., 2007 and Saleeby, 2000). For example, a number of items in this subscale were derived for safeguard cost based on Milne et al. and Saleeby's studies (Champion & Scott, 1997 and Saleeby, 2000). Self-efficacy was measured with items developed by Compeau and Higgins (1995), making minor amendments to adapt it to the anti-phishing education context. The number of items developed for avoidance motivation was based on the behavioural intention measures from technology adoption research (Davis, 1989 and Compeau & Higgins, 1995), with a focus on threat avoidance rather than IT adoption. Finally, threat avoidance was measured with three self-developed items.

Therefore, the pilot study questionnaire contained four items for perceived threat, four items for perceived severity, three items for perceived susceptibility, four items for safeguard effectiveness, three items for safeguard cost, 6 items for self-efficacy, three items for avoidance motivation, and three items for avoidance behaviour. In total 30 items were evaluated using a five-point scale Likert at 1 = 'Strongly disagree' and 5 = 'Strongly agree'. A sample set of questionnaire is shown in Table 1.

### 3.2. Participants

A pilot study questionnaire survey was run with sixteen first year undergraduate students from the Department of Information Systems and Computing, Brunel University, London. A summary of the demographics of the participants in the pilot study is shown in Table 2.

### 3.3. Procedure

The pilot study questionnaire survey was conducted in-person. First participants were asked to read and sign the consent form. Then the individual participants were asked whether or not they knew what the term "Phishing Attack" means. 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 phishing attack and given a short verbal description. Then participants were asked to complete the questionnaire. The individual participant was given 10 min to complete the questionnaire. They were also informed that they could provide any comments and feedback on both the content and format of the study had just been asked to take part.

### 3.4. Results

Cronbach's alpha, which is known as a coefficient alpha was used to measure the internal consistency of the questionnaire (Pallant, 2007). Previous research has indicated that an alpha score that is greater than 7.0 indicates that there is a good level of internal scale consistency (Cronbach, 1951; Pallant, 2007 and Zaharias & Poylymenakou, 2009).Therefore, Cronbach's alpha was calculated for each construct of the questionnaire and is summarised in Table 3.

**Table 1**
A sample set of questionnaire.

| **1. Perceived Susceptibility** | **Strongly agree 1** | **Agree 2** | **Neutral 3** | **Disagree 4** | **Strongly disagree 5** |
|---|---|---|---|---|---|
| It is extremely likely that my computer will be infected by a phishing attack in the future | ☐ | ☐ | ☐ | ☐ | ☐ |
| My chances of getting phishing attacks are great. | ☐ | ☐ | ☐ | ☐ | ☐ |
| I feel phishing attack will not infect my computer in the future | ☐ | ☐ | ☐ | ☐ | ☐ |
| **2. Perceived Severity** | **Strongly agree 1** | **Agree 2** | **Neutral 3** | **Disagree 4** | **Strongly disagree 5** |
| A phishing attack would steal my personal information from my computer without my knowledge | ☐ | ☐ | ☐ | ☐ | ☐ |
| Phishing attack would invade my privacy | ☐ | ☐ | ☐ | ☐ | ☐ |
| I feel phishing attack would not steal my personal information from my computer without my knowledge | ☐ | ☐ | ☐ | ☐ | ☐ |
| I feel phishing attack would not invade my privacy | ☐ | ☐ | ☐ | ☐ | ☐ |
| **3. Perceived Threat** | **Strongly agree 1** | **Agree 2** | **Neutral 3** | **Disagree 4** | **Strongly disagree 5** |
| Phishing attacks pose a threat to me | ☐ | ☐ | ☐ | ☐ | ☐ |
| A phishing attack is a danger to my computer | ☐ | ☐ | ☐ | ☐ | ☐ |
| It is risky to use my computer if it being phishing attacked | ☐ | ☐ | ☐ | ☐ | ☐ |
| I feel a phishing attack will not cause any harm to my computer. | ☐ | ☐ | ☐ | ☐ | ☐ |
| **4. Perceived Safeguard Effectiveness** | **Strongly agree 1** | **Agree 2** | **Neutral 3** | **Disagree 4** | **Strongly disagree 5** |
| Game based anti-phishing education would be useful for detecting phishing attack | ☐ | ☐ | ☐ | ☐ | ☐ |
| Game based anti-phishing education would increase my performance in protecting my computer from phishing attacks | ☐ | ☐ | ☐ | ☐ | ☐ |
| Game based anti-phishing education would enable me to detect phishing attacks on my computer faster | ☐ | ☐ | ☐ | ☐ | ☐ |
| I feel game based anti-phishing education would not be useful for protecting my computer from phishing attacks | ☐ | ☐ | ☐ | ☐ | ☐ |

**Table 2**
Participant demographics in the pilot study.

| Characteristics | Total |
|---|---|
| Sample size | 16 |
| *Gender* | |
| Male | 10 |
| Female | 6 |
| Age range (18–25) | 16 |
| *Average hours spent per week on the internet* | |
| 0–5 | 0 |
| 6–10 | 19 |
| 11–15 | 12 |
| 16–20 | 19 |
| 20+ | 50 |

**Table 3**
Cronbach's alpha scores for the questionnaire constructs in the pilot study.

| Constructs | Cronbach's alpha (>0.70) |
|---|---|
| Perceived susceptibility | 0.716 |
| Perceived severity | 0.869 |
| Perceived threat | 0.770 |
| Perceived safeguard effectiveness | 0.904 |
| Perceived safeguard cost | 0.938 |
| Self-efficacy | 0.798 |
| Avoidance motivation | 0.751 |
| Avoidance behaviour | 0.880 |

### 3.5. Summary

Based on the feedback obtained from the wording of some measurement items of each construct was slightly revised. The final questionnaire contained four items for perceived threat, four items for perceived severity, three items for perceived susceptibility, four items for safeguard effectiveness, three items for safeguard cost, 6 items for self-efficacy, three items for avoidance motivation, and three items for avoidance behaviour. Therefore, total 30 items were used in the main study to measure 8 constructs in the research model using a five-point scale Likert at 1 = 'Strongly disagree' and 5 = 'Strongly agree'.

## 4. Main study

### 4.1. Participants

The questionnaire was administrated to 151 participants, who were undergraduate students from Brunel University and Bedfordshire University. Participants' ages ranged from 18 to 25, with a gender split of 67% male and 33% female. They had average of 16–20 h per week of Internet experience (SD = 1.19). Each participant took part in the survey on a fully voluntary basis. A summary of the demographics of the participants in the main study is shown in Table 4.

### 4.2. Procedure

The questionnaire was handed out to participants' in-person by the researcher. First, the nature of the research was explained to each participant individually and they were given an informed consent form to read and sign. They were also told that they were free to withdraw from the study at any time without having to give a reason for withdrawing. Then the individual participants were asked whether or not they knew what the term "Phishing Attack" means. Those who gave a positive response were asked to give a short verbal description to confirm their understanding, whilst negative respondents were read a brief definition of a phishing attack and also given a short verbal description. Then participants were asked to complete the questionnaire, which measured the eight constructs; perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, avoidance motivation and avoidance behaviour. The individual participant was given 10 min to complete the questionnaire. After completing the questionnaire, participants were thanked for their valuable time and effort in taking part in the study.

**Table 4**
Participant demographics in the main study.

| Characteristics | Total |
|---|---|
| Sample size | 151 |
| *Gender* | |
| Male | 101 |
| Female | 50 |
| Age range (18–25) | 151 |
| *Average hours per week on the internet* | |
| 0–5 | 3 |
| 6–10 | 12 |
| 11–15 | 14 |
| 16–20 | 14 |
| 20+ | 57 |

**Table 5**
Cronbach's alpha scores for the questionnaire constructs in the main study.

| Constructs | Cronbach's alpha (>0.70) |
|---|---|
| Perceived susceptibility | 0.730 |
| Perceived severity | 0.766 |
| Perceived threat | 0.701 |
| Perceived safeguard effectiveness | 0.803 |
| Perceived safeguard cost | 0.805 |
| Self-efficacy | 0.714 |
| Avoidance motivation | 0.753 |
| Avoidance behaviour | 0.762 |

### 4.3. Results

As in the pilot study, Cronbach's alpha was calculated for each construct to measure the internal consistency of the questionnaire items. The results of this analysis are summarised in Table 5. Previous research has been shown minimum level of Cronbach's alpha is 0.7 to be internally consistent of a set of items as a group (Cronbach, 1951; Pallant, 2007 and Zaharias & Poylymenakou, 2009).

In addition, the Kaiser–Meyer–Olkin (KMO) value measure was used to assess the adequacy of the sample and the KMO value should be greater than 0.6 for a satisfactory analysis to proceed (Cronbach & Meehl, 1955). For the sample used in this study the KMO = 0.718.

### 4.4. Model testing

The study employed a multiple regression analysis to test the Liang and Xue's theoretical model using the following parameters: phishing attack and anti-phishing education as a malicious IT threat and safeguarding measure respectively.

The model testing results are shown in Fig. 2. The model calculated *R* square value for perceived threat, avoidance motivation, and avoidance behaviour, which was defined as how much of variance in the dependent variable is explained by its independent variables in the model (Davis et al., 1983). In the results for the model in this study 36% of variance is explained in perceived threat, 22% of variance in avoidance motivation, and 15% of

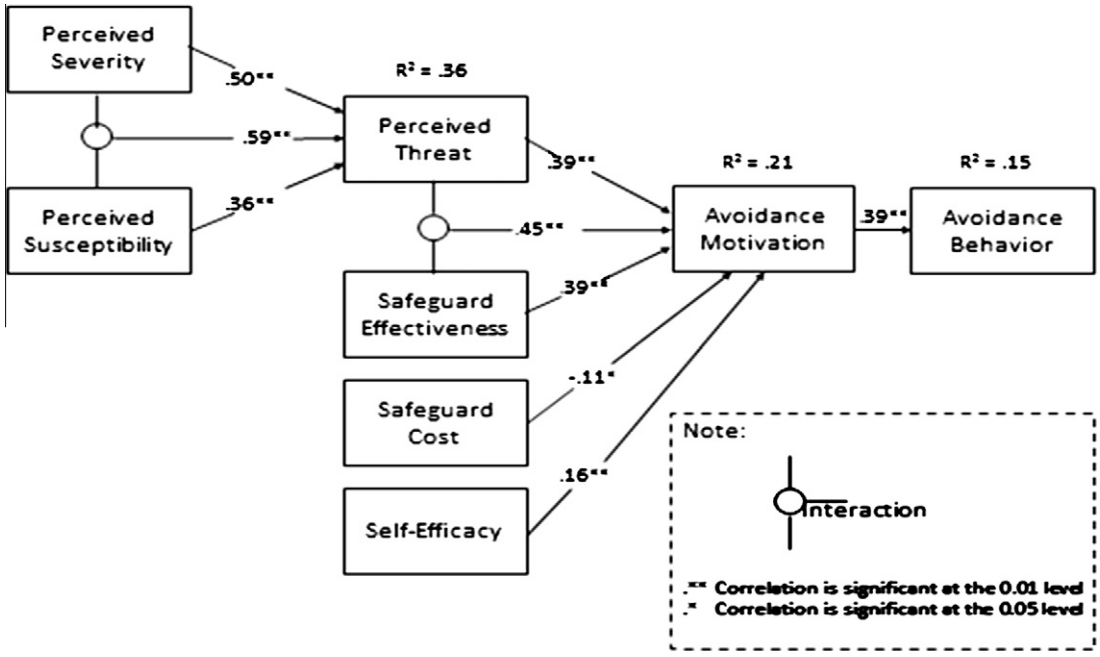


**Fig. 2.** Model testing results.

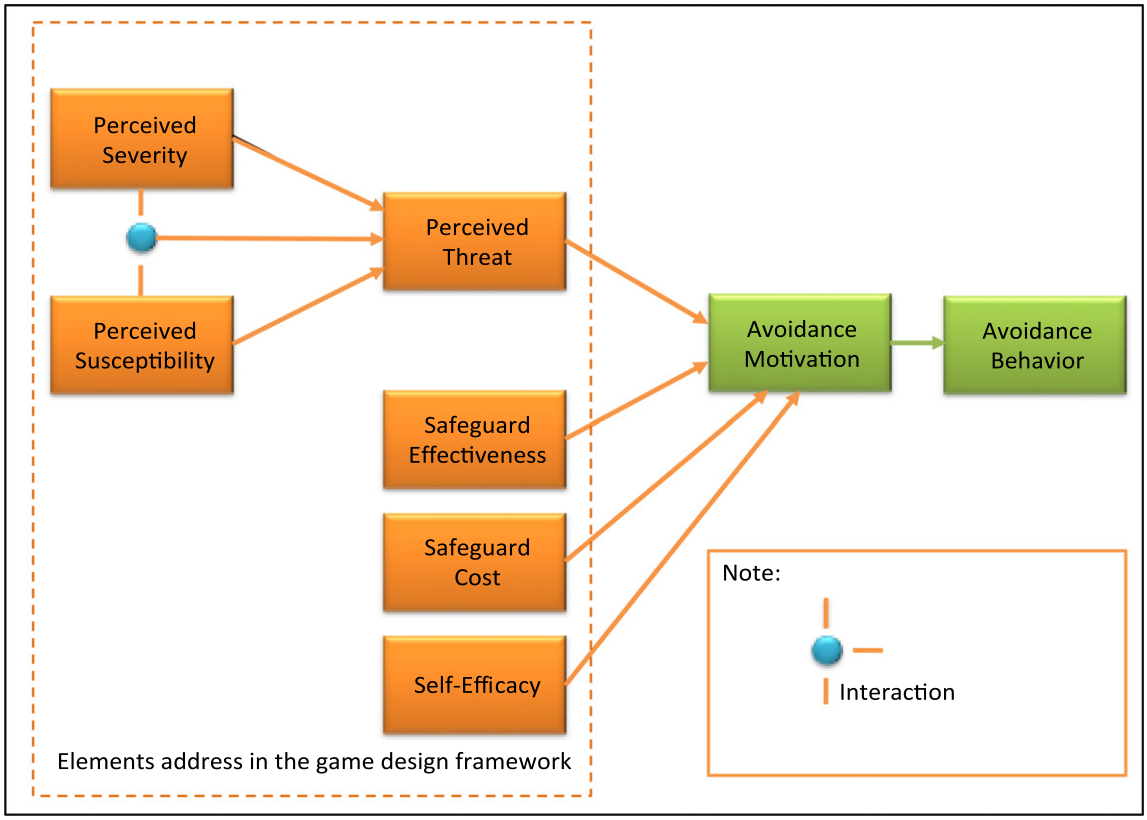


**Fig. 3.** The game design framework.

variance in avoidance behaviour. Pearson correlation analysis was then employed to describe the strength and direction of the linear relationship between two constructs. The results indicate that perceived threat is significantly determined by perceived severity ($r = .499^{**}$, and Sig. = .000) and perceived susceptibility ($r = .357^{**}$, and Sig. = .000). Avoidance motivation is significantly determined by perceived threat ($r = .386^{**}$, and Sig. = .000). According to Liang and Xue's and Baron and Kenny's research, these results show that the influences of perceived susceptibility and severity on avoidance motivation are fully mediated by perceived threat.

As Fig. 2 shows, avoidance motivation is also significantly determined by safeguard effectiveness ($r = .381^{**}$, and Sig. = .000),

self-efficacy ($r = .162^{*}$, Sig. = .047), and safeguard cost ($r = -.112^{*}$, Sig. = .037). Finally, avoidance motivation is found to be significantly influence by avoidance behaviour ($r = .390^{**}$, and Sig. = .000).

To evaluate the interaction effects of both perceived susceptibility and severity, and perceived threat and safeguard effectiveness, Chin et al.'s product-indicator approach was used (Chin, Marcolin, & Newsted, 2003). Interaction variables were created by cross multiplying the items of perceived susceptibility and severity, and perceived threat and safeguard effectiveness (Liang & Xue, 2010). As Fig. 2 shows, the interaction between perceived severity and susceptibility was statistically significant on perceived threat ($r = .588^{**}$, and Sig. = .000). Finally, the interaction between perceived threat and safeguard effectiveness was statistically significant on avoidance motivation ($r = .452^{**}$, and Sig. = .000).

In summary, the model testing results provided support to all of the hypotheses. Moreover, age, gender, and Internet experiences were included as control variables on avoidance motivation and avoidance behaviour in the model testing. However, none of these control variables was found to have a statistically significant effect on either avoidance motivation or avoidance behaviour. This is similar to the finding of Liang and Xue's empirical study.

## 5. Game design framework

This study empirically investigated what key elements should be addressed in the game design framework for computer users to avoid phishing attacks through motivation. The elements of a theoretical model derived from TTAT, was used to address in the game design framework. Fig. 2 shows the model testing results. The model accounts for 36% of variance in perceived threat, 21% of variance in avoidance motivation, and 15% of variance in avoidance behaviour. Perceived threat is significantly determined by perceived severity ($r = .499^{**}$, and Sig. = .000), perceived susceptibility ($r = .357^{**}$, and Sig. = .000) and their interaction ($r = .588^{**}$, and Sig. = .000). Therefore, perceived severity and perceived susceptibility elements addressed in the game design framework for computer users to thwart phishing attacks. As Fig. 2 shows, avoidance behaviour is significantly determined by perceived threat ($r = .386^{**}$, and Sig. = .000), safeguard effectiveness ($r = .381^{**}$, and Sig. = .000), and safeguard cost ($r = -.112^{*}$, Sig. = .037), and self-efficacy ($r = .162^{*}$, Sig. = .047). However, it is interesting to note that safeguard cost negatively effects avoidance motivation though it is significantly determined by avoidance motivation. This is because the user's motivation to avoid the IT threat is expected be reduced by the potential cost of using the safeguard measure (Liang & Xue, 2010). Therefore, perceived threat, safeguard effectiveness, safeguard cost, and self-efficacy elements should be addressed in the game design framework. Finally, avoidance motivation is found significantly influence avoidance behaviour ($r = .390^{**}$, and Sig. = .000).

In summary, this study results provided support to determine what key elements should be addressed in the game design framework for computer users to avoid phishing attacks through motivation. Therefore, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, perceived threat, and perceived susceptibility elements addressed in the game design framework. The game design framework is shown in Fig. 3.

## 6. Discussion

This study empirically investigated a game design framework for computer users to thwart phishing attacks. Therefore, phishing attack and anti-phishing education were considered as a malicious IT threat and safeguarding measure respectively in order to test a theoretical model derived from TTAT (Liang & Xue, 2010). The study paid particular attention to threat perception because it plays a vital role in influencing computer users' avoidance behaviour. Data analysis results showed in Fig. 2, the model is able to explain a considerable amount of variance in users' motivation to avoid IT threats (22%) and actual avoidance behaviour (15%). Therefore, this study conveys a simple, yet powerful message to motivate computer users to avoid malicious IT threats.

However, it is interesting to note that avoidance behaviour is quite low though it is significant (Pallant, 2007). There is a possible explanation for this result. When users decide that the IT threat can be avoided by the safeguarding measures, they may take a problem-focused coping measure. However, when the IT threat could not be avoided completely, they may take an emotion-focused coping approach (Liang & Xue, 2010; Liang & Xue, 2009 and Rhoa & Yub, 2011). Lazarus and Folkman asserted two types of coping could be performed to deal with the threat; problem-focused and emotion-focused (Lazarus & Folkman, 1984). Problem-focused coping referred to adaptive behaviors that take a problem-solving approach. It directly deals with the malicious IT threat by taking safeguarding measure such as updating password regularly, disabling cookies, and installing and configuring safeguarding IT. When people face the problem as a challenge, they seem to take a problem-oriented coping behavior and treat the problem as a thing that can be controlled. In contrast, emotion-focused coping, the problem identified as a threat and loss, people tend to perceive it as a thing cannot be solved by them and hence, take an emotional coping behavior. Beaudry and Pinsonneaut stated that if users perceive the malicious IT threat, they take problem-focused coping, or if they believe that the threat is not avoidable, they will inactively avoid the threat by performing emotion-focused coping (Beaudry & Pinsonneaut, 2001). Therefore, it can therefore be argued in the current study, that users' emotion-focused coping behaviour would have caused for avoidance behaviour of phishing threat, which will account for the variance of avoidance behaviour.

Computer users have to be convinced and feel that such malicious IT threats exist in the cyberspace and are avoidable. The study found some evidence in the data analysis results that the model is able to explain a respectable amount of variance in threat perception (36%). This figure is little higher than Liang and Xue's empirical study, which is 33% (Liang & Xue, 2010). Therefore, perceived threat element is significantly important to address in the game design framework for computer users to enhance avoidance behaviour through motivation to thwart phishing attacks. Furthermore, the study demonstrates threat perception that users need to be aware of likelihood and severity of being attacked by malicious IT threat. If users actually perceive the threat, they are more motivated to avoid it. The safeguarding measure was evaluated from three aspects; taking into account safeguard effectiveness, cost related to safeguard measure, and users confident of using the safeguard. If the level of effectiveness of the safeguarding measure is high then users are more motivated to avoid threats. So, the safeguard effectiveness element is important in the game design framework for computer users to thwart phishing threats. Users' high confidence in taking the safeguard measures influences their motivation to avoid threats. Therefore, self-efficacy should also be included in the game design framework for avoiding threats through motivation.

When the safeguard cost is high, users are less motivated to avoid threats. Liang and Xue describes when time, money, inconvenience and comprehension needed to use the safeguarding measure is high, users are less motivated to avoid threats (Liang & Xue, 2009; Liang & Xue, 2010). The current study results also demonstrated safeguard cost negatively affects avoidance motivation. Therefore, safeguard cost should address in the game design framework, as a payback to safeguarding effectiveness. Liang and

Xue's model testing results did not support the interaction between perceived severity and susceptibility on perceived threat (Liang & Xue, 2010). Surprisingly, this study revealed that perceived threat is significantly determined by the interaction between perceived severity and susceptibility ($r = .588^{**}$, and Sig. = .000).

Moreover, this study emphasises that avoidance motivation is significantly determined by the interaction of perceived threat and safeguard effectiveness ($r = .452^{**}$, and Sig. = .000). This result contradicts with Liang and Xue's findings regarding the interaction between perceived threat and safeguard effectiveness on avoidance motivation (Liang & Xue, 2010). However, they suggest the interaction between perceived threat and safeguard effectiveness can be viewed from two perspectives. First, when the threat level is high, perceived threat can be viewed to negatively moderate the relationship between safeguard effectiveness and avoidance motivation. Second, when the level of safeguard effectiveness is high, it can be viewed to negatively moderate the relationship between perceived threat and avoidance motivation. Therefore, this study does not provide evidence to address the interaction of perceived threat and safeguard effectiveness in the game design framework.

## 7. Conclusion and future work

This study attempted to develop a game design framework, which enhances computer users' avoidance behaviour through motivation to prevent themselves from phishing attacks. The study empirically investigated what elements should address in the game design framework for computer users to thwart phishing attacks. A theoretical model derived from TTAT was used to develop the game design framework. To test the model, phishing attack and anti-phishing education were considered as a malicious IT threat and safeguarding measure respectively.

Finally, the current study results provided support to define what elements should be included in the game design framework for computer users to thwart phishing attacks. Therefore, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, perceived severity, and perceived susceptibility elements should be incorporated into the game design framework for computer users to avoid phishing attacks through motivation.

Furthermore, for future research we will attempt to design and evaluate a mobile game using MIT App Inventor Emulator as a tool to educate computer users against the dangers of phishing attacks. The study will use the game design framework developed on the results from the study reported in this paper.

## References


Aggarwaly, A., Rajadesingan, A., Kumaraguru, P. (2012). PhishAri: Automatic realtime phishing detection on twitter. In *Seventh IEEE APWG eCrime researchers summit (eCRS)*. Las Croabas, Puerto Rico, 22–25 October 2012. <http://precog.iiitd.edu.in/Publications_files/AA_AR_PK_eCRS_2012.pdf> Accessed 03.12.12.

Allen, M. (2006). Social engineering: A means to violate a computer system. Tech. rep., SANS Institute.

Arachchilage, N. A. G., & Cole, M. (2011). Design a mobile game for home computer users to prevent from "phishing attacks". *Information Society (i-Society)*, 485–489. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5978543&isnumber=597843 Accessed 22.12.11.

Beaudry, A., Pinsonneault, A. (2001). IT-induced adaptation and individual performance: A coping acts model. In *Twenty-second international conference on, information systems* (pp. 475–480).

Brody, R. G., Mulig, E., & Kimball, V. (2007). Phishing, pharming and identity theft. *Journal of Academy of Accounting and Financial Studies, 11*, 43–56.

Champion, V., & Scott, C. (1997). Reliability and validity of breast cancer screening belief scales in African American women. *Nursing Research, 6*(46), 331–337.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic mail emotion/adoption study. *Information Systems Research, 2*(14), 189–217.

CNN.com, 2005. A convicted hacker debunks some myths. <http://www.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/index.html> Accessed 04.04.11.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: development of a measure and initial test. *MIS Quarterly, 19*, 189–211.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*, 297–334.

Cronbach, L. J., & Meehl, P. E. (1955). Construct validity in psychological test. *Psychological Bulletin, 52*, 281–302.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–338.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1983). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003.

Dhamija, R., Tygar, J. D. (2005). The battle against phishing: Dynamic security skins. In *Symposium on usable privacy and security SOUPS '05*, Pittsburgh, Pennsylvania, 6–8 July 2005 (Vol. 93, pp. 77–88). <http://doi.acm.org/10.1145/1073001.1073009> Accessed 20.03.11.

Dhamija, R., Tygar, J. D., Hearst, M. (2006). Why phishing works. In *The SIGCHI conference on human factors in computing systems*, Montréal, Québec, Canada, 22–26 April 2006.

Downs, J. M., Holbrook, M., Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Second symposium on usable privacy and security SOUPS '06*, Pittsburgh, Pennsylvania, 12–14 July 2006 (Vol. 149, pp. 79–90). <http://doi.acm.org/10.1145/1143120.1143131> Accessed 10.01.12.

Downs, J. S., Holbrook, M., Cranor, L. F. (2007). Behavioural response to phishing risk. In *Anti-phishing working groups – 2nd annual eCrime researchers summit*, October 2007, Pittsburgh, Pennsylvania (pp. 37–44) doi: 10.1145/1299015.1299019 Accessed 25.03.11.

Drake, C. E., Oliver, J. J., Koontz, E. J. (2006). *Mail frontier anatomy of a phishing email.* <http://www.mailfrontier.com/docs/MF_Phish_Anatomy.pdf> Accessed 03.04.11.

Grinter, R., Rodden, T., Aoki, P., Cutrell, E., Jeffries, R., Olson, G. (2006). *Eds.CHI '06* (pp. 581–590). <http://doi.acm.org/10.1145/1124772.1124861> Accessed 15.05.11.

Hiner, J. (2002). *Change your company's culture to combat social engineering attacks*. <http://articles.techrepublic.com.com/5100-1035_11-1047991.html> Accessed 15.07.11.

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social phishing. *communications of the ACM, 50*(10), 94–100.

James, L. (2005). *Phishing exposed*, Syngress, Canada.

Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika, 39*(1), 31–36.

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

Lazarus, R., & Folkman, S. (1984). *Stress, coping, and adaptation*. New York: Springer-Verlag.

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.

Miller, M. W. R., Garfinkel, S. (2005). *Do security toolbars actually prevent phishing attacks*, Posters SOUPS.

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology, 7*, 163–184.

Moreno-Ger, P., Burgos, D., Sierra, J. L., & Fernández-Manjón, B. (2008). Educational game design for online education. *Computers in Human Behavior, 24*(6), 2530–2540.

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.

Pallant, J. (2007). *A step by step guide to data analysis using SPSS for windows (Version 15), SPSS survival manual*. Buckingham: Open University Press.

Ponnurangam, K., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., Hong, J. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. In *APWG eCrime researchers summit*, 4–5 October 2007, Pittsburgh, PA, USA.

Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. *Information Management & Computer Security, 20*(5), 382–420. http://dx.doi.org/10.1108/09685221211286548. Accessed 03.12.12.

Rhoa, H., Yub, I. (2011). *The impact of information technology threat avoidance factors on avoidance behavior of user.*

Richmond, R. (2006). *Hackers set up attacks on home PCs, financial firms: Study*. <http://www.marketwatch.com/News/Story/Story.aspx?dist=newsfinder&siteid=google&guid=%7B92615073-95B6-452EA3B9 569BEACF91E8%7D&keyword=> Accessed 27.03.11.

Robila, S. A., Ragucci, J. W. (2006). Do not be a phish: steps in user education. In *11th annual SIGCSE conference on innovation and technology in computer science education*, Bologna, Italy, June 2006, 26–28. doi: 10.1145/1140124.1140187 Accessed 29.03.11.

Rosenstock, I. M. (1974). The health belief model and preventive health behavior. *Health Education Monographs, 2*, 354–386.

Saleeby, J. R. (2000). Health beliefs about mental illness: an instrument development study. *American Journal of Health Behavior* (24), 83–95.

Sanchez, F., Duan, Z. (2012). A sender-centric approach to detecting phishing emails. In *ASE/IEEE international conference on cyber security*, Washington DC, USA, December 14–16, 2012. <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. <http://www.schneier.com/crypto-gram-0010.html> Accessed 02.04.11.

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

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.

Smith, H., Milberg, S., & Burke, S. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167–196.

Sonderegger, A., & Sauer, J. (2010). The influence of design aesthetics in usability testing: effects on user performance and perceived usability. *Applied Ergonomics, 41*(3), 403–410.

Timko, D. (2008). The social engineering threat. *Information Systems Security Association Journal.*.

Walls, R. (2012). Using computer games to teach social studies. *Digital Media; Project Assignment*, Uppsala University, <http://uu.diva-portal.org/smash/record.jsf?pid=diva2:561746> Accessed 03.12.12.

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

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.

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

Zaharias, P., & Poylymenakou, A. (2009). Developing a usability evaluation method for e-learning applications: beyond functional usability. *International Journal of Human–Computer Interaction, 25*(1), 75–98.

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. <http://lorrie.cranor.org/pubs/toolbars.html> Accessed 04.06.11.