Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.016660
Article

Tech Science Press

Assessing User's Susceptibility and Awareness of Cybersecurity Threats

Maha M. Althobaiti*

College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
*Corresponding Author: Maha M. Althobaiti. Email: maha_m@tu.edu.sa
Received: 07 January 2021; Accepted: 07 February 2021

Abstract: Cybersecurity threats, including those involving machine learning, malware, phishing, and cryptocurrency, have become more sophisticated. They target sensitive information and put institutions, governments, and individuals in a continual state of risk. In 2019, phishing attacks became one of the most common and dangerous cyber threats. Such attacks attempt to steal sensitive data, such as login and payment card details, from financial, social, and educational websites. Many universities have suffered data breaches, serving as a prime example of victims of attacks on educational websites. Owing to advances in phishing tactics, strategies, and technologies, the end-user is the main victim of an attack scenario. According to several studies, the end-user can play a significant role in preventing a phishing attack. Therefore, this study was conducted to investigate the levels of user awareness regarding cyber threats and explore the relationship between the knowledge on cybercrimes and the awareness of phishing, within the context of cybercrime targeting educational websites. An observational experiment using 'think aloud' method was conducted with 20 students from Taif University. The results indicated that although the participants demonstrated an advanced level of information technology experience as specialists in computer science and computer engineering, their susceptibility to phishing was high. The results of this study will contribute to the cybersecurity research field in terms of proposing risk management plans, delivering embedded training to end-users, and improving spam detecting tools.

Keywords: Cybersecurity; cyberthreats; cybercrimes; spam; awareness

1 Introduction

Cybersecurity threats have become a popular research area in the field of computer security. Different fields and technologies, such as education, healthcare, Internet of Things, and big data, are affected by cybersecurity attacks [1]. The damage caused by cybercrimes can be classified into two main cost categories: economic and moral. In terms of economic harm, companies may lose valuable and sensitive information or large amounts of capital because of cyber-attacks. In terms of moral damage, the misuse of any stolen identity information may significantly affect an individual's or organization's reputation [2].

The Anti-Phishing Working Group defines phishing as "a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account

credentials" [3]. The process of phishing is usually conceived by expert web designers who create websites that appear to be legitimate; then, they steal personal information when victims access and interact with such sites. Another commonly used phishing tactic involves sending an email as a first attempt to steal sensitive and valuable information, such as identity and bank details, by asking the victim to click on a link or download a file. Such emails are usually designed to appear legitimate to the user. Users play a significant role in phishing attack scenarios, and the user's response to a scam can enhance cyberspace security [4]. Therefore, approaches should be developed to increase user awareness and provide users with knowledge of cyberattacks [5].

Attackers also use spam emails that are designed to appear as communications from legitimate sources [6]. Cybercrimes committed through spam emails are considered one of the most frequently used approaches for distributing malware and implementing other established cybercrimes, such as stealing personal information [7]. Spam can comprise meaningless advertisements through unwanted emails, messages, or social media communications. However, these can also contain malware or malicious bots/viruses that have been created to access the recipient's confidential information from the receivers [6]. Although spam might appear to have a minor impact at the individual level, one study reported that in 2018, the daily global average of spam emails was approximately 400 billion, representing over 80% of all daily email communications during that year [8]. Such a prevalent and universal threat of malware-based spam can have a major impact on both economic and social welfare [6].

According to Cybersecurity Ventures, by 2021, cybercrime will cost the world approximately six trillion dollars annually compared to three trillion dollars in 2015 [9]. In 2019, phishing attacks were considered one of the most dangerous types of cyber-attacks [10]. Moreover, spam emails have been reported to be one of the ten deadly cybersecurity threats amid the COVID-19 pandemic [11]. Phishing and denial-of-service attacks that aim to steal documents are the most common cyberthreats to educational institutions. For example, websites belonging to universities in the United Kingdom suffered damaging attacks [12]. One such university was attacked 100 times in one month [12]. Decreasing victimization of educational websites in phishing attacks will have a substantial economic and educational impact and make cyberspace more secure. Therefore, an observational experiment was conducted in the present study to investigate users' awareness and ability to identify spam and phishing emails.

The remainder of this paper is organized as follows. Section 2 presents a review of relevant research on users' susceptibility to cybercrimes. Section 3 outlines the methodology used to conduct this study, including the selected educational organization, experimental design, and procedure. Section 4 describes the findings and results. Finally, Section 5 summarizes the general conclusions derived from the study.

2 Literature Review

Although several studies have focused on understanding and investigating methods and tools used in cybercrimes, such as phishing [13,14], limited research has been conducted to understand users' perceptions of cybercrimes or their level of awareness of such crimes. Societal, economic, and other vital infrastructures have become fundamentally reliant on internet technologies and information system solutions [6]. Consequently, cybercrimes have become more frequent and catastrophic.

In a study on social engineering, spear-phishing, which targets specific victims, and phishing attacks, Butavicius et al. [15] examined the impact of various social engineering techniques by sending phishing and legitimate emails to over 121 university students. Their results suggested that students often viewed both types of emails as genuine and not malicious. Students could not distinguish between spear-phishing attempts and standard phishing attacks. Furthermore, spear-phishing emails often applied an authority-based social engineering approach, so students received spam emails from a sender who had some authority at their school. Consequently, the students were more inclined to treat such emails as genuine.

Sun et al. [16] explored the impact of internet self-efficacy on anti-phishing behavior using a questionnaire survey of 434 university students. Their findings revealed that experience and technical knowledge enhanced internet users' threat perception and anti-phishing behavior. Similarly, in a study on the factors affecting vulnerability to phishing attacks, Iuga et al. [17] conducted a web-based evaluation of 382 respondents, asking them to distinguish genuine websites from phishing pages. They discovered that gender and knowledge of computer systems significantly impacted the effective detection of phishing emails or attacks. Meanwhile, Broadhurst et al. [6] argued that the impact of technical knowledge on phishing vulnerability is not yet completely understood.

Considering the social engineering aspect of cybercrimes, some studies have focused on educating users as an effective means of attack prevention [18–21], resulting in a web-based game for teaching users how to detect phishing scams [22,23]. Other studies have focused on using software to detect phishing through machine learning, uniform resource locator (URL) feature classification, and contextual analysis [24–27].

Carella et al. [28] performed an experiment in which participants received various levels of security awareness training and used different approaches to analyze phishing scam software. They found that security awareness training reduced the number of times users clicked on links contained in phishing attacks. In another empirical study, Alsharnouby et al. [27] used an eye-tracking method for obtaining objective quantitative data to discover which strategies users employed to determine if a website was legitimate. The results revealed an average success rate of only 53%. Furthermore, the participants spent only 6% of the total experiment time looking at security indicators, such as the URL bar and the SSL padlock, to determine website legitimacy.

Hasan et al. [29] evaluated the relationship between various factors, including users' age, knowledge on cybercrime, and awareness of risks involved with cybercrimes. They quantitatively surveyed 342 accounting students at the Universiti Teknologi MARA, Shah Alam, Malaysia. The results showed that female students were more aware of cyber threats, such as phishing and spam attacks, than their male counterparts. Moreover, well-educated students aged 18–23 years showed a higher level of awareness of cybercrimes and the potential risks of such attacks.

The relationship between certain demographic factors and users' responses to cyber-attacks has been examined in several studies. For instance, in a quasi-experimental study, Broadhurst et al. [6] recruited 138 students and subjected them to some form of social engineering. The researchers sent spam emails and phishing attacks. The spam emails were focused on prompting the recipients to either provide personal information or click on fake links that could introduce malicious code to their systems. This study revealed that first-year students tended to be more susceptible to phishing attacks than more experienced students.

Abbasi et al. [30] investigated whether online users with heightened safety awareness might be more observant and apply security countermeasures. They sampled 509 university students and created three clusters: those who had a high level of knowledge on information technology (IT) tools and avoided potential phishing risks, those who had experienced previous phishing attacks and did not trust or avoided phishing websites, and those with a higher level of awareness and considerable experience with phishing attacks. The researchers concluded that online users who effectively detected phishing attacks were often those who were knowledgeable about phishing attack methods and understood the potential impact of such attacks. However, the researchers also discovered that some of these strategies negatively affected the users' ability to identify phishing attacks effectively because previous experiences and phishing knowledge appeared to make users over-confident in identifying such attacks. The results suggested that higher awareness of cyber risks and susceptibility to such risks could reduce phishing attacks.

In a study focused on exploring individual differences in information security awareness, Hadlington et al. [31] had over 1,000 participants complete a survey created to investigate users' vulnerability to

cybercrimes. The researchers adopted a unique approach by examining the relationship between cybercrime awareness and personality attributes (i.e., impulsivity). The results showed that 60% of the survey respondents were highly vulnerable to a wide range of cyber-attacks. Users who showed a lower level of information security awareness combined with higher impulsivity were highly vulnerable to cybercrimes. The results highlighted that students could potentially be classified as low risk with increased knowledge on cybercrimes, such as phishing attacks, that could aid in effectively detecting attacks such as phishing attacks.

Thus, it can be deduced that there is increasing awareness of the significance of human factors in effectively preventing cybercrimes and improving information security [32]. However, current security approaches and technological solutions appear to be ineffective in preventing cybercrimes. This could be because of online users failing to adopt the required security protocols when using the Internet or their tendency to partake in activities that increase their susceptibility to cybercrimes [33]. Therefore, it is crucial to understand end-users' vulnerability to cybersecurity threats. Identifying such vulnerabilities will help security tool developers in creating effective security solutions to increase users' awareness of cybercrimes. This study suggests that such preventative solutions would aid in reducing educational institutions' risk of suffering from cyber attacks such as spam emails.

This study aims to investigate the level of user awareness regarding phishing emails that target education websites. It uses a think-aloud method, which, to our knowledge, has never been used before in phishing investigation studies. Here, the user was asked to perform a specific task and verbally explain their thoughts while completing an assignment [34].

3 Materials and Methods

This section describes the methodology used to investigate users' susceptibility to and awareness of phishing. First, a specific educational institution was selected to investigate the level of spam and phishing emails it received and what approach it used to detect such emails. Second, an experiment and associated procedure, tailored to the users' educational institution, were designed.

3.1 Selection of an Educational Institution

Taif University in the Kingdom of Saudi Arabia was selected in this study as a sample educational institution. Its website (www.tu.edu.sa) (see Fig. 1) is used by current students and visitors and provides visitors with the information needed to apply and study at the university. It also provides enrolled students with numerous electronic services, including a learning management system, email, a digital library, and information regarding the academic system. Similar to other universities, Taif University has faced various cybersecurity threats, of which phishing is among the most common. The Deanship of E-learning and Information Technology uses one of the most popular and advanced detection tools to automatically repel potential spam and phishing messages. However, these tools cannot repel all types of malicious messages. Moreover, user awareness is required to detect email fraud. Therefore, in this study, the Deanship of E-learning and Information Technology was requested to send some of the detected phishing emails to the researcher (see Fig. 2). An analysis of the content of these emails showed that most had the subject heading "Call for papers" and requested the recipient to click on a link to a malignant website or an invitation to join a Microsoft Teams meeting. These emails appeared to target both academic and support staff to steal research and other information. Based on the Deanship's reports on detected spam and phishing emails.

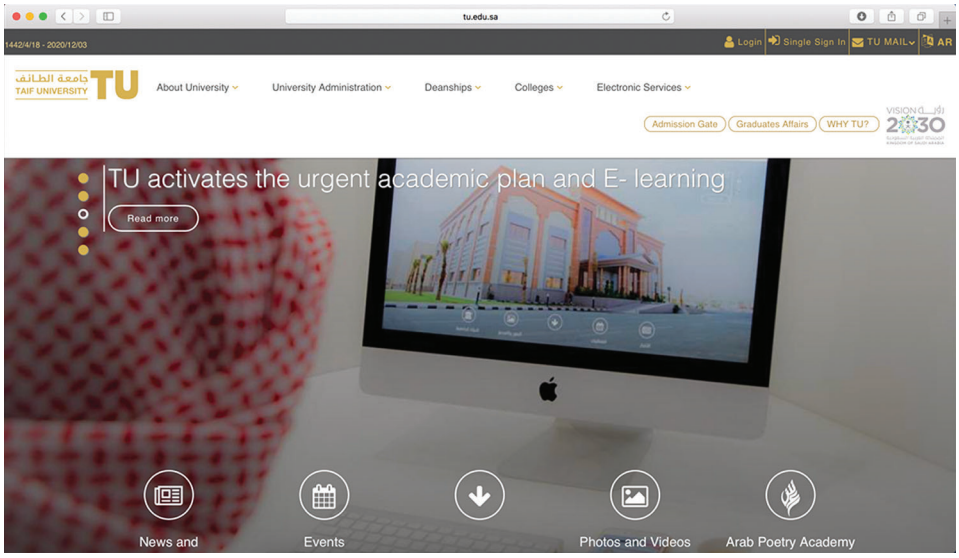

Figure 1: Home page of Taif University's website

Figure 2: Sample of spam email received by a user at Taif University

3.2 Experimental Design and Procedure

To fulfil the aim of the study, an experimental approach known as a think-aloud protocol was used. This protocol is defined as a method that requests the subjects to express their thoughts during their performance of an experimental task [34,35]. The experimental task was based on the analysis of actual phishing emails, as explained in Section 3.1, to obtain results that were as accurate as possible. In the task, 50% of the

participants received a phishing email that invited them to join a lecture by providing their personal information. The remaining participants received two emails: one was a phishing attempt, and the other was a genuine invitation for the participant to join a lecture by clicking on the provided link. The task was presented to the participants in a format that facilitated the simulation of a real-world context and improved the ecological validity of the task [36]. The participants were then asked to check their email, identify the message from their lecturer, and accept the invitation to join a lecture by replying to the email.

Because the study was conducted during the COVID-19 pandemic, an online approach was implemented using the Blackboard system, which is an application used for online learning, teaching, and discussion. The researcher, who was present during the experiment, asked the participants to think aloud. The researcher did not engage with the participants during the experiment but was responsible for calculating the time each participant took to perform the task and guiding them to fill out the post-experiment questionnaire. All participants performed the same task, the only difference being that 50% of them received two emails instead of one. The researcher's intention was to observe whether the participants receiving two emails would detect a similarity in the name of the sender of both emails.

The procedure for each experiment was as follows. The researcher divided the students into two breakout groups. They were then sent to a control room or an experiment room and instructed to read the consent form, fill the pre-experiment questionnaire, and perform the requested task while sharing their computer screen and thinking aloud. After finishing the task, the participants were asked to complete the post-experiment questionnaire. During the experiment, the observer filled an observation sheet for each user. This sheet recorded the participant's interaction with the received email and captured other information, such as the date of the experiment, duration of each task, and other participant comments.

The user's susceptibility and awareness of phishing were measured using four identified security attributes: attention, caution, motivation, and wariness. These attributes were used by Althobaiti et al. [37] and can be applied in any security task. Tab. 1 lists the security measurements used in the experiment in this study.

Table 1: Security attributes used in the experiment

Security attribute	Security measurement
Attention	Check the email subject, sender name, and notice of both emails.
Caution	Check the sender email.
Motivation	Interacting with the email by replying or clicking on the invitation link.
Wariness	Providing the sender with the required data (personal data).

3.3 Participants

The study sample comprised students at Taif University because the task simulated a spam email targeting the members of this university. A sample size of 20 participants as stated by Macefield [38] provides statistically significant results in the think-aloud method. Therefore, the required number of 20 participants was met; more participants were also welcomed. A notice was placed on the college blackboard to invite any interested students to participate in a research experiment spanning two weeks. All the recruited participants (females) were from the computer sciences and computer engineering departments of the Computing and Information Technology College.

3.4 Data Collection

In this study, data were collected through observation and a questionnaire. An observation sheet was used, as described in Section 3.2, to record the participants' thoughts, start and end times of the task, and any participant comments. The questionnaire included a pre-experiment section and a post-experiment section. The pre-experiment questionnaire consisted of several demographical questions, whereas the post-experiment survey focused on the knowledge on cybercrime and Internet usage.

4 Results and Discussion

Most of the participants (95%) used social media, 60% rated their IT experience as adequate, and 20% rated their IT experience as advanced (see Tab. 2). All the participants, except one, had experience in online shopping. Four participants shopped online frequently, 13 shopped sometimes, and two participants rarely shopped online.

Table 2: Social media use, IT experience, and online shopping

Social media use	
Yes	95%
No	5%
Level of IT experience	
Advanced	20%
Above average	20%
Adequate	60%
Online shopping	
Frequently	20%
Sometimes	65%
Rarely	10%
Never	5%

We also measured the four aforementioned security attributes: attention, caution, motivation, and wariness. Attention was measured by checking the email's subject line and sender name and noticing the difference in the sender names. One group received two emails, phishing and genuine, in which the sender names differed by one letter. During the experiment, by observing the participants and listening to their thought process, it appeared that none of them had read the email subject line. In the group that received two emails, none had noticed the difference in the sender names. Moreover, none of the participants in either group exhibited any hesitation in opening the email.

Caution was measured by observing whether the participants checked the email's sender. The results revealed that none of the participants in either group checked the sender's email address either before or after reading the email's content. This indicates that verifying the sender's email address is not habitual, even if the email's presentation or content is unusual.

Motivation was measured by observing the users' reaction to the email's content. Only six participants (30%) read the email's content very carefully. Four of those participants hesitated to reply and asked whether they were required to reply. Two expressed hesitation in providing all the required information, including name, email address, and national ID number, by asking whether it was compulsory to give their national

ID number. The remaining 70% of the participants did not present any concern or apprehension and quickly read and replied to the email. An analysis of the observation sheet of the group that received two emails showed that no one in that group hesitated to click on the link that invited them to a lecture session.

Wariness was measured by whether the users replied to the email. The results revealed that 90% of the participants responded to the email and provided all the required information. Based on this, it can be assumed that the participants did not have any experience in the domain of security and were not aware of the effects of their actions or decisions with respect to the provision of personal information via email. The results of this study contrast those of Hasan et al. [29], who showed that female and well-educated students have a high level of awareness of cybercrimes. The experiment in this study, however, which was conducted on a sample comprising only well-educated females, did not show that the participants have a high level of awareness of cybercrimes. Moreover, they were unware of the potential risks of providing personal information without checking the sender's email to ensure that their details are provided to known persons only.

All the participants reported that they had not been victims of cybercrimes prior to the experiment. Regarding the post-experiment question on the safety of the Internet, 65% of the participants considered the Internet to be safe to some extent, 30% considered it to be unsafe to some extent, and 5% (one participant) considered it not safe at all. However, this single student did not appear to be careful during the experiment and replied to the phishing email. Furthermore, 12 participants indicated that they could recognize and discover cybercrimes, whereas five indicated that they could not; those who indicated they could recognize cybercrimes had no prior experience with them. The last two questions were regarding whether the participant received phishing emails and what they did with such emails (see Tab. 3). Although most of the participants indicated that they take action regarding the spam email, they were unable to identify the spam email during the experiment. Thus, the low level of the participants' awareness of phishing emails points to their poor knowledge of cybercrimes, because phishing is considered to be a cybercrime as it aims to steal sensitive and important information.

Table 3: Post-questionnaire results

Recognize cybercrime	
Strongly agree	1
Agree	12
Neutral	2
Disagree	5
Internet safety	
To some extent safe	13
To some extent unsafe	6
Not safe at all	1
Reception of phishing email	
Frequently	0
Sometimes	3
Rarely	10
Never	7
Response to phishing email	
Block	8
Ignore	6
Delete	6

The completion time of the experiment was measured from when the user checked the email inbox until they replied to the email. The average time spent was 1.62 min; three students spent more than 2 min. The completion time for each group is shown in Fig. 3.

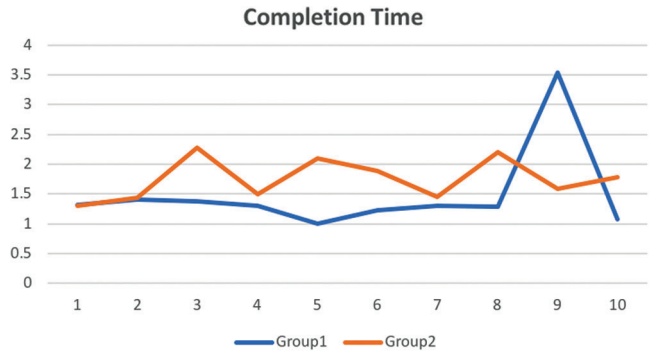

Figure 3: Comparison of completion time between the two groups

5 Conclusion

In this study, levels of user awareness of cyberthreats to an educational website were investigated through an observational experiment. The results, based on an analysis of their response to a phishing email, indicate that the participant's level of awareness of phishing email was quite low. Moreover, the results reveal that although the participants indicated an advanced level of IT experience as specialists in computer science and computer engineering, their susceptibility to phishing was nevertheless high. The main limitation of this study is that the entire sample comprised of people who had attained the same education level and belonged to the same age group and the same gender. Thus, future work should consider participants from different age groups and genders and with varied education levels. The results of the present study will be useful in proposing risk management plans, delivering embedded training to end-users, designing warning messages, and improving spam-detecting tools.

Acknowledgement: The author would like to thank the Deanship of E-learning and Information Technology in Taif University for their support by sharing information and samples of spam emails.

Funding Statement: This study was funded by the Dean of Scientific Research, Taif University, KSÁ (research project number 440-6129).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] D. K. Alferidah and N. Jhanjhi, "Cybersecurity impact over Bigdata and IoT growth," in *Int. Conf. on Computational Intelligence (ICCI)*. Bandar Seri Iskandar, Malaysia, pp. 103–108, 2020.

[2] D. K. Oropeza Mendoza, "The scam in the ciber space: Phishing," *Journal of Forensic Sciences & Criminal Investigation*, vol. 4, no. 1, pp. 1–3, 2017.

[3] Anti-Phishing Working Group. *Phishing Activity Trends Report*, 2017 [Online]. Available: https://ttcsirt.gov.tt/documents/phishtrend.pdf

[4] N. A. G. Arachchilage, C. Namiluko and A. Martin, "A taxonomy for securely sharing information among others in a trust domain," in *8th Int. Conf. for Internet Technology and Secured Transactions (ICITST-2013)*. London, UK, pp. 296–304, 2013.

[5] M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," *Arabian Journal for Science and Engineering*, vol. 45, no. 1, pp. 3171–3189, 2020.

[6] R. Broadhurst, K. Skinner, N. Sifniotis, B. Matamoros-Macias and Y. Ipsen, "Phishing and cybercrime risks in a university student community," *International Journal of Cybersecurity Intelligence & Cybercrime*, vol. 2, no. 1, pp. 4–23, 2019.

[7] M. Alazab and R. Broadhurst, "An analysis of the nature of spam as cybercrime," in *Cyber-Physical Security*. Cham: Springer, pp. 251–266, 2017.

[8] Talos. *Email & Spam Data*, 2018 [Online]. Available: https://www.talosintelligence.com/reputation center/emailrep#global-volume

[9] Cybersecurity Ventures. *Cybercrime Damages $6 Trillion by 2021*, 2017 [Online]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[10] University of San Diego. *Cyber Security Threats in 2019*, 2019 [Online]. Available: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

[11] N. A. Khan, S. N. Brohi and N. Zaman, "Ten deadly cyber security threats amid COVID-19 pandemic," Taylor's Univ., Selangor, Malaysia, Tech. Rep. techrxiv.1227892.v1, 2020.

[12] BBC News. UK Universities Targeted by Cyber-Thieves, 2017 [Online]. Available: https://www.bbc.com/news/technology-41160385

[13] J. R. C. Nurse, "Cybercrime and you: How criminals attack and the human factors that they seek to exploit," in *The Oxford Handbook of Cyberpsychology*. Oxford: Oxford University Press, pp. 662–690, 2018.

[14] J. R. C. Nurse and M. Bada, "The group element of cybercrime: Types, dynamics, and criminal operations," in *The Oxford Handbook of Cyberpsychology*. Oxford: Oxford University Press, pp. 690–715, 2018.

[15] M. Butavicius, K. Parsons, M. Pattinson and A. McCormac, "Breaching the human firewall: Social engineering in phishing and spear phishing emails," in *Australasian Conf. on Information Systems*. Adelaide, Australia, pp. 12–23, 2015.

[16] J. C. Y. Sun, S. J. Yu, S. S. J. Lin and S. S. Tseng, "The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference," *Computers in Human Behavior*, vol. 59, no. 4, pp. 249–257, 2016.

[17] C. Iuga, J. R. C. Nurse and A. Erola, "Baiting the hook: Factors impacting susceptibility to phishing attacks," *Human-Centric Computing and Information Sciences*, vol. 6, no. 1, pp. 1, 2016.

[18] I. Kirlappos and M. A. Sasse, "Security education against phishing: A modest proposal for a major rethink," *IEEE Security & Privacy Magazine*, vol. 10, no. 2, pp. 24–32, 2012.

[19] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, IN: John Wiley & Sons, 2002.

[20] B. Schneier, "Semantic attacks: The third wave of network attacks," in *Crypto-Gram Newsletter*, 2017 [Online]. Available: http://www.schneier.com/crypto-gram-0010.html

[21] A. Ferreira, L. Coventry and G. Lenzini, "Principles of persuasion in social engineering and their use in phishing," in *Human Aspects of Information Security, Privacy, and Trust HAS 2015*. Cham: Springer, pp. 36–47, 2015.

[22] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor *et al.,* "Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish," in *Proc. of the 3rd Sym. on Usable Privacy and Security—SOUPS '07*, New York, NY, USA, pp. 88–99, 2007.

[23] N. A. G. Arachchilage and S. Love, "A game design framework for avoiding phishing attacks," *Computers in Human Behavior*, vol. 29, no. 3, pp. 706–714, 2013.

[24] R. P. Khadir and P. Sony, "Efforts and methodologies used in phishing email detection and filtering: A survey," *International Journal of Advanced Research in Computer Science*, vol. 6, no. 2, pp. 23–27, 2015.

[25] J. Wang, Y. Li and H. R. Rao, "Overconfidence in phishing email detection," *Journal of the Association for Information Systems*, vol. 17, no. 11, pp. 759–783, 2016.

[26] V. S. Lakshmi and M. S. Vijaya, "Efficient prediction of phishing websites using supervised learning algorithms," *Procedia Engineering*, vol. 30, pp. 798–805, 2012.

[27] M. Alsharnouby, F. Alaca and S. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," *International Journal of Human-Computer Studies*, vol. 82, pp. 69–82, 2015.

[28] A. Carella, M. Kotsoev and T. M. Truta, "Impact of security awareness training on phishing click-through rates," in *2017 IEEE Int. Conf. on Big Data (Big Data)*. Boston, MA, USA, pp. 4458–4466, 2017.

[29] M. S. Hasan, R. A. Rahman, S. F. H. B. T. Abdillah and N. Omar, "Perception and awareness of young internet users towards cybercrime: Evidence from Malaysia," *Journal of Social Sciences*, vol. 11, no. 4, pp. 395–404, 2015.

[30] A. Abbasi, F. M. Zahedi and Y. Chen, "Phishing susceptibility: The good, the bad, and the ugly," in *2016 IEEE Conf. on Intelligence and Security Informatics (ISI)*. Tucson, AZ, USA, pp. 169–174, 2016.

[31] L. Hadlington and S. Chivers, "Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors," *Policing: A Journal of Policy and Practice*, vol. 14, no. 2, pp. 479–492, 2020.

[32] M. Anwar, W. He, I. Ash, X. Yuan, L. Li *et al.,* "Gender difference and employees' cybersecurity behaviors," *Computers in Human Behavior*, vol. 69, no. 3, pp. 437–443, 2017.

[33] L. Hadlington and K. Parsons, "Can cyberloafing and internet addiction affect organizational information security?," *Cyberpsychology Behavior, and Social Networking*, vol. 20, no. 9, pp. 567–571, 2017.

[34] R. Jääskeläinen, "Think-aloud protocols," in *Routledge Encyclopedia of Translation Studies*. London: Routledge, pp. 269–273, 2001.

[35] C. Lewis and J. Rieman, *Task-Centered User Interface Design: A Practical Introduction*. New York, NY, USA: ACM, 1993.

[36] J. S. Dumas and J. C. Redish, *A Practical Guide to Usability Testing*. Bristol: Intellect Books, 1999.

[37] M. M. Althobaiti and P. Mayhew, "Users' awareness of visible security design flaws," *International Journal of Innovation, Management and Technology*, vol. 7, no. 3, pp. 96–100, 2016.

[38] R. Macefield, "How to specify the participant group size for usability studies: A practitioner's guide," *Journal of Usability Studies*, vol. 5, no. 1, pp. 34–45, 2009.