Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks

Therdpong Daengsi1 · Phisit Pornpongtechavanich2 · Pongpisit Wuttidittachotti3

Received: 19 February 2021 / Accepted: 8 November 2021 / Published online: 15 November 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract
Cybersecurity is crucial at present because cyber threats (e.g., phishing) have become a very common occurrence in everyday life. A literature review showed that there are no studies based on cybersecurity awareness which involved a large number of Thai users. Thus, this research focused on the cybersecurity awareness of approximately 20,000 nationwide employees in a large financial institution in Thailand. The study consisted of three phases, a first phishing attack, knowledge transfer through a mixed-approach and a second phishing attack with different content. After data validation and analysis of the results, it was found that the level of cybersecurity awareness of employees improved significantly. The number of employees who opened the phishing email decreased by 71.5%. Therefore, this approach could be applied to cybersecurity enhancement in other organizations and other sectors/industries. Also, it was found that gender played a significant role in cybersecurity awareness within the Thai cybersecurity ecosystem since Thai female employees were found to have a higher level of cybersecurity awareness than male employees. Furthermore, it was found that the different generations of Thai employees (Generations Y and X and Baby Boomers) did not affect cybersecurity awareness.

Keywords Cybersecurity · Phishing · Cybersecurity Awareness · Knowledge Transfer · Gender · Age

1 Introduction

At present, Internet technology provides people with many benefits (Gupta et al., 2018). For example, they can gain access to many online services:
voice over IP / video telephony (e.g., Facebook messenger and LINE)
- e-commerce / online shopping (e.g., Amazon and eBay)
- e-learning / virtual classroom (e.g., Zoom, Google Meet and Microsoft Teams)
- video-conferencing / teleconferencing / virtual conferencing
- social media networking (e.g., Facebook, Twitter, WhatsApp, Instagram and Snapchat)
- video streaming (e.g., YouTube and Netflix)
- online gaming (e.g., League of Legends and Arena of Valor)
- Internet banking

Particularly, those small and medium enterprises (SMEs) affected by the COVID-19 pandemic, (e.g., restaurants, barber shops, spa and massage therapy shops, dental clinics and convenience stores) are being impacted, since the governments in many countries control their hours of business and the number of customers. However, these businesses can use Internet technology maintain their operations. For example, people can order goods or food using mobile applications and a wait delivery at home. Also, many people can work from home, while students can study online instead of in the classroom. Nevertheless, due to the growth of the Internet, cyber threats are affecting users’ lives (e.g., personal information leakage) more and more. While security issues are very hard to avoid (Yeom et al., 2020), it has been pointed out that the vulnerability of most security systems stems from users’ lack of knowledge of how to use the of the technology, so information leakages by insiders are common (Yeom et al., 2020).

Previously, cyber-attacks were normally indiscriminate without a specific target. However, current cyber-attacks have transformed into goal-oriented attacks on designated targets (Kim et al., 2019a, 2019b). They have also become more complex and advanced. One kind of serious cyber-attack in this era is phishing. In these attacks the phishers usually try to steal users’ credentials by using fake email accounts and/or fake websites (Chaudhry et al., 2016). According to a report on data breaches by Verizon, as in (Anstett, 2021), it was mentioned that 30% of phishing emails were read by the victims (Cranor, 2018). Also, it was reported that 12% of those victims clicked on fake websites or bogus attachments (Chen et al., 2018) and about 50,000 or 20% of the employees from a total of 250,000 employees in one well-known organization clicked on a malicious link. Based on breaches involving industries, it was announced by Verizon that about 10% of the breaches were in the financial industry (Verizon, 2019) causing significant financial loss not only to the financial companies but also to their customers and staff. Furthermore, it was mentioned that gender and age affect cybersecurity awareness as shown in a few previous studies (Farooq et al., 2015; Fatokun et al., 2019; Verkijika, 2019).

In view of the above information, a few interesting issues related to cybersecurity awareness of the employees within a financial organization in the Kingdom of Thailand were raised, since financial organizations are concerned with cyber-attacks, including phishing (Wei et al., 2020). Some of these issues were: 1) the level of cybersecurity awareness of Thai users at present 2) improvements in the approach to cybersecurity awareness 3) the role that gender plays in Thai user’s cybersecurity awareness and 4) how different age groups are affected by...
cybersecurity awareness. Thus, in order to clarify these issues, the main research questions (RQs) of this study were as follows:

RQ1: Is cybersecurity awareness the same or different before and after the knowledge transfer process?
RQ2: Is cybersecurity awareness the same or different for male and female employees before and after the knowledge transfer process?
RQ3: Is cybersecurity awareness the same or different for different age groups?

This article is a modified and extended version of an article by Chatchalermpun et al. (2020). Additionally, in this work several issues have received considerably more attention than in the previous version, for example, additional background information and an extended literature review, as well as more information about knowledge transfer processes and cyber-attack simulations and an analysis of the data using statistical tests. The article structure is as follows: firstly, background information on phishing and cybersecurity awareness, secondly cybersecurity plans and previous research works are described, thirdly, the methods used in phishing attack simulations and knowledge transfer is explained, fourthly, the results and, fifthly, the analysis. A discussion follows in Sect. 6, before the conclusion is presented in Sect. 7, which includes the limitations of the study.

2 Background

2.1 Phishing

Phishing is used by an attacker to obtain sensitive information from the victims (Iuga et al., 2016). This kind of cyber-attack or threat intends to deceive victims to obtain sensitive and important information from them, such as, usernames, passwords and financial information, in order to steal victims’ money or to install malware on the victims’ devices (Bahnsen et al., 2017; Chaudhry et al., 2016; Peng et al., 2018). These attacks are related to sending some content or messages via email with an URL, which presents itself as a legitimate website that is actually controlled by the attacker (Fig. 1). In addition, phishing attacks are defined as criminal activities utilizing both technological techniques and social engineering techniques (Aleroud & Zhou, 2017; Bahnsen et al., 2017; Peng et al., 2018). Although phishing may be easy to avoid, advances in the phishing community are making phishing scams more difficult to identify from the victims’ point of view (Vayansky & Kumar, 2018). For example, spear phishing, which is sending a fake email or message to a specific group of users, rather than spamming users randomly. Spear phishing is usually performed by the attacker who studies potential victims and their settings before sending a message or an email appearing to be from a legitimate source or organization that the user is familiar with.
The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) defined the meaning of the term cybersecurity as ‘…the collection of things, consisting of security concepts, policies, tools, guidelines, security safeguards, actions, risk management methods, training, technologies, assurance and best practices, which can be applied to protect users’ assets and the organization and cyber environment’ (ITU-T, 2008). Those assets include networked devices, services, infrastructure, personnel, telecommunications systems, applications, and all of transmitted and/or stored information within the cyber environment, in order to secure the organization and users’ assets based on three main objectives consisting of availability, integrity, and confidentiality (ITU-T, 2008). Therefore, it can be stated that cybersecurity is a crucial factor in this era and has become a critical in this age of digital transformation (Ahmed et al., 2019; Ricci et al., 2019). It is the protection of security and privacy against cyber-attacks due to security risks and vulnerabilities. Furthermore, it becomes a distinctive and active research area that also focuses on defense mechanisms and devising solutions against the threats impacting information systems, networks and applications (Furfaro et al., 2020).

2.2 Cybersecurity, Awareness and Plan

The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) defined the meaning of the term cybersecurity as ‘…the collection of things, consisting of security concepts, policies, tools, guidelines, security safeguards, actions, risk management methods, training, technologies, assurance and best practices, which can be applied to protect users’ assets and the organization and cyber environment’ (ITU-T, 2008). Those assets include networked devices, services, infrastructure, personnel, telecommunications systems, applications, and all of transmitted and/or stored information within the cyber environment, in order to secure the organization and users’ assets based on three main objectives consisting of availability, integrity, and confidentiality (ITU-T, 2008). Therefore, it can be stated that cybersecurity is a crucial factor in this era and has become a critical in this age of digital transformation (Ahmed et al., 2019; Ricci et al., 2019). It is the protection of security and privacy against cyber-attacks due to security risks and vulnerabilities. Furthermore, it becomes a distinctive and active research area that also focuses on defense mechanisms and devising solutions against the threats impacting information systems, networks and applications (Furfaro et al., 2020).

The term awareness is important for cybersecurity. It has been described as a part of the Continuous Monitoring strategy of Information Security (ISCM) provided by the US National Institute of Standards and Technology (NIST) (Jagatic et al., 2007). It is concerned with the raising of cybersecurity awareness in an organization (Nachin et al., 2019; NIST, 2011). As mentioned, cybersecurity awareness is not only providing training programs for users or employees, but it also increases the awareness of users or employees in an organization to understand cybersecurity and to learn how to respond to cyberthreats or cyber-attacks properly. Therefore,
providing cybersecurity awareness is a very important factor in training users or employees in an organization to prepare appropriate responses.

Furthermore, as related in (Information Systems Audit & Control Association, 2019) as a part of the Control Objectives for Information and Related Technologies (COBIT) framework, in order to handle cybersecurity risks, information security and privacy risk treatment plans must be defined and managed appropriately. These plans must describe the way to manage information security risks and align with the strategy and architecture of each organization. Also, a plan must ensure that recommendations for implementing cybersecurity improvement are based on business cases, operations, services, and the development of solutions. A plan should cover security risk scenario simulations, cybersecurity exercises or drills, and cybersecurity awareness training. For a plan to enhance the cybersecurity awareness of employees in an organization, it should be used as a part of the organization’s program for cybersecurity awareness. Such a customized program may be utilized as a medium to educate and/or train and improve awareness among employees or users in each organization to protect themselves and their organizations from cyber-attacks (Daengsi et al., 2021).

Related Factors in Cybersecurity Awareness.

There are several factors that come into play in cybersecurity awareness, including human factors. These factors include age, gender, education, university qualifications and IT experience (Bordonaba-Juste et al., 2020; Jeong et al., 2019; Li et al., 2020). However, only gender and age are being considered and analyzed in this article because these are the basic factors that several previous research studies have considered in models with a correlation between these two factors and cybersecurity behaviors, cybersecurity awareness or related issues (Farooq et al., 2015; Fatokun et al., 2019; Jeong et al., 2019; Li et al., 2020; Verkijika, 2019) (Fig. 2).

As mentioned in Bordonaba-Juste et al., (2020), age is a key factor that accounts for differences in human behavior in digital culture and online content consumption. People who have had similar experiences and have lived at the same period of time will express similar values, beliefs and attitudes, and these account for the differences in other generations. In Fig. 3, one can see that four generation classifications are mentioned, consisting of Generation Z (Gen Z) or Millennials, Generation Y (Gen Y), Generation X (Gen X) and Baby Boomers (BB) (Bordonaba-Juste et al., 2020). Age can be also defined as a crucial factor when differentiating between individuals because people at different stages of life experience distinct and diverse social, organizational and environmental challenges and contexts (Jeong et al., 2019). According to previous research studies (Li et al., 2020; Sarno et al., 2019), younger people are more likely to become victims of phishing (or other cyber-attacks) than older people. However, there were a few studies that showed inconsistent results (Baillon et al., 2019; Gavett et al., 2017). For example, it has been mentioned in (Gavett et al., 2017) that both younger and older adults were suspicious about phishing attacks in approximately equal numbers.

With regard to gender, several previous research studies have concluded that differences in gender cause different perceptions of technology. Several prior works have reported that females were believed to be at risk of cyber-attacks (e.g., Jagatic et al., 2007; Sheng et al., 2010). Sheng et al. (2010) reported that females were
significantly more likely to become victims of phishing than males. However, this result is inconsistent with the study of McGill and Thompson (2018). Their results reveal that females show significantly lower overall levels of security risk behavior than males.

The human factors mentioned above play a role in cybersecurity awareness and behaviors, including prior training and working experiences, but non-human factors are relevant as well. The content of the phishing email is also an important factor.
This issue was reported in (Furnell, 2007) who stated that the address of the sender, logos and banners, the level of attention to email subject lines, email content or urgency cues, all significantly impact on eliciting a response to phishing emails.

2.3 Exercises and Drills in Cybersecurity

The term ‘drill’ is almost the same as ‘exercise’ because they relate to similar activities, particularly when associated with training sessions (Dewar, 2018). In this article, ‘exercise’ means processes to train for, assess or evaluate practice, and gain higher efficiency in a corporation. In addition, an exercise provides a good opportunity to validate plans, policies and procedures (Aoyama et al., 2017). Furthermore, exercises help to train staff or employees in their responsibilities and roles. According to NIST (2018), an exercise is a scenario-driven simulation of an emergency case or situation, which is provided to validate the effectiveness of at least one or more aspects of information technology plans. Thus, based on the meaning of the term ‘exercise’, cybersecurity exercises can be arranged or applied in several ways to strengthen or improve the potential or capability of cybersecurity. An exercise might be conducted as a public exercise or privately by hiring security specialists, so the organization can obtain the benefits from each specific simulation to enhance their organizational cybersecurity (Aoyama et al., 2017).

Cybersecurity drill, hereafter called ‘cyberdrill’, is a training process that simulates a cyber-attack on staff or employees whose work is related to cybersecurity incident response (Nachin et al., 2019). It is similar to the simulation of a security drill that is expected to be an alternative solution for preparedness for internet breach accidents or attacks which occur due to the low levels of security awareness of users (Kim et al., 2017). The Bank of Thailand, the regulator for financial services organizations (including commercial banks) in the Kingdom of Thailand, describes it as the simulation of cyber-attack scenarios with one or more forms of techniques and threats to make staff or employees more familiar with cyber-attacks (Bank of Thailand, 2019). Moreover, cyberdrills can determine if employees are vulnerable to being victims of future cyber threats. Rapid response to an incident leads the organization into a state of cybersecurity resilience that has a robust defence strategy against cyber-attacks. Besides, the response can help the corporation or organization to maintain service level agreements with internal customers and external customers. Therefore, cyberdrills can make staff or employees in a corporation or organization aware of cyber-attacks or cyber threats and provide more effective responses (NIST, 2018).

2.4 Previous Research Works

After studying previous research studies on phishing and cybersecurity awareness, it was found that there are many interesting studies (see Table 1) that provide useful information and concepts which can be applied in this research. Several of them studied students only. This means that they may be in different categories when compared with this article. However, the most relevant studies are described as follows:
Table 1 Summary of previous research works

| Reference                  | N   | Age (years)       | Participants       | Country   | Remark                        |
|----------------------------|-----|-------------------|--------------------|-----------|-------------------------------|
|                            |     |                   | Students | Employees/workers |                  |
| Kumaraguru et al. (2009)   | 515 | Main proportion = 18–25 | ✓       | ✓            | US                            |
| Iuga et al. (2016)         | 382 | > 18              | ✓       | ✓            | UK                            |
| Anwar et al. (2017)        | 579 | 18–40             | ✓       | ✓            | US                            |
| Albladi and Weir (2018)    | 27  | 25–44             | ✓       |              | UK                            |
|                            |     |                   |          |              | IS Specialists / experts      |
| Baillon et al. (2019)      | 10,929 | Mean = 47       | ✓       |              | Netherlands                  |
| Abdullah and Mohd (2019)   | 39  | N/A               | ✓       |              | Malaysia                      |
| Verkijika (2019)           | 231 | > 18              | ✓       | ✓            | Africa                        |
| Kim et al., (2019a, 2019b) | 208 | > 19              | ✓       | ✓            | US                            |
| Ikhsan and Ramli (2019)    | 305 | N/A               | ✓       |              | Indonesia                     |
| Ricci et al. (2019)        | 233 | > 18              | ✓       |              | US                            |
| Nachin et al (2019)        | 4,523 | N/A                     | ✓   |              | Thailand                      |
| Donalds and Osei-Bryson (2020) | 248 | 18–55           | ✓       |              | Jamaica                       |
| Li et al. (2020)           | 6,938 | Main proportion = 27–41 | ✓       |              | US                            |

1) Carella et al. (2017) found that document training is the most effective when compared to in-class training or no training.
2) Filippidis et al. (2018) found that master students tend to have more ISA than Bachelor level graduates.
3) Bin Othman Mustafa et al. (2019) proposed the Information Security Awareness – a knowledge-attitude-behavior (ISA-KAB) model for increasing the level of awareness based on phishing attacks and found that the awareness level in every dimension (knowledge, attitude and behavior) increased.
4) Mousa (2019) studied the students in ICT- and non—ICT related fields and found the students only had a moderate knowledge of cybersecurity, while it was found that ICT students do not have more skills than non–ICT students and that there were no differences among students’ responses depending on their gender.
5) Diaz et al. (2018) found that the students who were from different educational backgrounds responded to the same phishing email in different ways, particularly when comparing the students from the College of Natural and Mathematical Sciences with the College of Arts, Humanities, and Social Sciences.
6) Fatokun et al. (2019) found that gender, age and educational level were the most important factors in mediating students’ cybersecurity behaviors. Their findings indicate the need for specific cybersecurity training for students.

7) Peker et al. (2018) developed a module that helped to raise security awareness and then found that the module had the most effect on non-computer science majors. They also found that there was no significant difference in levels of cybersecurity awareness between female and male students.

Concentrating on previous cybersecurity awareness studies with workers or employees, there are several interesting studies that described their findings as follows:

1) Nachin et al. (2019) studied increasing cybersecurity awareness with more than 4,500 employees from 20 organizations and then found that the simulation-based delivery approach can help to improve or increase cybersecurity awareness level and is more practical than an instructor-led delivery approach. Nevertheless, both approaches should be utilized and combined.

2) Ikhsan and Ramli (2019) measured the level of information security awareness of government employees through case studies with 736 respondents in an organization in Indonesia using a behavior and knowledge approach over a questionnaire form in a phishing simulation. They found that the level of information security awareness of the staff or employees was 79.3% approximately. This score almost reached the level of ‘good’. (lower than 59% = ‘poor’, 60% to 79% = ‘average’ and 80% to 100% = ‘good’).

3) Albladi and Weir (2018) conducted their study with 30 specialists and 12 experts who responded to their survey based on social networks. They found that education, computer knowledge and security awareness were considered the high rate factors in protecting users from cyber-attacks. Also, in this study a framework for evaluating and understanding employees in organizations was proposed.

4) Abdullah and Mohd (2019) used spear phishing simulations in the telecommunication and defense sub-sector. They found that after conducting the second simulation using a different approach compared with the first one, 31% (12 users) of the same participants accessed the link in their emails. This means that changing an approach can deceive users although they have basic cybersecurity skills.

5) Ricci et al. (2019) conducted a survey with 233 subjects and found that many of them were worried about cyber threats/attacks and also about their children exploring the online domain. The majority of them were interested in learning more about cybersecurity if their employers would support the costs for cybersecurity training. However, they found that many of the subjects were only willing to participate in short sessions of cybersecurity seminars (60–90 min).

6) Li et al. (2020) presented a simulated phishing experiment targeting more than 6,900 workers at a university, focusing on demographic factors (e.g. age and gender). Their analysis of demographic factors, effects of repeated exposure to phishing exploits, and effects of phishing email content revealed significant effects...
on different age groups, on email types and marginally significant gender differences.

7) Kumaraguru et al. (2009) studied 515 subjects using a training system called PhishGuru. It was found that there was no difference between female and male subjects accepting phishing messages both before and after the cybersecurity training, while subjects in the 18 to 25 age group were typically more vulnerable to phishing attacks on all days of the study compared to the older subjects. Lastly, their survey results show that most subjects enjoyed receiving training during their normal use of email.

8) Kim et al., (2019a, 2019b) reported that the youngest group from different groups among four distinct age groups (19 to 30 years, 31 to 40 years, 41 to 65 years, and more than 65 years) tended to express the highest level of cybersecurity awareness, whereas the oldest group tended to show the lowest level of cybersecurity awareness.

9) Baillon et al. (2019) studied a very large number of employees in The Netherlands and found that the younger age group of employees (16–25 years) were least likely to visit the phishing links, whereas the employees in the age group above 46 years were about 15% more likely to access the fake link than the youngest group.

10) Anwar et al. (2017) assessed the effect of gender on the relations between psychosocial factors and self-reported cybersecurity behaviors. It was found that gender had some effects following prior experience, self-efficacy in behavioral information security and computer skills, but that it had little effect on self-reported cybersecurity behaviors and cues-to-action.

11) Donalds and Osei-Bryson (2020) studied cybersecurity compliance behavior utilizing data from 248 respondents. The results from this study confirmed that individual decision styles, specifically dominant decision styles, and dominant orientation influence an individual’s cybersecurity compliance behavior.

12) Verkijika (2019) found that not only the direct supportive influence of anti-phishing self-efficacy and anticipated regret on behavior and mobile phishing avoidance motivation but also the interaction of these factors significantly influenced avoidance behavior. Furthermore, gender moderated the influence of anti-phishing self-efficacy on individual behavior and avoidance motivation with the relationships being more pronounced for female than for male respondents.

13) Iuga et al. (2016) found that the years of computer usage and gender of the participants had a significant impact on the detection rate of phishing, pop-up based attacks had greater success than other approaches and that a psychological anchoring effect was also observed in phishing. They concluded that a careful combination of user training, automated tools and more effective cybersecurity awareness campaigns can help avoid cyber-attacks.

The above information focusing on studies with employees is summarized in Table 1. As for the number of subjects or participants, most of the studies involved hundreds of participants. Furthermore, all previous works studied westerners from the US and UK and other subjects in Asian countries, including Indonesia. Although there has been some research based on Thai employees, there is
a research gap for this study to present research work conducted with different methodologies and with a larger number of Thai employees (20,000+).

3 Research Design and Methodology

This study was designed to investigate phishing attacks for cybersecurity simulation drill tests for the employees of a large financial services organization that has hundreds of branches nationwide in the Kingdom of Thailand, and more than 20,000 employees, consisting of about 29% and 71% for males and females respectively. It has been divided into three phases, consisting of two phases of phishing attack simulations and one phase of knowledge transfer (Fig. 4), which are described as follows:

1) **Phase I:** 1st round phishing attack (Attack I) was in October 2019. The first phase of this study was conducted for cyber-risk assessment. The cybersecurity simulation drill test using a phishing attack was performed by experts from other companies. As for the drill test itself, the experts sent the first phishing emails which consisted of an offer of more Gmail storage. Then, the data from this test was gathered, processed and analyzed.

2) **Phase II:** knowledge transfer. After the first-round phishing attack simulation the knowledge transfer processes were conducted. These processes, called a mixed approach, were comprised of:

3) An email with an explanation of the first-round phishing attack simulation.

![Overview of research methodology](image.png)
4) E-learning: the employees who clicked on the link and/or filled-in the password were asked to take an e-learning course in order to improve their cybersecurity knowledge. This process included phishing awareness training, which trained employees to report as well as to spot real-world phishing emails (Carella et al., 2017).

5) Special activity: the activity for this study was a cybersecurity day that was conducted at the head office. On that day, speakers who were network security specialists, conducted seminars, workshops and demonstrations.

6) Phase III: The 2nd-round phishing attack (Attack II) was in February 2020, four months after the first phase, and the last phase was conducted again for all employees in the same organization as for the first phase. The simulation drill test using phishing emails was also the same except for the content in the phishing email which was related to a fake promotion from a popular e-commerce website/application in the Kingdom of Thailand, called “Shopee” (Shopee, 2021). Then, the data from this attack were gathered and they were processed and analyzed.

However, after finishing Attacks I and II, the data from both tests were validated by mapping the records of the employees from the Attack II on to the records of the employees from Attack I (the unmapped records were discarded). Then, the validated data gathered from 20,134 employees, including 5,855 males and 14,279 females, were analysed. The results of Attacks I and II are presented in the next section.

4 Results

One can see in Fig. 5 that the results from Attack I in Phase I, the numbers of responses for opened emails (called Scenario 1: S1), opened and clicked links (called Scenario 2: S2), and open, clicked links and filled-in passwords (called Scenario 3: S3) are 23.4%, 22.1% and 15.1%, respectively. However, after conducting the mixed approach, combining the knowledge transfer processes in Phase II and Attack II in Phase III, one can see in Fig. 1 that all responses, including opened

Fig. 5 Comparison of the overall response rates before and after knowledge transfer
emails, opened and clicked links, and opened, clicked links and filled-in passwords significantly decreased with values of 6.7%, 5.8% and 2.0%, respectively.

In addition, in this study, the gender issue was considered as well. Figure 6 shows that both before and after knowledge transfer all values of the responses from 14,279 female employees were lower than the responses from 5,855 male employees. Further details are as follows:

- 29.3% of male employees opened emails compared to 21.0.5% of female employees
- 28.2% of male employees opened emails and clicked on the links compared to 19.5% of the female employees
- 19.7% male employees clicked on the links and filled in the passwords compared to 13.2% of the female employees

In Fig. 6, one can see that after the knowledge transfer, the percentages for both male and female employees were significantly reduced, but in every case the responses from female employees were lower than those from the male employees. For example, in the case of opened emails and clicked links, the male employees showed 6.9%, whereas the female employees showed 5.4%. In the case of opened emails, clicked links and filled-in passwords, the male employees showed 2.2%, whereas the female employees showed only 2.0%. This means that 98% of the employees did not fill-in their passwords on the fake link or webpage.

![Response rate](image)

**Fig. 6** Comparison of response rates by gender before and after knowledge transfer
In addition, this study investigated the effects of age. Unlike other previous works as described in Sect. 2, the range of ages in this article was divided according to the generational cohort theory, consisting of BB, Gen X and Gen Y, who were 56–60 years, 40–55, and 24–39 years’ old in 2020 respectively, however, the employees who were 39 and 55 years’ old (for whom it could not be confirmed by the human resources department that all of them were born by the end of 1979 and 1964, respectively) were removed in order to validate the data. While the employees who were less than 24 years’ old in 2020 were considered as outliers and their data were also discarded in order to validate the data before the analysis.

Figure 7 shows the results from Phase I, where one can see that Gen Y had the highest cybersecurity awareness level overall at about 21%, 19.5% and 13.2% for S1 to S3, respectively. Moreover, focusing on male and female employees, Fig. 7 shows that the level of cybersecurity awareness was highest when Gen X is compared to BB. Gen X had the lowest level of cybersecurity awareness. Figure 8 shows the results from Attack II, after conducting the mixed approach where Gen Y had the lowest level of cybersecurity awareness when compared to Gen X and BB because BB had the highest values on the chart for all cases and both genders. This means that the knowledge transfer helped Gen X and BB to improve their cybersecurity awareness when compared to Gen Y. On the other hand, it can be stated that Gen Y showed the least improvement in cybersecurity awareness, whereas BB showed the most improvement. One can see the differences and changes by comparing Figs. 7 and 8.

![Figure 7](image)

**Fig. 7** Response rates for Attack I before knowledge transfer

---

 Springer
There are two parts in this section. The first part compares the results from Attack I with those from Attack II. The data for the analysis from the previous section, as presented in Figs. 5 and 6, have been validated again, after the records which lacked data for age and gender were discarded. Therefore, a total of 19,938 records from the participants (age 24–60 years) were analyzed, and the results of Attacks I and II were compared (note: the results from Phase II were gathered after the knowledge transfer). Table 2 shows the overall results (from the validated data related to Fig. 1) using a Chi-square test with 95% confidence interval for the hypotheses of the three scenarios, including S1, S2 and S3 as mentioned in Sect. 4 (Results). The p-values for H1-H3 are less than 0.001, where H1-H3 are the hypotheses for a comparison of the results between Attacks I and II associated with the scenarios S1-S3. There is evidence that cybersecurity awareness of the employees improved significantly.

![Fig. 8 Response rates for Attack II after knowledge transfer](image)

### Table 2 Comparison of the overall results of Attacks I and II

| Scenario | Phishing Response | Hypothesis | Chi-square | p-value | Remark |
|----------|-------------------|------------|------------|---------|--------|
| S1       | Opened            | H1         | 2087.565   | <.001*  |        |
| S2       | Opened & Clicked  | H2         | 2048.626   | <.001*  |        |
| S3       | Opened, Clicked & Filled-in password | H3         | 1966.400   | <.001*  |        |

* = Significant  
N = 18,923 records
Table 3 shows that for the gender analysis the p-values for H4-H9 or from most of the scenarios are less than 0.001, where H4-H9 are the hypotheses for a comparison of the results between male and female employees from Attacks I and II referring to the scenarios S1-S3, except for hypothesis H9, which is associated with S3 from Attack II, where the p-value is 0.462. From the results or p-values as shown in Table 3, it can be inferred that the male employees in this study were significantly more likely to become victims of phishing than the female employees, except for scenario S3, filling in the passwords, where there was no significant difference in the phishing responses.

The data from both phases were analyzed according to the age generation of the employees and the results are shown in Table 4. For Attack I, one can see that the p-values are higher than 0.05 for the hypotheses H10-H18 in every case. This means there is no significant difference between Gen Y, Gen X and BB. Similarly, the results from Attack II show that the results for the hypotheses H20-H27 in Table 5 show p-values of higher than 0.05, except for the hypothesis H19 for which the p-value is only 0.032. This means there is a significant difference among Gen Y, Gen X and BB for S1. However, similar to the results in Table 4, the age generation does not seem to be a factor in cybersecurity awareness.

Furthermore, this study also re-investigated the effects of gender on cybersecurity awareness for each generation using statistical analysis. According to Fig. 6,
it can be inferred from the validated data (from an analysis of Attack I) that there was a higher level of cybersecurity awareness in females than in males. In Table 6 it can be seen that the p-values for hypotheses H28-H36 are lower than 0.05, which means that the male employees who were untrained or did not benefit from the knowledge transfer in each generation tended to become victims of phishing significantly more than the untrained female employees in the same generation. In other words, untrained employees or users of either gender in the same generation affected their cybersecurity awareness. However, after the knowledge transfer to those employees, it was found that gender in generation BB did not play a role in cybersecurity awareness in any of the scenarios because the p-values for hypotheses H39, H42 and H45 (in Table 7) were 0.872, 0.922 and 0.638 respectively. Whereas gender in Gen Y and Gen X played a role in cybersecurity awareness in scenarios S1 and S2 (but not S3) because the p-values for hypotheses H37-H38 and H40-H41 (but not for hypothesis H43 in scenario S3) were less than 0.05 (see Table 7). This means gender in Gen Y and Gen X tended to play a role in cybersecurity awareness.

Table 5 Comparison of the results for Gen Y, Gen X and BB from Attack II

| Scenario | Phishing Response | Hypothesis | Gender | N     | Chi-square | p-value | Remark |
|----------|-------------------|------------|--------|-------|------------|---------|--------|
| S1       | Opened            | H19        | All    | 18,923| 6.563      | .038*   | S1     |
|          |                   | H20        | M      | 5,515 | 5.343      | .069    | Insignificant |
|          |                   | H21        | F      | 13,408| 4.028      | .133    | Insignificant |
| S2       | Opened & Clicked  | H22        | All    | 18,923| 4.137      | .126    | Insignificant |
|          |                   | H23        | M      | 5,515 | 3.523      | .172    | Insignificant |
|          |                   | H24        | F      | 13,408| 2.835      | .242    | Insignificant |
| S3       | Opened, Clicked & Filled-in password | H25 | All | 18,923 | 2.850 | .241 | Insignificant |
|          |                   | H26        | M      | 5,515 | 1.054      | .590    | Insignificant |
|          |                   | H27        | F      | 13,408| 3.190      | .203    | Insignificant |

* = Significant

Table 6 Comparison of the results of Attack I for males and females from each generation

| Scenario | Phishing Response | Hypothesis | Generation | N    | Chi-square | p-value | Remark |
|----------|-------------------|------------|------------|------|------------|---------|--------|
| S1       | Opened            | H28        | Gen Y      | 11,452| 81.910     | <.001*  |        |
|          |                   | H29        | Gen X      | 5392 | 55.281     | <.001*  |        |
|          |                   | H30        | BB         | 2079 | 15.552     | <.001*  |        |
| S2       | Opened & Clicked  | H31        | Gen Y      | 11,452| 97.057     | <.001*  |        |
|          |                   | H32        | Gen X      | 5392 | 56.146     | <.001*  |        |
|          |                   | H33        | BB         | 2079 | 20.106     | <.001*  |        |
| S3       | Opened, Clicked & Filled-in password | H34 | Gen Y | 11,452 | 81.218 | <.001* |        |
|          |                   | H35        | Gen X      | 5392 | 39.65      | <.001*  |        |
|          |                   | H36        | BB         | 2079 | 8.167      | .004*   |        |

* = Significant
After conducting the study and analysis, there are several issues to be discussed in this section, which are as follows:

1) Unlike all previous research works as presented in Table 1 in Sect. 2, in which the data was obtained from about 30–11,000 participants, this work studied data obtained from more than 20,000 Thai employees nationwide in a financial services company in the Kingdom of Thailand. This study was conducted on a very large scale to study a phishing attack on Thai users.

2) From the results of the first phase as shown in Fig. 5, one can see that before obtaining the knowledge transfer associated with cybersecurity, the employees had a low level of cybersecurity awareness because more than 22% of the employees became victims of the phishing email by clicking on the malicious link provided in the phishing attack simulation. This is a higher number than the results of 12% and 20% as reported in Cranor (2018) and Chen et al. (2018), respectively.

3) After conducting the knowledge transfer processes using the mixed approach, it was found that the overall level of cybersecurity awareness of the employees for phishing improved significantly. The number of employees who opened and clicked links (S2) decreased from about 22% to only about 6%. According to Ikh-san and Ramli (2019), who stated that the cybersecurity awareness level for phishing of the employees improved from about 100%-22% = 78%, when ‘averaged’, to 100%-6% = 94% is ‘very good’. Note: 80% to 100% = ‘good’ in Filippidis et al. (2018) but 80% to 89% and 90% to 100% have been modified and categorized as ‘good’ and ‘very good’ respectively. The approach with utilizing cybersecurity awareness enhancement as presented in this study is useful for cybersecurity improvement not only in organizations within the financial services sector but also in other organizations in other sectors.

4) According to a comparison of the results presented in Figs. 5 and 6 which were obtained by using a statistical analysis technique called Chi-square, it was found that the cybersecurity awareness level of the employees improved significantly...
with p-values of <0.001. This means that the hypothesis test results answer RQ1 in Sect. 1 (RQ1: Is cybersecurity awareness the same or different before and after the knowledge transfer process?) However, the high level of cybersecurity awareness might be due to the effects of different content in the phishing emails used in the second attack simulation which might have impacted positively on the phishing simulation results of the post—knowledge transfer.

5) With regard to gender, it was found from this study that Thai females have a higher level of cybersecurity awareness of phishing than Thai males, particularly the Thai women in Gen Y and Gen X. However, the different proportions of females (71%) and males (29%) in this study might have affected the gender analysis. One can see that the results from the gender analysis in Table 3 show p-values of 0.001 or lower for 5 of the 6 hypotheses. Of course, these results answer RQ2 in Sect. 1 (RQ2: Is cybersecurity awareness the same or different for male and female employees before and after the knowledge transfer?). Furthermore, it is possible that these results might be due to the nature of Thai women who are naturally cautious and careful if anything is suspicious. Therefore, this issue should be investigated further in a future work, while a comparison between Thai females and the females from other countries would be interesting.

6) Based on the age generation of the Thai employees as analyzed in the previous section, it was found that untrained employees in Gen Y had a higher level of cybersecurity awareness of phishing compared to Gen X and BB, whereas the untrained workers in Gen X had a lower level of cybersecurity awareness. However, after the knowledge transfer from online training, it was found that the trained employees from generation BB had a higher level of phishing awareness compared to Gen Y and Gen X, whereas the trained workers in Gen Y had a lower level of cybersecurity awareness in this study. Nevertheless, after the analysis using Chi-square, it was found that there were no significant differences between Gen Y, Gen X and BB overall (the p-values were higher than 0.05), even though the results from Attack I tended to result in more differences than the results from Attack II. Therefore, it can be stated in this article that the age generation of Thai employees, consisting of Gen Y, Gen X and BB, did not play a role in their cybersecurity awareness. Thus, the results based on age generation answer RQ3 in Sect. 1 (RQ3: Is cybersecurity awareness the same or different for different age groups?). However, this issue may be further studied in-depth to investigate other industries in the future.

7 Conclusion

This research used phishing attack simulations with a very large number of employees (20,134 employees, compared to previous works) within a large financial service organization in the Kingdom of Thailand. A spear phishing attack was simulated on 5,885 male and 14,279 female employees, and the results from the first-round phishing simulation were that 23.4% of the employees opened the malicious emails, while 22.1% of them did not only open the email, but also clicked on the link which means they had a low awareness of cybersecurity. However, after providing a mixed
approach, which was based on knowledge transfer developed from the guidelines related cybersecurity frameworks, it was found that the cybersecurity awareness of the employees improved significantly because after the intervention 94% of them did not click on the link in the phishing email and 98% of the employees did not fill in the passwords on the phishing webpage. This means that the cybersecurity awareness of the Thai employees in this organization was ‘very good’ (90% to 100%). Therefore, the concept of a cyber-attack simulation and knowledge transfer as described in this study is highly recommended for use in other organizations, and in other countries as well, to enhance the cybersecurity awareness level of employees in order to prevent damage from cyber-attacks. Furthermore, this research found that gender plays a role in cybersecurity awareness, as the Thai female employees in the financial services company in this study had a higher level of cybersecurity awareness than the male employees. In addition, the results showed that the age generation of the Thai users impact on their cybersecurity awareness.

8 Limitations of the Study

This study was conducted on phishing attacks on Thai employees in the financial services sector in Thailand only. It did not cover other kind of attacks or threats, other industries or sectors, or other groups of users, including students, retired people and employees in other countries. Therefore, those issues should be studied further in-depth in the future. Also, the issues of gender and age generation as considered in this study need to be further investigated in the future with other groups of subjects in other industries or other countries, while other human factors, including education, university qualifications and IT experience have yet to be investigated with Thai employees or users. Furthermore, behavior related to computer and Internet usage as well as cultural issues should also be considered in future research work, since the effects in different cultures may vary.

Acknowledgements We are grateful to Rajamangala University of Technology Phra Nakhon, Rajamangala University of Technology Rattanakosin (Wang Klai Kangwon Campus) and King Mongkut’s University of Technology North Bangkok for supporting this research. Not least of all, thanks to all participants and the source of the data set.

Declarations

Conflict of Interest None.

References

Abdullah, A. S., & Mohd, M. (2019). Spear Phishing Simulation in Critical Sector: Telecommunication and Defense Sub-sector. 2019 International Conference on Cybersecurity, ICoCSec 2019, 26–31. https://doi.org/10.1109/ICoCSec47621.2019.8970803

Ahmed, N., Islam, M. R., Kulsum, U., Islam, M. R., Haque, M. E., & Rahman, M. S. (2019). Demographic factors of cybersecurity awareness in Bangladesh. 2019 5th International Conference on
Advances in Electrical Engineering, ICAEE 2019, June 2018, 685–690. https://doi.org/10.1109/ICAEE48663.2019.8975603

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. Human-Centric Computing and Information Sciences, 8(1), 1–24. https://doi.org/10.1186/s13673-018-0128-7

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. Computers and Security, 68, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

Anstett, A. (2021). What is spear phishing?. Wandera, Retrieved Jul 27, 2021, from https://www.wandera.com/what-is-spear-phishing/

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees’ cybersecurity behaviors. Computers in Human Behavior, 69, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Aoyama, T., Nakano, T., Koshijima, I., Hashimoto, Y., & Watanabe, K. (2017). On the complexity of phishing URLs using recurrent neural networks. ECrime Researchers Summit, 1–8. https://doi.org/10.1109/ECRIME.2017.7945048

Baillon, A., De Bruin, J., Emirmahmutoglu, A., Van De Veer, E., & Van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. PLoS ONE, 14(12), 1–15. https://doi.org/10.1371/journal.pone.0224216

Bin Othman Mustafa, M. S., Nomani Kabir, M., Ernawan, F., & Jing, W. (2019). An Enhanced Model for Increasing Awareness of Vocational Students Against Phishing Attacks. 2019 IEEE International Conference on Automatic Control and Intelligent Systems, I2CACIS 2019 - Proceedings, June, 10–14. https://doi.org/10.1109/I2CACIS.2019.8825070

Bahnsen, A. C., Bohorquez, E. C., Villegas, S., Vargas, J., & Gonzalez, F. A. (2017). Classifying phishing environments, techniques, and countermeasures: A survey. Computers and Security, 68, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

Baillon, A., De Bruin, J., Emirmahmutoglu, A., Van De Veer, E., & Van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. PLoS ONE, 14(12), 1–15. https://doi.org/10.1371/journal.pone.0224216

Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. Proceedings - 2017 IEEE International Conference on Big Data, Big Data 2017, 2018-January, 4458–4466. https://doi.org/10.1109/BigData.2017.8258485

Chatchalermpun, S., Wuttiditachotti, P., & Daengsi, T. (2020). Cybersecurity Drill Test Using Phishing Attack: A Pilot Study of a Large Financial Services Firm in Thailand. ISCAIE 2020 - IEEE 10th Symposium on Computer Applications and Industrial Electronics, 283–286. https://doi.org/10.1109/ISCAIE47305.2020.9108832

Chaudhry, A J, Chaudhry, A S & Rittenhouse, G R. (2016). Phishing Attacks and Defenses. International Journal of Security and Its Applications, 10(1), 247–256. http://article.nadiapub.com/IJSIA/vol10_no1/23.pdf

Chen, Y., YeckehZaare, I., & Zhang, A. F. (2018). Real or bogus: Predicting susceptibility to phishing with economic experiments. PLoS ONE, 13(6), 1–18. https://doi.org/10.1371/journal.pone.0198213

Cloudflare. (2020). What is a Phishing attack?. Cloudflare, Retrieved Jul 27, 2021, from https://www.cloudflare.com/learning/access-management/phishing-attack/

Cranor, L. (2018). 25 Security awareness training and phishing prevention. Carnegie Mellon University, Retrieved Jul 27, 2021, from https://canvas.cmu.edu/files/965667/download?download_frd=1

Daengsi, T., Wuttiditachotti, P., Pornpongtechanavich, P., & Utakrit, N. (2021). A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization. 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 102–106, doi: https://doi.org/10.1109/ICSCEE50312.2021.9498208

Dewan, R. S. (2018). Cybersecurity and Cyberdefense Exercises. ETH Library, Retrieved Oct 7, 2021, from https://doi.org/10.3929/ethz-b-000314593

Diaz, A., Sherman, A. T., & Joshi, A. (2018). Phishing in an academic community: A study of user susceptibility and behavior. ArXiv. https://doi.org/10.1080/01611194.2019.1623343

Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. International Journal of Information Management, 51, 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

Cloudflare. (2020). Retrieved Jul 27, 2021, from https://www.cloudflare.com/learning/access-management/phishing-attack/
Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information security awareness in educational institution: An analysis of students’ individual factors. *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, 1, 352–359. https://doi.org/10.1109/Trustcom.2015.394

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series*, 1339(1). https://doi.org/10.1088/1742-6596/1339/1/012098

Filippidis, A. P., Hilas, C. S., Filippidis, G., & Politis, A. (2018). Information security awareness of Greek higher education students - Preliminary findings. *2018 7th International Conference on Modern Circuits and Systems Technologies, MOCAST 2018*, 1–4. https://doi.org/10.1109/MOCAST.2018.8376578

Furfaro, A., Pace, P., & Parise, A. (2020). Facing DDoS bandwidth flooding attacks. *Simulation Modelling Practice and Theory*, 98(June 2019), 101984. https://doi.org/10.1016/j.simpat.2019.101984

Furnell, S. (2007). Phishing: Can we spot the signs? *Computer Fraud & Security*, 3, 10–15. https://doi.org/10.1016/S1361-3723(07)70035-0

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLoS ONE*, 12(2), 1–16. https://doi.org/10.1371/journal.pone.0171620

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z

Ikhsan, M. G., & Ramli, K. (2019). Measuring the Information Security Awareness Level of Government Employees Through Phishing Assessment. *34th International Technical Conference on Circuits, Systems, Computers and Communications, ITC-CSCC 2019*, 4–7. https://doi.org/10.1109/ITC-CSCC.2019.8793292

Information Systems Audit and Control Association. (2019). *COBIT 2019 Framework: Governance and Management Objectives*, ISACA, Retrieved Jul 27, 2021, from https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19fgm

ITU-T. (2008). X.1205: Overview of cybersecurity. ITU-T, Retrieved Jul 27, 2021, from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-Centric Computing and Information Sciences*, 6(1). https://doi.org/10.1186/s13673-016-0065-2

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94–100. https://doi.org/10.1145/1290958.1290968

Jeong, J., Mihelic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. *Proceedings - 2019 IEEE 5th International Conference on Collaboration and Internet Computing, CIC 2019*, CiC, 338–345. https://doi.org/10.1109/CIC48465.2019.00047

Kim, B. H., Kim, K. C., Hong, S. E., & Oh, S. Y. (2017). Development of cyber information security education and training system. *Multimedia Tools and Applications*, 76(4), 6051–6064. https://doi.org/10.1007/s11235-016-4395-y

Kim, E., Yoon, J. K., Kwon, J., Liaw, T., & Agogino, A. M. (2019a). From innocent irene to parental patrick: Framing user characteristics and personas to design for cybersecurity. *Proceedings of the International Conference on Engineering Design, ICED, 2019-August(August)*, 1773–1782. https://doi.org/10.1017/dsi.2019.183

Kim, H., Kwon, H. J., & Kim, K. K. (2019b). Modified cyber kill chain model for multimedia service environments. *Multimedia Tools and Applications*, 78(3), 3153–3170. https://doi.org/10.1007/s11042-018-5897-5

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of Phish : A Real-World Evaluation of Anti-Phishing Training Categories and Subject Descriptors. *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS `09*, 12.

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020). Experimental Investigation of Demographic Factors Related to Phishing Susceptibility. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2240–2249. https://doi.org/10.24251/hicss.2020.274

McGill, T., & Thompson, N. (2018). Gender differences in information security perceptions and behaviour. *ACIS 2018 - 29th Australasian Conference on Information Systems*, 1–11. https://doi.org/10.5130/acis2018.20
Nachin, N., Tangmanee, C., & Piromsopa, K. (2019). How to increase cybersecurity awareness. ISACA Journal, 2, 45–50.

NIST. (2011). Information Technology Security Training Requirements. Special Publication (SP) 800–16, USA, Retrieved Jul 27, 2021, from http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, Retrieved Jul 27, 2021, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Peker, Y. K., Ray, L., & Da Silva, S. (2018). Online cybersecurity awareness modules for college and high school students. Proceedings - 2018 National Cyber Summit Research Track, NCS 2018, 24–33. https://doi.org/10.1109/NCS.2018.00009

Peng, T., Harris, I., & Sawa, Y. (2018). Detecting Phishing Attacks Using Natural Language Processing and Machine Learning. Proceedings - 12th IEEE International Conference on Semantic Computing, ICSC 2018, 2018-Janua, 300–301. https://doi.org/10.1109/ICSC.2018.00056

Ricci, J., Breitinger, F., & Baggili, I. (2019). Survey results on adults and cybersecurity education. Education and Information Technologies, 24, 231–249. https://doi.org/10.1007/s10639-018-9765-8

Sarno, M D, Lewis, E J, Bohil, J C & Neider, B M. (2019). Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults, Human Factors. The Journal of the Human Factors and Ergonomics Society, 62(5). https://doi.org/10.1177/0018720819855570

Shaymaa Mousa. (2019). Cyber Security: Exploring Awareness among University. 5, 88–97.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? 373. https://doi.org/10.1145/1753326.1753383

Shopee. (2021). Shopee Thailand. Shopee, Retrieved Oct 24, 2021, from https://shopee.co.th/

Verizon. (2019). 2019 Verizon Data Breach Investigations Report: First impressions from the perimeter. Verizondigitalmedia, Retrieved Jul 27, 2021, from https://www.verizondigitalmedia.com/blog/2019-verizon-data-breach-investigations-report-first-impressions/

Vayansky, I., & Kumar, S. (2018). Phishing – challenges and solutions. Computer Fraud and Security, 2018(1), 15–20. https://doi.org/10.1016/S1361-3723(18)30007-1

Verkijika, S. F. (2019). “If you know what to do, will you take action to avoid mobile phishing attacks”: Self-efficacy, anticipated regret, and gender. Computers in Human Behavior, 101(January), 286–296. https://doi.org/10.1016/j.chb.2019.07.034

Wei, W., Ke, Q., Nowak, J., Korytkowski, M., Scherer, R., & Woźniak, M. (2020). Accurate and fast URL phishing detector: A convolutional neural network approach. Computer Networks, 178(April). https://doi.org/10.1016/j.comnet.2020.107275

Yeom, S., Shin, D., & Shin, D. (2020). Scenario-based cyber attack-defense education system on virtual machines integrated by web technologies for protection of multimedia contents in a network. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-019-08583-0

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
Authors and Affiliations

Therdpong Daengsi¹ · Phisit Pornpongtechavanich² · Pongpisit Wuttidittachotti³

Terdpong Daengsi therdpong.d@rmutp.ac.th
Phisit Pornpongtechavanich phisit.kha@rmutr.ac.th

¹ Department of Sustainable Industrial Management Engineering, Faculty of Engineering, Rajamangala University of Technology Phra Nakhon (North Bangkok Center), Bangkok, Thailand

² Department of Information Technology, Faculty of Industry and Technology, Rajamangala University of Technology Rattanakosin (Wang Klai Kangwon Campus), Hua Hin, Prachuap Khiri Khan, Thailand

³ Department of Data Communication and Networking, Faculty of Information Technology and Digital Innovation, King Mongkut’s University of Technology North Bangkok, Bangkok, Thailand