Improving cybersecurity awareness using phishing attack simulation

Surachai Chatchalermpun¹, Therdpong Daengsi²

¹Computer Engineering Department, Southeast Asia University
²Sustainable Industrial Management Engineering Department, Rajamangala University of Technology Phra Nakhon

*therdpong.d@rmutp.ac.th

Abstract. This paper aims to present a case study of the cybersecurity awareness level of the workers in a financial institution in Thailand. In this study, there were 2 phases of cyber drills using a spear-phishing email. The first phase was conducted with more than 20,300 workers. It was found that there were 23.25% of potential victims. However, the second phase was conducted four months later with more than 20,200 workers after performing knowledge transfer. The number of workers who opened phishing emails in the second phase decreased to 6.76% only. Therefore, it can be indicated that an appropriate cybersecurity knowledge transfer can reduce a large number of potential victims and cyber threats that may occur in such organizations.

1. Introduction

The Internet is now everywhere, therefore, people can connect it via Wi-Fi and mobile devices that support 4G/5G technology easily. They use the Internet to access web services for various purposes and come in many activities easily, including e-commerce and Internet banking [1]. It could be used widely not only through web services but also applications and software. If users apply knowledge and skills about applications and software development in a creative way, it is really useful for others. In contrast, if some users use their knowledge and skills in a wrong way, it will become cybersecurity issues that aim to attack people to steal, eliminate, breach, and deceive the data to gain a financial advantage or other benefits, including taking advantage of organizations or deceptive business practices.

One of the serious cybersecurity threats is phishing that the attackers mainly try to steal the credentials of other people using disguised emails and/or fake websites [1]. The impacts of phishing attacks might vary from a loss of money to the compromising of whole entities, where workers or users have not paid attention enough and provided credentials to access organizational information systems. Symantec described that the global average rate of email phishing was 1 in 3,200 emails approximately in 2018, meanwhile, it was 1 in 1,380 emails approximately in Thailand [3]. In the same year, it also found that email phishing and associated email occupied about a fifth of total security incidents in the United States [4]. In Q3/2018, Kaspersky Lab reported that more than 137 million cases related to phishing websites were found [5], and more than 30% of all the phishing attacks targeted to the financial services such as payments systems and e-commerce [6].
Therefore, the objective of this study is to examine the level of cybersecurity awareness for the workers in a large Thai financial institution based on cyber drills by using phishing techniques, before providing appropriate training to prevent the cyber risks that may occur in the organization.

2. Background

2.1 Phishing
Phishing is one of the most common attacks (mostly via email), but it is dangerous [1]. The overview of the phishing attack is shown in Figure 1 [7]. However, attackers are using more complicated attacks to increase the success rate in breaching IT systems’ security at present and stealing data. They make a major change from normal phishing attacks to spear-phishing attacks that lead to effects for victims seriously, to break through antispam mechanisms and detection techniques [8].

For spear phishing, it is a targeted or special attack. It can be directed towards targeted groups of users or specific users with the same criteria, or organizations. The content inside the phishing email is well customized for targeted users, groups of users, or organizations as opposed to spam mails and bulk phishing [8]. Unlike normal phishing, the attackers gather information and study about potential victims to allow them a chance of sending convincing content emails to the victims [9].

2.2 Cyber Drill
Cyber drill or cybersecurity drill is a process that simulates a cyber-attack on workers in the organization whose task is related to incident response [10]. It has been defined as the simulation of cyber-attack scenarios with a selected technique and threat to make workers more familiar with those attacks [11]. A cyber drill can find out if workers become potential victims of cyber-attacks or not. Rapid incident response helps to lead the organization to a cybersecurity resilience state, which is very vigorous against the consequences of cyber-attacks. Therefore, the cyber drill can improve workers to be aware of cybersecurity threats and also provide higher efficient responses [10].

2.3 Related Research Works
Abdullah and Mohd [9] conducted two simulations with 39 participants in 2018. It was found from the first simulation that all of them did not respond to the phishing emails because they were able to identify every indicator on each phishing email. However, after conducting the second simulation with a different approach, 12 participants responded to the phishing email by accessing the link in the email.

![Figure 1. Overview on phishing](image-url)
Ikhsan and Ramli [12] measured the level of information security awareness (ISA) of workers. Mainly, they conducted measuring through case studies in a government organization in Indonesia using phishing attack simulation. From this study, it was determined that the ISA level of those workers was 79.32%. Carella et al. [13] studied the consequence of security awareness training on users who access malicious links in phishing emails. The three security training approaches consist of document training, in-class training, and no training. They found that document training is the most effective rather than another two approaches.

Mustafa et al. [14] studied the general awareness level and analyzed before providing the education treatment based on the enhanced KAB model. Then enhancing awareness level of information security study was conducted. Also, it was found that the awareness level is increased. Besides, it was stated in [15-16] and could be inferred that 30 in 100 of phishing emails were opened by the users. Consequently, 12 in 100 of those users accessed the fake website or the malicious attachment.

3. Methodology

3.1 Cyber Drill: Phase I
In the first phase, the phishing simulation was conducted using phishing emails in early Q4/2019, while the content in the email was about Gmail storage. It was distributed to more than 20,000 workers, in a large financial institution in Thailand. After data gathering from the same raw data set as in [17], the result from the first simulation can be obtained and shown in the next Section IV.

3.2 Knowledge Transfer
The knowledge transfer was conducted as follows:
   a. Email with the details about Phase I - cyber drill: all workers were sent an email that explained the details about Phase I – cyber drill, to let them realize about the phishing simulation and to gain their security awareness.
   b. E-learning: the workers who at least opened the email and accessed the fake URL were classified as the high potential victims. They were sent the email with an e-learning lesson to learn by themselves.
   c. Security day: to awake and actuate the workers, the security day was promoted at the headquarter. On that day, there were several activities, including seminars about cyber threats and risks.

3.3 Cyber Drill: Phase II
In this phase, the phishing simulation was conducted again in Q1/2020. The content in the email was changed to the promotion from a popular e-commerce website in Thailand called ‘Shoppee’. The second phishing email with the fake promotion was sent to the same targeted users as in Phase I, although the users in this phase, not the same as in Phase I (due to staff turnover).

4. Results and Comparative Results
Since gathering and validating the data from the cyber drill - Phase I, the spear-phishing email with Gmail storage was sent to about 20,340 workers. After responding by those users, all responses were divided into 4 categories as shown in Figure 2, there was 76.75% took no action, whereas 23.25 % of users opened the email. When zoom-in at 23.25%, there were 1.32% opened the email only, 6.93% opened the email and clicked the link only, and 15% opened the email, clicked the link, and filled-in their passwords.

For Phase II that was conducted after performing the knowledge transfer, the spear-phishing email by sending Shoppee promotion about 20,260 users. After responding by those, all responses were classified as shown in Figure 3, 93.24% took no action, whereas 6.76 % of users opened the email. When zoom-in this part, it was found that there were 0.85% opened the email only, 3.85% opened the email and clicked the link only, and 2.06% opened the email, clicked the link, and filled-in their passwords.

Comparing the data from Phase II and Phase I by focusing on the part of workers who were classified as the potential victims. The percentage of responses from those users decreased by about 16.5%, by 16% for opened the email only, opened and clicked the link only; and 13% for opened the email, click the link, and filled-in password, respectively. Moreover, when calculated for the change rate, the
cybersecurity awareness improvement of the last three categories was decreased significantly as shown in Table I. It was reduced by about 71% for opened the email only, 73% for opened and clicked the link only, and 86.3% for opened the email, clicked the link, and filled-in password.

![Figure 2. Result from 20,339 users in Phase I](image1)

![Figure 3. Result from 20,259 users in Phase II](image2)

| Category                                         | Change rate (%) |
|--------------------------------------------------|-----------------|
| No Action                                        | ↑ 21.49         |
| Opened email                                     | ↓ 70.92         |
| Opened email and clicked link                     | ↓ 73.05         |
| Opened email, clicked link and filled-in password | ↓ 86.27         |

5. Discussion

There are several issues to be discussed as follows:

a. This spear-phishing study was conducted with the greatest number of users, more than 20,000 users when compared with prior works [10][12-14].
b. The cybersecurity awareness of the workers from Phase I was at the level of 77.75% that was categorized as AVERAGE following [12]. However, after the knowledge transfer processes, it was reached at 93.24% that was categorized as GOOD.

c. In Phase I, it has been found that the portion of opened email category (23.25%) is lower than 30% as mentioned in [15-16], whereas the number of workers (about 22%) who opened the email and clicked the fake link is greater than the number of 12% as stated in [15-16].

d. From Phase II, it has been found that the number of opened email category (6.76%) is significantly lower than 30%, whereas the number of users (only about 5.9%) who opened the email and clicked the disguised link is significantly lower than 12% as mentioned in [15-16].

e. From the results, the cybersecurity awareness level of the users has been improved significantly. Since all categories as in Table 1 were improved with the change rate of 71-86%. However, the improvement might be from the changed content in the second phishing.

6. Conclusion
This study has proven that cyber drills and cybersecurity knowledge transfer could improve the level of cybersecurity awareness in the financial institution, a targeted sector for attackers. Thus, with a high level of awareness across all workers, this can help to reduce risks or threats, as well as it is more likely that a potential victim will report a suspected instance and the appropriate incident response will be triggered in time to mitigate damage.

Acknowledgement
Thank you to Southeast Asia University and Rajamangala University of Technology Phra Nakhon for supporting. Finally, thank you Mr.Artid Srirngam for English editing.

References
[1] A. A. Zuraiq and M. Alkasassbeh, "Review: Phishing Detection Approaches," Proc. ICTCS 2019, pp. 1-6, 2019.
[2] J. A. Chaudhry, S. A. Chaudhry, and R. G. Rittenhouse, “Phishing Attacks and Defenses,” Int. J. Secur. Appl., vol. 10, no. 1, pp. 247-256, 2016.
[3] Symantec, “ISTR Internet Security Threat Report,” Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.
[4] J. Slye, “End-User Cybersecurity Violations Continue to Plague Federal Agencies,” Available: https://iq.govwin.com/neo/marketAnalysis/view/End-User-Cybersecurity-Violations-Continue-to-Plague-Federal-Agencies/3716?researchTypeId=1.
[5] Kaspersky, “Spam and phishing in Q3 2019.” Available: https://securelist.com/spam-report-q3-2019/95177/.
[6] Kaspersky, “The number of phishing attacks rose by 27.5% to reach over 137 million in Q3 2018,” Available: https://www.kaspersky.com/about/press-releases/2018_number-of-phishing-attacks-rise-in-q3
[7] Cloudflare, “What is a Phishing attack?,” 2020. Available: https://www.cloudflare.com/learning/access-management/phishing-attack/
[8] V. Shakela and H. Jazri, "Assessment of Spear Phishing User Experience and Awareness: An Evaluation Framework Model of Spear Phishing Exposure Level (SPEL) in the Namibian Financial Industry," Proc. icABCD 2019, pp. 1-5, 2019.
[9] A. S. Abdullah and M. Mohd, "Spear Phishing Simulation in Critical Sector: Telecommunication and Defense Sub-sector," Proc. ICoSec 2019, pp. 26-31, 2019.
[10] N. Nachin, C. Tangmanee, and K. Piromsopa, “How to Increase Cybersecurity Awareness” ISACA J., vol.2, pp. 45-50, 2019.
[11] BOT, “Cyber Resilience Readiness Assessment Framework,” Available: https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/FSINotifications/Cyber%20resilience%20framework%202019.pdf. (In Thai).
[12] M. G. Ikhsan and K. Ramli, "Measuring the Information Security Awareness Level of Government Employees Through Phishing Assessment," *Proc. ITC-CSCC 2019*, pp. 1-4, 2019.

[13] A. Carella, M. Kotsoev and T. M. Truta, "Impact of security awareness training on phishing click-through rates," *Proc. Big Data 2017*, pp. 4458-4466, 2017.

[14] M. S. bin Othman Mustafa, M. N. Kabir, F. Ernawan and W. Jing, "An Enhanced Model for Increasing Awareness of Vocational Students Against Phishing Attacks," *Proc. I2CACIS 2019*, pp. 10-14, 2019.

[15] A. Anstett, “What is spear phishing?,” Available: https://www.wandera.com/what-is-spear-phishing/.

[16] L. Cranor, “25 Security awareness training and phishing prevention,” Available: https://canvas.cmu.edu/files/965667/download?download_frd=1.

[17] S. Chatchalermpun, P. Wuttidittachotti, T. Daengsi, “Cybersecurity Drill Test Using Phishing Attack: A Pilot Study of a Large Financial Services Firm in Thailand,” *Proc. ISCAIE 2020*, pp. 283-286, 2020.