Comparative Phishing Attack Simulations: A Case Study of Critical Information Infrastructure Organization Using Two Different Contents

Patsita Sirawongphatsara
Computer Science
RMUTTO
Chonburi, Thailand
patsita_si@rmutto.ac.th

Soawanee Prachayagringkai
Computer Science
DRU
Bangkok, Thailand
soawanee.p@dru.ac.th

Phisit Pornpongtechavanich
Information Technology
RMUTR
Prachuap Khiri Khan, Thailand
phisit.kha@rmutr.ac.th

Tipmanee Rompun
Sustainable Industrial Management Engineering
RMUTP
Bangkok, Thailand
tipmanee-r@rmutp.ac.th

Kamolrak Chaowmak
Information Technology
Samutprakan Technical College
Samutprakan, Thailand
kamolrakc@sptc.ac.th

Nattapong Phanthuna
Electrical Engineering
RMUTP
Bangkok, Thailand
nattapong.p@rmutp.ac.th

Therdpong Daengsi
Sustainable Industrial Management Engineering
RMUTP
Bangkok, Thailand
therdpong.d@rmutp.ac.th

2023 10th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) | 979-8-3503-0686-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/EECSI59885.2023.10295679

***Abstract*— Nowadays, cybersecurity is an important issue at the personal and organizational levels. Therefore, cybersecurity simulation should be conducted in organizations that are considered critical information infrastructure. According to the simulated phishing attack, during the initial attempt, an email offering a fake promotion from a well-known IT equipment store was sent to employees of a railway company in Thailand. The results indicated that out of around 700 employees who received these phishing emails, 9.5% fell for the trap. This demonstrated a higher level of awareness about cyber threats compared to the average rate of 12%. However, the training was performed for the employees who fell into the trap of the first attack. Then, a simulated phishing email attack was executed for the second time by sending an email, notifying the employees to change their passwords, from a fake IT administrator. The results revealed that 8.0% of the employees who do not fall in the first attack were deceived, while there was 1.4% of the employees who fell into both attacks with different contents. Therefore, this study shows that different contents can impact different awareness of users or employees. Thus, it suggests that the process of knowledge transfer based on cybersecurity awareness is very important still.**

Keywords- Cyberdrill; CSA; CII; fake website; victim

I. INTRODUCTION

Recently, the National Cyber Security Agency of Thailand (NCSA) which was established in 2019 to address cybersecurity-related issues has announced the cybersecurity act, which focuses on cybersecurity policy and action plans [1-2]. According to section 49 of the cybersecurity act [1], the NCSA has the authority to establish general cybersecurity policies and action plans. This board also has the right to set minimum standards for computer and related systems used in government agencies and Critical Information Infrastructure (CII) entities in several services, including national security, banking and finance, and transportation and logistics [3].

For transportation and logistics, every company operating transportation services, including railway transportation and air transportation must comply with the Cybersecurity Act and manage policies and action plans associated with cybersecurity issues. Furthermore, all companies defined or classified as CII organizations must enhance their employees' cybersecurity knowledge to avoid potential out-of-service situations. Such incidents could have a significant impact on people who rely on electric trains for transportation.

To comply with the cybersecurity act, one of the electric train companies operating in Bangkok and metropolitan areas conducted a small project with the main objective of enhancing their employees' cybersecurity awareness. This project was a collaborative effort between the train company and an academic institution. As a result of the project, several interesting cybersecurity issues were identified. It is essential to present and share these issues with similar organizations classified as CII organizations or other companies interested in improving their employees' cybersecurity awareness. Moreover, these issues can serve as valuable examples or case studies for academics in the field.

II. BACKGROUND

A. Overview of Cybersecurity Awareness

It denotes cybersecurity awareness (CSA) or information security awareness (ISA) is the knowledge of cybersecurity and the appropriate response to cyber threats or cyberattacks [4]. Therefore, it is crucial to provide users and employees with CSA training. The plan to improve employee cybersecurity knowledge should be implemented in conjunction with the organization's CSA program. Users or employees in each business may be trained, educated, and made more aware of ways to defend themselves and their organizations against cyberattacks using the tailored software.

Cybersecurity awareness (CSA) is supported by three factors as follows [5]:

1) People: rationally speaking, this factor carries the highest risk of human mistakes, and human intervention is

harder to predict and more uncertain than software and its system. For the workforce to be the best defense against cyberattacks, employee training, awareness, and resources are crucial.

2) Processes: This second pillar of the three involves personnel training and the appropriate technology. Some of the processes that could be applied are auditing, frameworks, risk assessments, and the deployment of management system methodologies. Processes are only as effective as the individuals who adhere to them and the skilled employees.

3) Technology: It is essential for managing and lowering the risk of cyber threats in organizations, particularly in the public sector where records and potentially sensitive data are exchanged among many systems and people. Without access to data, organizations would be unable to run, making it even more crucial to utilize the proper software to safeguard these procedures and data access.

To minimize the effects of cyberattacks, each organization needs to integrate the factors abovementioned.

B. *Phishing*

Phishing via email is one of the cyber threats that may be communicated to users with ease. These phishing-related facts in 2022 are fascinating and can be presented as follows:

- Phishing, which affecting around 300,000 people was the most prevalent type of cybercrime reported to the United States Internet Crime Complaint Center [6].
- 44 percent of businesses reported a breach of client or customer data, down from 54 percent in 2021. 43 percent of the respondents reported frequently becoming infected with ransomware by email in 2022 [7].
- Phishing assaults primarily targeted delivery companies. Over 27% of financial phishing assaults worldwide were carried out by them. E-stores came in second with almost 16 percent of the attacks, while payment systems were third with 10.39 percent [8].

Although it is one of the most frequent attacks, this one is risky [4]. Phishing employs both technological and social engineering methods. See Fig. 1 [4], which presents the phishing attack's overall layout. To boost their chances of successfully compromising the security of IT systems and stealing data, attackers are currently employing more sophisticated methods. To get through spam filters and detection methods, they drastically alter traditional phishing attempts into spear-phishing attacks that have catastrophic consequences for victims [10]. It is a focused or unique attack for spear phishing. It may be addressed to certain individuals who meet certain requirements, targeted groups of users, or organizations. As opposed to spam emails and bulk phishing, the content inside the phishing email is properly personalized for the targeted users, groups of users, or organizations [9]. In contrast to standard phishing, the attackers research and acquire data about possible victims in order to increase the likelihood that they would be able to send the victims emails with convincing content [9].

C. *Cybersecurity Exercise and Cybersecurity Drill*

The term “exercise” in this paper refers to practices for improving performance in an organization through practice, assessment, and training. A controlled chance to validate policies, strategies, and procedures is also provided by an exercise [11]. Exercises also assist in educating staff members on their duties and responsibilities. The National Institute of Standards and Technology (NIST) described an exercise as a scenario-driven simulation of an emergency situation that is offered to test the efficacy of one or more components of IT strategies [11-12]. Thus, based on the various definitions of the term "exercise," cybersecurity exercises can be conducted in a variety of ways as a chance to build or develop the capability or potential concerning cybersecurity.

Cyberdrill is a training procedure that mimics a cyberattack on employees or individuals whose jobs involve cybersecurity incident response [13]. It is defined as the simulation of cybersecurity attack scenarios with a kind of threat and/or tactics to make users more aware of the threats [14]. Cyberdrills can also identify whether a worker is at a high risk of falling victim to cybersecurity threats. Thus, cyber drills can lead to increase employee awareness of cybersecurity issues and enable more effective responses.

D. *Previous Related Works*

Phishing, CSA, or ISA, and the factors that link to them are the subject of many intriguing publications. The following succinct summary applies to those works:

- Daengsi et al. [4] found that Thai personnel working in technology and social-based departments within the same firm, such as human resources and IT were aware of cybersecurity issues.

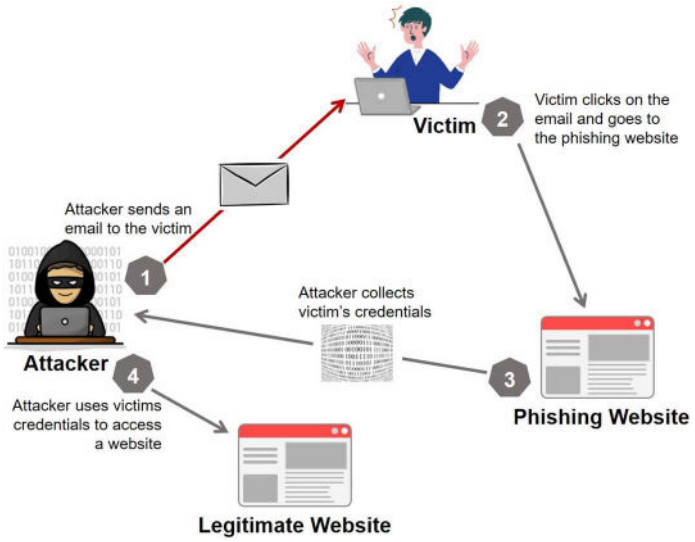

Fig. 1. Overview on phishing techniques

- Abdullah and Mohd [10] conducted research on the spear phishing simulation in organizations under the telecommunication and defense sub-sector. The results showed that all samples were not fooled by spear-phishing emails received by email, indicating that the CSA level of the population was high.
- Nachin et al. [13] mentioned that, according to research, the simulation strategy is more useful than an instructor approach for achieving CSA level in enterprises. However, it is best to mix and make use of both possibilities.
- Nur [15] performed a survey in Somalia and discovered that the banking and telecom industries are the top two targets for phishing and vishing attacks.
- Diaz et al. [16] discovered a substantial difference between the responses to the same phishing attack simulation from students in the College of Arts, Humanities, and Social Sciences and those in the College of Natural and Mathematical Sciences.
- Fatokun et al. [17] found from their research that students' cybersecurity practices are significantly influenced by their educational background, age, and gender.
- Mousa [18] discovered that Saudi Arabian IT students do not possess greater talents than non-IT pupils. Additionally, a substantial disparity between male and female students was discovered.
- Li et al. [19] revealed that there were substantial age effects, differences in email type, and significant gender effects from the study utilizing phishing attack simulation.
- Aljeaid et al. [20] discovered that the sort of attack technique influences users' perceptions and confirmed that users are susceptible to attack if they lack CSA and education.
- Chatchalermpun and Daengsi [21] found that cyber drills and information transfer helped reduce the number of employees who put in passwords in the false link from 15% to only 2%, according to their study with a large number of workers in a financial firm.
- Davis and Grant [22] studied and indicated that gamified phishing was very effective since it caught students' interest and improved their understanding.
- Sutter et al. [23] revealed over 31,000 people took part in a 12-week phishing awareness training research that included 144 different simulated phishing attempts. According to data research, 66% of users weren't the targets of phishing scams.
- Castaño et al. [24] developed a tool to detect text and phishing websites. The results showed that the developed algorithm was 92.50% accurate.

According to the review, there is no work that investigates the effects of employees' jobs in various divisions. There is therefore room to carry out a study to look into this matter.

III. Methodology

This study is a small collaborative project between a research team from Rajamangala University of Technology Phra Nakhon (RMUTP) and a railway company in Thailand. It is divided into three steps (see Fig. 2) as follows:

1) Step 1: In this step, a fake website was created. It looked like one of the well-known websites of one company that sells IT items. after creating the fake website, an email with the fake promotion and a fake link was sent to all employees within the company in May 2023. The result is shown in Section IV.

2) Step 2: For the training, the knowledge about personal data protection and organizational data protection was transferred to the employees who fell into the trap of the first phishing attack. The train was divided into two sessions. Each session took 3 hours.

3) Step 3: This round of phishing attacks was conducted in July 2023 using a different content compared to the first attack. The fake website was created and it looked like the organization's website. It was sent to all employees via email with the trick of asking employees for their passwords within three days. The result from this round is shown in Section IV.

IV. Results and Discussion

This section shows the results from two rounds of phishing attacks, as in Fig. 3 and Fig. 4.

Overall, the result from the second attack is better than the first attack. The number of employees who fell into the trap slightly decrease from 9.5% to 9.4%, while both results are lower than the general average value (12%) as mentioned in [12]. For the whole organization, it can be stated that after the knowledge transfer process, the percentage of employees who fell into the trap of phishing decreased by about 1.05% (it was from $(9.5\text{-}9.4)/9.5*100\%$).

However, after checking the emails that responded to both attacks. It was found that there are only 1.4% of the employees fell into the trap in both rounds of the attacks, meaning the knowledge transfer process can educate the employees and help them to gain more awareness. In addition, it was found that there were new employees who fell into the second attack but they did not fall into the first attack. This result can be implied that the contents of phishing emails have different potential to victimize employees.

Therefore, cybersecurity simulation and training should be conducted with different contents frequently, to improve CSA level of employees or at least to maintain their CSA. For one of the limitations of this study, the results in this paper were from only one CII organization in Thailand, it cannot be representative of other CII organizations. Thus, future work with other organizations should be performed.

Fig. 2. Overview on methodologies in this study

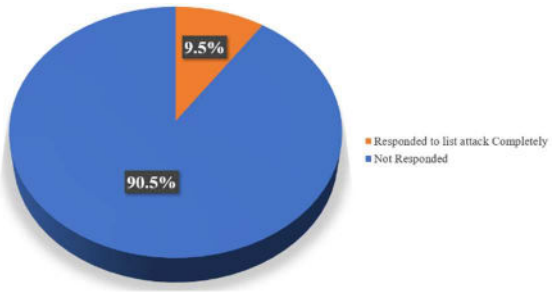

Fig. 3. The result from the first attack

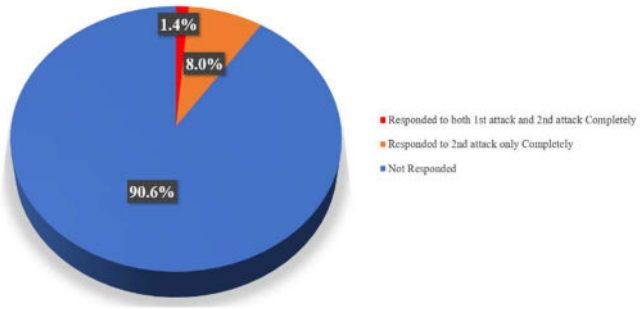

Fig. 4. The result from the second attack

V. Conclusion

In this study based on a railway company in Thailand, it was found that different content in phishing emails has impacted users or employees differently. Therefore, cybersecurity simulation and knowledge transfer should be performed continuously for the enhancement of cybersecurity awareness among employees. Therefore, the organization that is classified as CII, can be secured.

For future work, other contents should apply to the next simulations, while the methodologies presented in this study can be utilized by other CII organizations in Thailand and other countries.

Acknowledgments

Thank you to TRM Platform and Rajamangala University of Technology Phra Nakhon for supporting.

References

[1] National Cyber Security Agency, "CyberSecurity Act," NCSA, https://www.ncsa.or.th/aboutncsa.html (In Thai)

[2] National Cyber Security Commission, "Cyber Security Policy and Action Plan (2022 -2027)," MDES, https://www.mdes.go.th/law/detail/6323 (In Thai)

[3] Thaicert, "Critical Information Infrastructure: CII," Thaicert, https://www.thaicert.or.th/en/cii/

[4] T. Daengsi, P. Wuttidittachotti, P. Pornpongtechavanich and N. Utakrit, "A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization," Proc. of ICSCEE 2021, Cameron Highlands, Malaysia, 2021, pp. 102-106.

[5] P. Ungkap and T. Daengsi, "Cybersecurity Awareness Modeling Associated with Influential Factors Using AHP Technique: A Case of Railway Organizations in Thailand," Proc. of DASA 2022, Chiangrai, Thailand, 2022, pp. 1359-1362.

[6] T. Langan, "Federal bureau of investigation internet crime report 2022," IC3, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[7] Statista, "onsequences of successful phishing attacks on organizations worldwide in 2021 and 2022," Statista, https://www.statista.com/statistics/1350723/consequences-phishing-attacks/

[8] Kaspersky, "The number of phishing attacks doubled to reach over 500 million in 2022," Kaspersky, https://www.kaspersky.com/about/press-releases/2023_the-number-of-phishing-attacks-doubled-to-reach-over-500-million-in-2022

[9] 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, Winterton, South Africa, 2019, pp. 1-5.

[10] A. S. Abdullah and M. Mohd, "Spear Phishing Simulation in Critical Sector: Telecommunication and Defense Sub-sector," Proc. ICoCSec 2019, Negeri Sembilan, Malaysia, 2019, pp. 26-31.

[11] T. Aoyama, T. Nakano, I. Koshijima, I. Koshijima, Y. Hashimoto, and K. Watanabe, "On the Complexity of Cybersecurity Exercises Proportional to Preparedness," Journal of Disaster Research, vol. 12, no. 5, pp. 1081-1090, October 2017.

[12] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," April 2018, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[13] N. Nachin, C. Tangmanee, and K. Piromsopa, "How to Increase Cybersecurity Awareness" ISACA Journal, vol.2, pp. 45-50, March 2019.

[14] BOT, "Cyber Resilience Readiness Assessment Framework," BOT, https://www.bot.or.th/Thai/FinancialInstitutions/PruReg_HB/FSINotifications/Cyber%20resilience%20framework%202019.pdf. (In Thai)

[15] A. O. Nur, "Cybersecurity Awareness in Somalia," Thesis, School of Technology, Communication and Transport, JAMK University of Applied Sciences, 2021

[16] A. Diaz, A. T. Sherman, and A. Joshi, "Phishing in an academic community: A study of user susceptibility and behavior," Cryptologia, vol. 44, no. 1, pp. 53-67, January 2020.

[17] F. B. Fatokun, S. Hamid, A. Norman and J. O. Fatokun, "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, vol. 1339, 012098, April 2019

[18] S. Mousa, "Cyber Security: Exploring Awareness among University Students at a Public Educational Institution," International Journal of Innovative Research and Knowledge, vol. 4(5), May 2019, pp. 88-97.

[19] W. Li, J. Lee, J. Purl, F. L. Greitzer, B. Yousefi and K. B. Laskey, "Experimental Investigation of Demographic Factors Related to Phishing Susceptibility," Proc. of HICSS 2020, Maui, HI, 2020 pp. 2240-2249.

[20] D. Aljeaid, A. Alzhrani, M. Alrougi and O. Almalki, "Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks," Information, vol. 11(12), 547, November 2020.

[21] S. Chatchalermpun and T. Daengsi, "Improving cybersecurity awareness using phishing attack simulation," https://iopscience.iop.org/article/10.1088/1757-899X/1088/1/012015/pdf

[22] N. Davis and E. S. Grant, "Simulated Phishing Training Exercises versus Gamified Phishing Education Games," Proc. of ICERECT 2022, Mandya, India, 2022, pp. 1-8.

[23] T. Sutter, A. S. Bozkir, B. Gehring and P. Berlich, "Avoiding the Hook: Influential Factors of Phishing Awareness Training on Click-Rates and a Data-Driven Approach to Predict Email Difficulty Perception," IEEE Access, vol. 10, pp. 100540-100565, September 2022.

[24] F. Castaño, E. F. Fernañdez, R. Alaiz-Rodríguez and E. Alegre, "PhiKitA: Phishing Kit Attacks Dataset for Phishing Websites Identification," IEEE Access, vol. 11, pp. 40779-40789, April 2023.