2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE) | 978-1-6654-3222-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICSCEE50312.2021.9498208

A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization

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

Pongpisit Wuttidittachotti
Data Communication and Networking
KMUTNB, Bangkok, Thailand
pongpisit.w@itd.kmutnb.ac.th

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

Nathaporn Utakrit
Department of Information Technology
KMUTNB, Bangkok, Thailand
nathaporn.u@itd.kmutnb.ac.th

***Abstract*— Cybersecurity is an important issue for people who usually use the Internet for their purposes (e.g., ecommerce) in this era of the COVID-19 pandemic. For cyberthreats, phishing, which can be sent via email, can harm information systems in the organization. However, the risks from this kind of threats can be reduced if the employees have cybersecurity awareness. To prove this hypothesis with Thai employees, this paper presents a comparative study of cybersecurity awareness enhancement associated with the employees who work in different departments within the same organization in Bangkok, Thailand. In this study, the first phishing attack simulation was conducted before providing knowledge and training in cybersecurity to the employees and attacking with the second simulation. After result collection and analysis, it has been found that there are significant differences in cybersecurity awareness level between Thai employees from technology-based departments (e.g., IT department) and socialbased departments (e.g., HR department) within the same organization. Of course, the technology-based employees are the better. Furthermore, it has been found that the cybersecurity awareness level of Thai employees from the social-based department, which were poor when compared to the other one, was improved obviously after they were involved with the cybersecurity awareness enhancement processes.**

I. Introduction

Nowadays, people usually involve with Internet for many purposes (e.g., e-commerce and Internet banking), particularly in the situation of COVID-19 pandemic. Therefore, cybersecurity becomes a crucial issue, particularly for the financial sector since it is one of the several sectors that has been attacking from cyberthreats.

One of those kinds of cyberthreats is email-phishing which can be sent fake emails to users in financial firms (e.g., banks) [1]. If a user clicks to access the malicious link or URL, the malware (e.g., ransomware) may be activated, and it can harm the information systems in the financial organization. Furthermore, this kind of attacks may impact customer accounts broadly. However, cyber-risks from cyberthreats and cyberattacks can be reduced if users have cybersecurity awareness, which is impacted from several individual factors, including, cybersecurity training, educational background, working experience, field of study, gender, age, training and area of living, as stated in the Information Security Awareness (ISA) model, as mentioned in [2].

However, in this paper, different departments or business units (BUs) in an organization that relates to job functions and background of employees (including field of study, educational background, working experience and training) has been focused and investigated referring to Thai employees who works for a financial company in Thailand, with the major hypothesis (H) as follows:

H_0: cybersecurity awareness level among employees from different departments is the same.

H_1: cybersecurity awareness level among employees from different departments is different.

II. Background

This section describes background information and literature review as follows:

A. Cybersecurity Awareness and Its Related Factors

Cybersecurity can be the collection of best practices, concepts, policies, assurance, guidelines, safeguards, actions, risk management methods, training, tools and technologies that can be used to protect users' assets and the organization environment [3]. The assets can be networked devices, infrastructure, telecommunications systems, services, applications, and all kinds of information within the cyber environment [3]. Those assets must be secured based on three main objectives, called CIA for short that consists of confidentiality (C), integrity (I) and availability (A) [3]. Cybersecurity is a crucial aspect of people in this digital age. It becomes a key defense in protection systems in organizations and users or employees that relates to the protection against cyber-attacks due to vulnerabilities and security risks [4].

For the term 'awareness' in this paper. it means information security awareness (ISA) or cybersecurity awareness (CSA). It can be defined as understanding cybersecurity and responding to cyberthreats or cyber-attacks properly. Therefore, providing cybersecurity awareness training to users or workers in an organization is very important. The organization's program for cybersecurity awareness should be applied with the plan to enhance cybersecurity awareness of workers. The customized program may be utilized as a medium to train and/or educate and raise awareness among users or employees in each organization, to protect themselves and their organization from cyber-attacks (e.g., phishing).

For CSA related factors, there are several factors, including gender, age, nationality, field of study, working experience and training, called demographic factors [2]. Those factors play the role in cybersecurity awareness. For example, it has been found in [5] that gender has some effects in security self-efficacy, prior experience and computer skills. While it has been revealed in [6] that the years of computer usage or experience and gender impact the detection rate of phishing significantly.

B. Phishing

For cyberthreats in this age, phishing becomes an important issue for not only individuals but also organization. It uses both social engineering techniques and technological techniques (see Fig. 1) [7]. Phishing is similar to fishing in terms of meaning, it is an act of deception whereby impersonation is utilized by phishers to take sensitive information (e.g., user ID, email password, social networking application password and bank account number) in order to steal money from victims' bank account or credit card, or to install malware on the victims' computers or mobile devices. Normally, this kind of attack is related to sending phishing email with messages, contents and/or fake links or websites that is managed by a phisher (see Fig. 2) [8]. Phishing seems easy to avoid, but it is very complicated to identify or detect in practice.

C. Previous Related Works

There are many interesting works based-on phishing and CSA or ISA and their related factors. Those works can be briefly described as follows:

- Nur [9] conducted the survey in Somalia and found that phishing and vishing attacks are in the top ranks in banking sector and telecom industry.
- Filippidis et al. [10] found that educational level and study program trended to influence ISA. For example, master degree students tended to have more ISA than bachelor degree students.
- Diaz et al. [11] found from the study that there was a significant difference between the students from the College of Arts, Humanities, and Social Sciences and the College of Natural and Mathematical Sciences for responding the same phishing attack simulation.
- Fatokun et al. [12] found from their study that educational level, age and gender are important factors about cybersecurity behaviors of students.
- Mousa [13] found that IT students in Saudi Arabia do not have more skills than non–IT students. Also, it was found that there was a significant difference between male and female students.
- Li et al. [14] found from the study using phishing attack simulation that there were significant age effects, differences of email type and significant gender effects.
- Armstread [15] studied and then suggested that information technology simulation and security awareness training is an effective training tool.
- Greene et al. [16] studied and found that, based on phishing awareness training, not only training the employees but also exploring alternative ways that should work for each organization should be conducted.

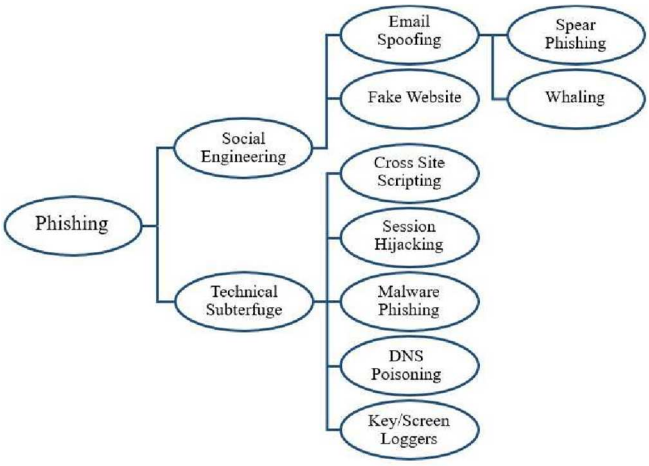

Fig. 1. Phishing techniques, adopted from [7]

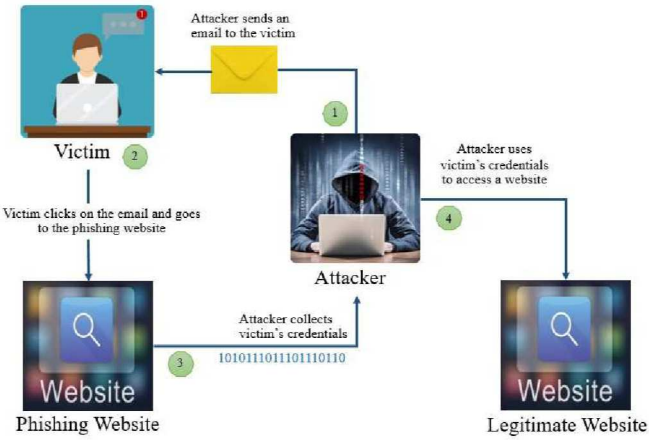

Fig. 2. Overview on phishing processes [8]

- Nachin et al. [17] studied and stated that the simulation approach can help to gain CSA level in organizations, and it is more practical than an instructor approach. However, both options should be combined and utilized.

- Carella et al. [18] studied the influence of CSA training and found that document training is the most effective compared with in-class training and no training.
- Aljeaid et al. [19] found that the type of technique to attack affects the users' judgments and confirmed that users can easily fall victim if they lack cybersecurity awareness and education.
- Chatchalermpun and Daengsi [8] found from their study with a huge number of Thai employees that cyber drills and knowledge transfer helped decreasing number of employees who filled in password in the fake link from 15% to only 2%.

From the review, there is no work that studies about effects of job functions of employees who work in different departments. Therefore, there is space to conduct a study in order to investigate this issue.

III. Methodology

In this study, the datasets collecting from a large financial company in Thailand, as mentioned in [8] were applied. However, only the data from the employees who work based on technologies, including employees in the information technology (IT) department (hereafter called TECH), and the employees who work based on social sciences, arts, humanities, including employees in human resources (HR) department and legal department (hereafter called SOCIAL), were studied and investigated. The utilized dataset consists of two sets from the phishing simulation study before and after conducting the cybersecurity awareness (CSA) enhancement processes (hereafter called Simulation 1 or SIM1 and Simulation 2 or SIM2, respectively). The processes covered mailing for the explanation about phishing simulation, proving e-learning program for employees who were in the criteria of victims.

After obtaining the data from Simulation1 and Simulation2 collected from the same 822 TECH-employees and 490 SOCIAL-employees, see Table. I, the data about employees who opened phishing email with and without filling-in password were validated, then were analyzed using the statistical technique called Chi-square [18]. The statistical results and analysis results are presented in the next section.

IV. Statistical Results and Discussion

From Simulation 1, as shown in Fig. 3 and Fig. 4, 19.66% of TECH employees and 31.43% of SOCIAL employees opened phishing email in Simulation1. Furthermore, some of them, 9.68% of TECH employees and 21.63% of SOCIAL employees, not only opened email but also clicked the fake line and filled in passwords in the fake link. However, after conducting the CSA enhancement processes in the organization, it has been found from Simulation2, as in Fig. 3 and Fig. 4, that 9.53% of TECH employees and 7.14% of SOCIAL employees opened the email in Simulation2, whereas some of them, 2.67% of TECH employees and 1.22% of SOCIAL employees also filled in passwords in the fake URL.

However, the results, as shown in Fig.3 and Fig. 4, were compared for the decreasing from Simulation1 and Simulation2 and then the differences or changes are presented in Table II. One can see that the change of 51.55% from TECH employees is less than the change of 77.27% from SOCIAL employees for opening phishing email, whereas the change of 94.34% from SOCIAL employees is greater than the change of 72.44% from TECH employees for filling password. That means that SOCIAL employees have more CSA improvement than TECH employees.

Moreover, to investigate whether there is a significant difference between TECH employees and SOCIAL employees within the same gender and overall, the hypotheses as in Table III were tested using a t-test. One can see as follows:

- Before enhancing the CSA, the Simulation 1 was conducted. As shown in Table II, there is no significant difference between TECH and SOCIAL in all cases about opening phishing email since p-values are greater than 0.050, whereas there are significant differences in all cases about filling password in Simulation1 between TECH and SOCIAL since pvalues are less than 0.050.
- After enhancing CSA and conducting the Simulation 2, it has been found that there are significant differences between TECH and SOCIAL in all cases since p-values are lower than 0.05, except the comparative result between TECH-females and SOCIAL-females (the p-value is 0.056, which is higher than 0.050) that trends to have insignificant difference.
- It can be implied from the hypothesis testing that it trends to have significant differences between two groups of departments in all cases about filling password, both in Simulation 1 and Simulation 2.

In addition, the findings in this study about the employees who have different job functions from technology-based departments and social-based departments are consistent with [9-11] that the studies about educational level and academic major, but they are inconsistent with [12].

TABLE I. Numbers of Employees in this Study

Groups of Departments		**Employees**	
	Male	***Female***	***Total***
TECH	428	159	587
SOCIAL	394	331	725
Total	822	490	1312

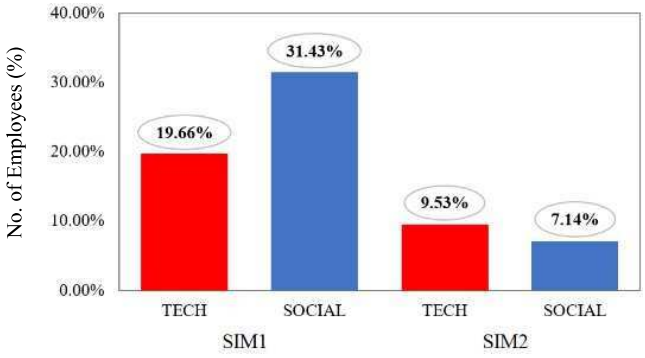

Fig. 3. Statistic of employees who opened phishing email.

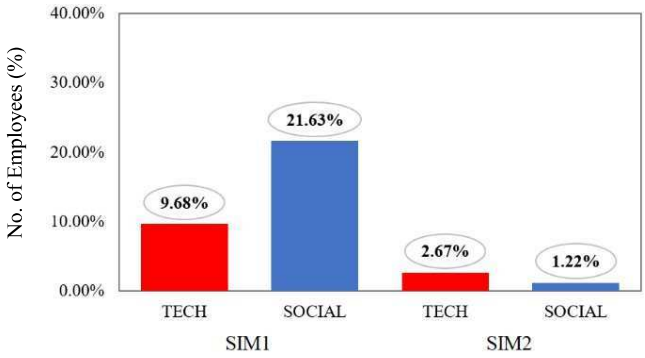

Fig. 4. Statistic of employees who filled in password into the fake link.

TABLE II. CHANGES OF RESPONDING TO PHISHING EMAIL FROM SIM1 AND SIME2

Group of Departments	Response	Change (%)	Remark
TECH	Email opening	51.55%	Decreased
	Password filling	72.44%	Decreased
SOCIAL	Email opening	77.27%	Decreased
	Password filling	94.34%	Decreased

TABLE III. ANALYSIS RESULTS

Hypotheses	Simulation	p-value
$H1_0$: CSA level from TECH-males = CSA level from SOCIAL-males for opening email	SIM1	0.414
$H1_1$: CSA level from TECH-male ≠ CSA level from SOCIAL-males for opening email	SIM2	0.005*
$H1_0$: CSA level from TECH-females = CSA level from SOCIAL-females for opening email	SIM1	0.993
$H2_1$: CSA level from TECH-females ≠ CSA level from SOCIAL-females for opening email	SIM2	0.002*
$H3_0$: CSA level from TECH-all = CSA level from SOCIAL-all for opening email	SIM1	0.987
$H3_1$: CSA level from TECH-all = CSA level from SOCIAL-all for email opening	SIM2	<0.001*
$H4_0$: CSA level from TECH-males = CSA level from SOCIAL-males for password filling	SIM1	0.038*
$H4_1$: CSA level from TECH-males = CSA level from SOCIAL-males for filling password	SIM2	0.009*
$H5_0$: CSA level from TECH-females = CSA level from SOCIAL-females for filling password	SIM1	0.014*
$H5_1$: CSA level from TECH-females = CSA level from SOCIAL-females for filling password	SIM2	0.056
$H6_0$: CSA level from TECH-all = CSA level from SOCIAL- all for filling password	SIM1	0.005*
$H6_1$: CSA level from TECH-all = CSA level from SOCIAL-all for filling password	SIM2	0.002*

*There are significant differences within 95% Confidence Interval.

Last but not least, the result from this study confirms that CSA enhancement process is an effective approach, which is consistent with [8], [14-17], particularly it has been found that the employees who work in social-based departments (e.g., HR Department) have low CSA level before the enhancement processes. However, they have been improved dramatically, when compared to the employees who work in technologybased departments (e.g., IT Department).

V. CONCLUSION

After the investigation in this study with Thai employees, it confirms that cybersecurity awareness enhancement processes (e.g., simulations and training) are important and useful for improvement of the cybersecurity awareness level of employees in organizations. Particularly, the employees, who may have work experience and educational background about social sciences, arts and humanities and work in socialbased departments, should be provided good training and lessons about cybersecurity awareness.

ACKNOWLEDGMENT

Thank you to Rajamangala University of Technology Phra Nakhon and Rajamangala University of Technology Rattankosin (Wang Klai Kangwon Campus), and King Mongkut's University of Technology North Bangkok for supporting this study. Lastly, thank you to Mr. Surachai Chatchalermpun for data sharing.

REFERENCES

[1] S. Chatchalermpun, P. Wuttidittachotti and T. Daengsi, "Cybersecurity Drill Test Using Phishing Attack: A Pilot Study of a Large Financial Services Firm in Thailand," Proc. of ISCAIE 2020, Malaysia, Apr. 2020, pp. 283-286

[2] A. Farooq, J. Isoaho, S. Virtanen and J. Isoaho, "Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors," Proc. of IEEE Trustcom/BigDataSE/ISPA 2015, Helsinki, Finland, Aug. 2015, pp. 352-359

[3] ITU-T, "X.1205: Overview of cybersecurity," 2008, Available: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

[4] http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S2077-72132017000100007

[5] M. Anwar, W. He, I. Ash, X. Yuan, L. Li and L. Xu, "Gender difference and employees' cybersecurity behaviors," Computers in Human Behavior, vol. 69, April 2017, pp. 437-443,

[6] C. Iuga, J.R.C. Nurse and A. Erola, “Baiting the hook: factors impacting susceptibility to phishing attacks,” Human-centric Computing and Information Sciences, vol. 6, no.8, 2016. Available: https://doi.org/10.1186/s13673-016-0065-2

[7] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, “Defending against phishing attacks: taxonomy of methods, current issues and future directions,” Telecommunication Systems, vol. 67, pp. 247–267, 2018

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

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

[10] A. P. Filippidis, C. S. Hilas, G. Filippidis and A. Politis, “Information Security Awareness of Greek Higher Education Students - Preliminary Findings,” Proc. of MOCAST 2018, Thessaloniki, Greece, 2018, pp. 14

[11] 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, 2020, pp. 53-67. Available: https://doi.org/10.1080/01611194.2019.1623343

[12] 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, 2019

[13] 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.

[14] 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 the 53rd Hawaii International Conference on System Sciences 2020

[15] S. K. Armstead, “The Effectiveness of Information Technology Simulation and Security Awareness Training on U.S. Military Personnel in IRAQ and Afghanistan,” Ph.D. Dissertation, Capella University, 2016

[16] K. K. Greene, M. Steves and M. Theofanos, “No Phishing beyond This Point,” in IEEE Computer, vol. 51, no. 6, pp. 86–89

[17] N. Nachin, C. Tangmanee, and K. Piromsopa, “How to Increase Cybersecurity Awareness,” ISACA Journal, vol.2, 2019.

[18] A. Carella, M. Kotsoev and T. M. Truta, “Impact of security awareness training on phishing click-through rates,” Proc. of Big Data 2017, Boston, MA, 2017, pp. 4458-4466

[19] 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, 2020.