www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

Analyzing the Impact of Information Security Awareness Training to the Employees of Telco Company XYZ

Erlangga Putro Subagyo[1], Kalamullah Ramli[2*]
[1,2]*Faculty of Electrical Engineering, Universitas Indonesia*
**Corresponding author*
*erlangga.putro@ui.ac.id, kalamullah.ramli@ui.ac.id**

Abstract

As a company that is operating in the telecommunication sector, XYZ must ensure that they have adequate capabilities to protect their company's and customers' sensitive data. Although various information security systems and processes are already in place, human resources still are the weakest link in cyber security. The new normal of Working From Home makes the threat even larger. Basically, Information Security Awareness (ISA) denotes whether or not users are aware of information security objectives. Using a phishing scenario, this study examined the level of ISA of XYZ employees and how ISA training might improve their awareness level. The simulation outcomes were compared to the results before and after they received ISA training on a percentage scale. The results showed a positive increase between before and after being given training. Employees who clicked on phishing URLs before training reached 31% reduced to 12% after training. Meanwhile, employees affected by phishing decreased from 24% to 4%. The study also revealed discovered that based on the nature of the job, employees who work at directorates who work more on non-technical matters have lower awareness when compared to employees who work at directorates who work more on technical work.

Keywords
information security awareness; phishing; training

I. Introduction

From the beginning of 2020 until this article was written, the world has been hit by the COVID-19 pandemic. This demands a change in the way things work in all sectors. Almost all companies applied the Work From Home working method, where employees can work from their respective homes by relying on an internet connection. This, of course, has its risks because several security holes are not protected by the company's security protection system for employees working at home.

The outbreak of this virus has an impact of a nation and Globally (Ningrum *et al*, 2020). The presence of Covid-19 as a pandemic certainly has an economic, social and psychological impact on society (Saleh and Mujahiddin, 2020). Covid 19 pandemic caused all efforts not to be as maximal as expected (Sihombing and Nasib, 2020).

The telecommunications sector is one of the sectors that "benefit" from this pandemic situation, where the need for an internet connection is increasing due to the implementation of the Work From Home working method. the internet has become an essential part of daily life rather than being a luxury. The demand for Home fiber connection installations and the purchase of internet data packages has increased significantly. According to data from we are social-Hootsuite, the number of internet users in Indonesia as of January 2021 has increased by 73,8% among Indonesia's population of 274.9 million, or about 202.6 million users. So, there has been an addition of 27 million

users over the past year. In terms of traffic, several telecommunications operators said there was an increase in traffic as a result of the pandemic, which reached 40%.

On the other hand, with the increase in internet service users, telecommunication operators must also be able to maintain the protection of their information; these include not only Company's data but also the Customer's data. Organizational survival has become increasingly dependent on information security. A data breach regarding those data will affect the credibility of the company; it can even continue to the legal realm. Operators must strengthen their cyber security system in terms of technology, process, and people.

Information Security Awareness (ISA) has a major impact on employees' information security behaviors and compliance with security policies (Bulgurcu et al., 2010 ; DeGroot et al., 2012). Previous research has suggested that a lack of employee ISA through Information Security Policies (ISP) and procedures is the primary cause of sensitive data mishandling (e.g., Siponen, 2000 & Abraham, 2011). How to improve end-user awareness is a key challenge in security. People are frequently the weakest link, and they are frequently to blame for a security system failure. Users' unconcerned behaviors are most of the cyber security threats that originate from, especially those users who are less aware of security threats and consequences. Therefore, humans play a critical role in the system's information security, and they must be aware of security risks in order for the system to be reliable and work optimally. One example of a personal data leak case involving a telecommunication company caused by a weak human factor is the leaking of personal data of one of the social media activists in Indonesia. This case leads to the social activist to threaten the telecommunications operator to take the matter to court. Employees' awareness of information security is still low, as seen by such a negative attitude.

This study measures the impact of ISA training on the level of XYZ employees' awareness based on the click-through rate on a phishing simulation. The simulation was divided into two phases. The first phase is conducted before the employees receive ISA Training, and the second phase is after the employees receive ISA Training. We looked into related studies before deciding on a scenario and the instruments that would be employed to achieve the desired outcome. We ended the study by comparing the results from phase 1 and phase 2 of the phishing assessment click-through rate to see if the training attained the goal of increasing employee ISA level.

The rest of this work is designed as follows. The literature review, related works, and measuring method are all described in Section II. The technique, data collection, and hypothesis are all described in Section III. After explaining the comparison of the simulation findings and interpreting them into a defined analysis, Section IV examines the assumptions. Section V finishes with a summary of the findings and research recommendations.

II. Review of Literature

2.1 Information

Information is akin to any other business asset that has great value to any organization and therefore needs protection. Data such as customer identity, MSISDN number, company financial data, are examples of information that has high value for the company. Leakage, loss or damage to such information will cause enormous losses to the company, both financially and corporate image. Not infrequently this can lead to the realm of law.

2.2 Information Security Awareness (ISA)

In a nutshell, ISA denotes whether or not users are aware of and dedicated to an organization's information security objective. It also includes employees' understanding of the company's information security procedures. Individual cognitive perceptions of information security and their adherence to mandatory information security policies are depicted in this idea. ISA has long been recognized as a critical component in accomplishing information security objectives in organizations.

In order to determine the degrees of ISA inside businesses, three factors need to be assessed. Attitude, knowledge, and behavior are the three components.

2.3 Simulated Phishing Training

Simulated phishing training is a sort of security education that educates corporate end-users how to prevent being phished when using email systems. Training systems that allow simulated phishing include mechanisms for producing phishing emails, recording user responses, and reporting the results. A simulated phishing system is depicted in Figure 1 below.

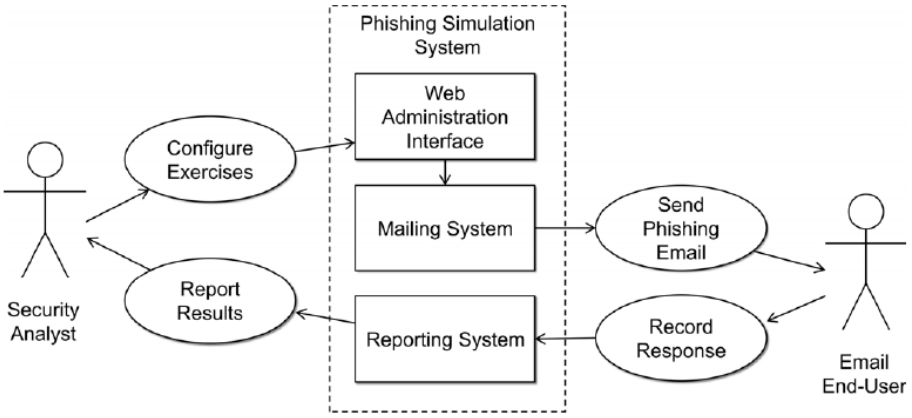

Figure 1. *Phishing simulation system*

2.4 Attack Simulation Technique

There are five social engineering/phishing techniques based on the MITRE Attack framework, as below:

a. Credential Harvest: a message with a URL will be generated by the attacker and emailed to the target recipients. They will be redirected to a website that asks for their personal information when they click on it.
b. Malware Attachment: The attacker sends a message to the recipient's email account with a malicious attachment (e.g., pdf, word document, etc.). The attachment would contain malware that may install itself on the recipient's device if clicked in an actual cyberattack.
c. Link in attachment: This is essentially a hybrid of the two previous procedures. The attacker will send a message that includes a malicious URL as an attachment. The end-user will then be led to a page that asks for personal information, similar to the one used in credential harvest.
d. Link to Malware: a message containing a malicious link to a website attachment (e.g Sharpoint, Dropbox) is being sent by the attacker. When a user clicks on the link, arbitrary code, such as a macro, is executed to aid the attacker in installing more code on the target's device, which could lead to malware infection.

e. Drive-by URL: The attacker provides the user a URL that leads to a trustworthy website. The website, on the other hand, is a hacked or clone of the original.

2.5 Related Works

Several studies to measure the ISA level has been conducted. Carella et al. studied 150 University of Northern Kentucky students who were the targets of phishing campaigns to see how information network security education affected their behavior when confronted with phishing assaults. The results revealed that the group that had gotten no prior information security training before the phishing campaign was six times more likely to be targeted by an attacker than the group that had received prior information security training.

Hantyoko and colleagues used the KAB modeling created by Kruger and Kearney to determine the level of ISA among personnel at the Ministry of Research, Technology, and Higher Education (2006). The findings revealed that 13 of the 21 characteristics placed employees in a favorable position in terms of ISA.

Gufron and colleagues use case studies at the Directorate General of ABC (DG ABC) in Indonesia to assess the level of information security knowledge among government personnel. This study combined a behavior approach with a phishing simulation and a knowledge approach with a Likert scale questionnaire. The simulation results and the questionnaire results have a substantial link, according to the findings. 69 percent of employees who read the email clicked on the link to the camouflage page, and through the quiz, it was discovered that DG ABC employees' ISA level was at 79.32 percent, which was the lower limit of the GOOD category.

Yesem and colleagues investigate the existing level of ISA among college and high school students and build a program to help them improve their knowledge. Their module's key elements are interaction and the display of alarming repercussions of regular Internet/technology users' reckless cyber behaviors. According to their survey data, the module has had a positive influence on both groups of students, with non-computer science majors having the most benefit. There is also no significant difference in ISA levels between male and female students, according to the findings.

The novelty feature of this research, based on the four studies above, is in merging the techniques and the research object, that is, the telecommunication company employees as the research object and simulated phishing training as the research method.

III. Research Method

3.1 Research Objects

This study involved all XYZ employees as the object of this research. The total number of XYZ employees from various directorates is 1535 people. Table I displays data on XYZ employees who are used as phishing objects based on the directorate.

Table 1. List of Phishing Objects

Directorate	# of Employee
President Office	25
Commercial	530
Corporate Affairs	57
Enterprise	138
Finance	216

Home Business	40
Human Resources	39
Information Technology	267
Network	223
Grand Total	**1535**

3.2 Phishing Simulation Tool & Technique

This study used Office 365 Attack Simulator as the phishing simulation system. Credential Harvest is the attack simulation technique that is used for the simulation. A message will be generated with a URL and, and being sent to the target recipients. They will be routed to a website that will ask for their personal credentials if they click on it. From the tool, we are able to grab the report of how many employees click the URL, and how many employees have submitted their credential data.

3.3 Phishing Simulation Scenario

The simulation is carried out in 2 stages:

a. The first phase is carried out before employees receive ISA training. This is to observe the security awareness level of XYZ employees before completing the training.
b. The second phase is carried out after employees receive ISA training. This is to observe the security awareness level of XYZ employees after completing the training.

The results of the first phase of the simulation will be compared with the results of the second phase of the simulation to measure the effectiveness of the training provided to employees.

3.4 Information Security Awareness Training

ISA awareness training module was developed in this study that is expected to be able to help to raise the level of ISA awareness among XYZ employees. ISA training is given to XYZ employees in the form of an online module. The material of the module consists of below topics:

a. Introduction of Information Security
b. What is a phishing attack and what are the common types of phishing technique
c. Password policy which complies with the security standard
d. How to recognize and deal with phishing

After completing the learning module, employees must be able to complete post-test questions with a minimum score of 80 to pass. If they didn't pass the minimum score, they should retake the post-test until they reach the minimum score.

3.5 Project Timeline

Due to a large number of employees, the phishing campaign is divided into several batches. ISA training is carried out in a span of 3 weeks, this is to give time and ensure all employees have completed their training modules. In detail, the project timeline can be seen in Table II below.

Table 2. Project Timeline

Week	Activity
Week 1	Phishing Campaign Batch 1 (before training)
Week 2	Phishing Campaign Batch 2 (before training)
Week 3	Phishing Campaign Batch 3 (before training)

Week 4	ISA Training for all Employee
Week 5	
Week 6	
Week 7	Phishing Campaign Batch 1 (after training)
Week 8	Phishing Campaign Batch 2 (after training)
Week 9	Phishing Campaign Batch 3 (after training)

IV. Results and Discussion

4.1 Results

a. Phishing Result Before Training

Among the 1535 employees who were sent phishing emails, there were 479 employees who clicked the malicious link which consist of 101 employees who only clicked without proceeding to provide their credentials and 378 employees who clicked the link and carry on to input their credentials as can be seen in Table III. As shown in Figure 1, in percentage terms, employees who only clicked on links were 31%. 6 % didn't proceed to credential input, while 25% proceed to credential input.

It is also discovered that based on the nature of the job, employees who work at directorates that are more on non-technical matters have lower awareness when compared to employees who work at directorates that are more on technical matters.

Table 3. Phishing Assessment Result Before Training

Directorate	Email Sent	Didn't Click Link	Only Clicked Link	Clicked & Phished
President Office	25	12	3	10
Commercial	530	350	40	140
Corporate Affairs	57	41	2	14
Enterprise	138	91	8	39
Finance	216	145	19	52
Home Business	40	17	3	20
Human Resources	39	25	2	12
Information Technology	267	201	17	49
Network	223	174	7	42
Total Employee	1535	1056	101	378

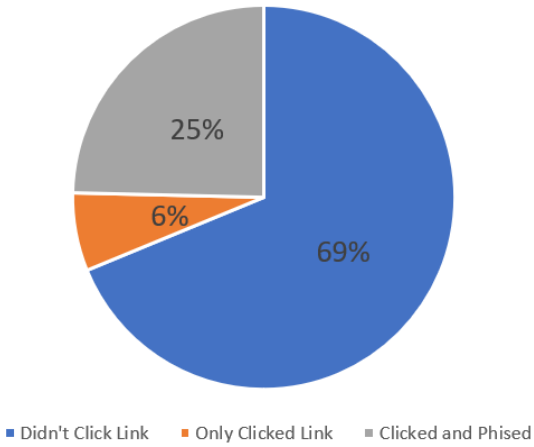

Figure 2. *Phishing Assessment Result by Percentage Before Training*

Table 4. Clicked & Phished Percentage

Directorate	Clicked & Phished Percentage
Home Business	50%
President Office	40%
Human Resources	31%
Enterprise	28%
Commercial	26%
Corporate Affairs	25%
Finance	24%
Network	19%
Information Technology	18%

b. Phishing Result After Training

After the training has been given, among the 1535 employees who were sent phishing emails, there were 170 employees who clicked the malicious link, which consist of 113 employees who only clicked without proceeding to provide their data credentials and 57 employees who clicked the link and carry on to input their credentials as can be seen in Table V. As shown in Figure 3, in percentage terms, employees who only clicked on links were 31%. 6 % didn't proceed to credential input, while 25% proceed to credential input.

Table 5. Phishing Result After Training

Directorate	Email Sent	Didn't Click Link	Only Clicked Link	Clicked & Phished
President Office	25	20	2	3
Commercial	530	454	51	25
Corporate Affairs	57	50	3	4
Enterprise	138	128	8	2
Finance	216	197	12	7
Home Business	40	32	4	4
Human Resources	39	34	2	3
Information Technology	267	248	14	5
Network	223	202	17	4
Total Employee	1535	1365	113	57

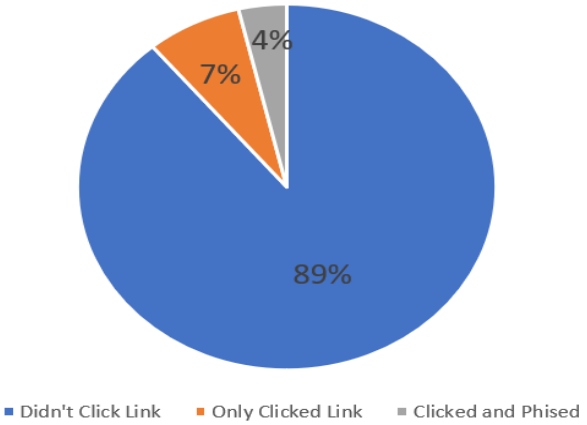

Figure 3. *Phishing Assessment Result by Percentage After Training*

4.2 Discussion

Based on the comparison between the results of the phishing assessment before and after the ISA Training, it can be concluded that the ISA Training provided to employees can significantly increase the level of ISA. Based on Figure 4, the number of employees who clicked after training was reduced by 6%, while the number of employees who clicked and provided their personal credentials was reduced by 21%.

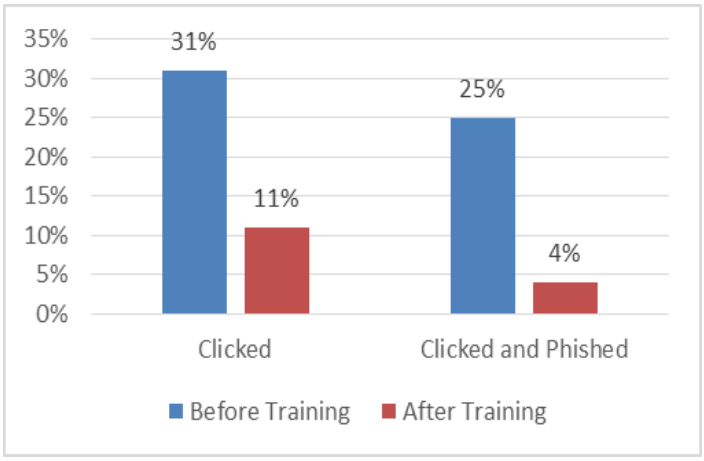

Figure 4. *Click Rate Comparison Before & After Training*

V. Conclusion

Based on this study, it is discovered that ISA level of XYZ employees was found low before the ISA Training was performed (31% clicked on the malicious link in the email content, while 25% of them carry on to submit their credentials. The ISA training succeeds to increase their level of awareness. After the training, the number of employees who clicked malicous link after training was reduced by 6%, while the number of employees who clicked and provided their personal credentials was reduced by 21%. It is also discovered that based on the nature of the job, employees who work at directorates who work more on non-technical matters have lower awareness when compared to employees who work at directorates who work more on technical work.

To maintain the level of awareness, it is recommended that the ISA training is performed at least once a year. Future research can use a combination of other attack simulation techniques to get a more holistic view of the level of awareness.

References

A. S. P. P. S S Tirumala, "A survey on Internet usage and cybersecurity awareness in students," *2016 14th Annual Conference on Privacy, Security and Trust (PST),* 2016.

A. W. D. P. Adetokunbo Bashorun, "Information Security: To determine its Level of Awareness in an Organization," *2013 7th International Conference on Application of Information and Communication Technologies,* 2013.

C. Indonesia, "cnnindonesia.com," 06 July 2020. [Online]. Available: https://www.cnnindonesia.com/teknologi/20200706072707-192-521192/data-pribadi-bocor-denny-siregar-ancam-gugat-telkomsel. [Diakses 06 March 2022].

D. E. I. I. I. Heru Sutadi, "kontan.co.id," 26 February 2021. [Online]. Available: https://adv.kontan.co.id/news/pandemi-dan-meningkatnya-kebutuhan-akses-data-internet. [Diakses 06 March 2022].

G. M. P. S. Steven McElwee, "Influencing Outcomes and Behaviors in Simulated Phishing Exercises," *SoutheastCon 2018,* 2018.

K. R. Mukhammad Gufron Ikhsan, "Measuring the Information Security Awareness Level of Government Employees Through Phishing Assessment," *2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC),* 2019.

L. R. S. d. S. Yesem Kurt Peker, "Online Cybersecurity Awareness Modules for College and High School Students," *2018 National Cyber Summit Research Track,* pp. 24-33, 2018.

Ningrum, P. A., et al. (2020). The Potential of Poverty in the City of Palangka Raya: Study SMIs Affected Pandemic Covid 19. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)* Volume 3, No 3, Page: 1626-1634

Saleh, A., Mujahiddin. (2020). Challenges and Opportunities for Community Empowerment Practices in Indonesia during the Covid-19 Pandemic through Strengthening the Role of Higher Education. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*. Volume 3, No 2, Page: 1105-1113.

Sihombing, E. H., Nasib. (2020). The Decision of Choosing Course in the Era of Covid 19 through the Telemarketing Program, Personal Selling and College Image. *Budapest*

M. K. T. M. T. Anthony Carella, "Impact of Security Awareness Training on Phishing Click-Through Rates," *2017 IEEE International Conference on Big Data (BIGDATA),* pp. 4458-4466, 217.

M. Kassner, "techrepublic.com," 21 December 2020. [Online]. Available: https://www.techrepublic.com/article/cybersecurity-pros-are-humans-really-the-weakest-link/#:~:text=%E2%80%9CPeople%20often%20represent%20the%20weakest,and%20first%20published%20in%202000.. [Diakses 06 March 2022].

M. M. K. S. R. Yaman Salem, "Evaluation of Information Security Awareness among Palestinian Learners," *2021 International Conference on Information Technology (ICIT),* pp. 21-26, 2021.

M. N. K. F. E. W. J. Mohd Sarifuddin bin Othman@Mustafa, "An Enhanced Model for Increasing Awareness of Vocational Students Against Phishing Attacks," *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS 2019), 29 June 2019, Selangor, Malaysia,* pp. 10-14, 2019.

Office365Reports, “Train Your Office 365 Users Against Phishing Attacks using Attack Simulation Training,” Microsoft, 12 March 2022. [Online]. Available: https://o365reports.com/2022/02/16/train-your-office-365-users-against-phishing-attacks-using-attack-simulation-training/. [Diakses 19 March 2022].

S. F. N. C. Emad Sherif, “Awareness, Behaviour and Culture: The ABC in Cultivating Security Compliance,” *The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015),* pp. 90-94, 2015.

S. G. S. M. I. A. S. Khando Khando, “Enhancing Employees Information Security Awareness in public and private organisations: A systemic literature review,” *computers & security 106 (2021) 102267,* vol. 106, pp. 1-22, 2021.

S. M. Hong Chan, “Significance of Information Security Awareness in the Higher Education Sector,” *International Journal of Computer Applications (0975 – 8887),* Vol. %1 dari %260– No.10, pp. 23-31, 2012.

T. B. Phil Legg, “Tools and Techniques for Improving Cyber Situational Awareness of Targeted Phishing Attacks,” *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA),* 2019.

T. D. S. I. Iffah Budiningsih, “Awareness, Dominant Factor For Improving Information Security,” *Cakrawala Pendidikan,* Vol. 38, No. 3, pp. 490-498, 2019.

Y. S. G. a. A. G. D. D. Hantyoko, “Information Security Awareness Level Measurement for Employee: Case Study at Ministry of Research, Technology, and Higher Education,” *2017 3rd International Conference on Science in Information Technology (ICSITech),* pp. 654-658, 2017.