Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 4 Iss. 4 October 2024, pp: 1330-1338
ISSN(P): 2797-2313 | ISSN(E): 2775-8575

Analysis of Measuring Information Security Awareness for Employees at Institution XYZ

Rachmat Bayu Permadi[1], Kalamullah Ramli[2*]

[1,2] Department of Electrical Engineering, Faculty of Engineering,
University of Indonesia, Indonesia

E-mail: rachmat.bayu@ui.ac.id[1], kalamullah.ramli@ui.ac.id[2]

Received Jun 8th 2024; Revised Jul 16th 2024; Accepted Jul 20th 2024
Corresponding Author: Kalamullah Ramli

Abstract

As a government institution in the field of civil servant management, XYZ Institution has data on 4.4 million Employees spread throughout Indonesia which needs to be maintained. Based on the BSSN report, there has been a significant increase in potential threats in recent years and is expected to continue in 2024, one of which is the threat of Phishing. This research was conducted to measure the level of Information Security Awareness (ISA) for employees at xyz institution. Phishing simulations and questionnaires are used to measure the level of ISA and how to provide ISA education so that it can increase the level of ISA employees. Simulation results will be compared before and after the provision of ISA education. The results of providing education have a positive impact for employees. Simulation before providing education there were 65% of employees clicking on phishing urls and after education there was a decrease to 17%. While employees who were exposed to phishing before education were 33% and after education there was a decrease to 16%. In addition, the questionnaire filled out by 150 employees showed results with a value of 86.54% for the level of ISA employee, which is in the good category.

Keyword: Education, Information Security Awareness, Phishing, Simulation

1. INTRODUCTION

XYZ Institution is a non-ministerial government institution whose main tasks and functions are in the field of personnel management in accordance with the provisions of laws and regulations. Institution XYZ is responsible to the President of the Republic of Indonesia through the Ministry of State Apparatus Utilization and Bureaucratic Reform [1]. Based on the State Civil Apparatus statistics book for semester II of 2023, the total number of government employees throughout Indonesia is 4.46 million. Of these statistics, 78% come from regional agencies and 22% come from central agencies spread throughout Indonesia [2].

Another important role of this xyz institution is to maintain data and be responsible for managing government employee data throughout Indonesia [3]. XYZ institution also provides convenience for the community and government employees by providing web-based services that can be accessed anywhere and anytime using an internet connection [4].

Along with the advancement of technology, information security threats will also increase. Based on the 2023 cyber security landscape report, BSSN analysis predicts several potential cyber threats that are predicted to emerge in 2024. These include Ransomware, Cyber Threats Based on Artificial Intelligence (AI), Web Defacement, Attack, Advanced Persistent Threat (APT), Internet of Things (IoT), Distributed Denial of Service (DDoS) and Phishing. The determination of these potential threats is based on a significant increase in numbers in recent years, showing an upward trend that is expected to continue in 2024 [5].

Most information security incidents are caused by humans [6] and most information security problems, both deliberate and inadvertent misbehaviour, are caused directly or indirectly by human mistake [7]. This indicates that humans really are the weakest element in information security.

From the xyz institution's side, based on information from the xyz Directorate, at least until 2023 there are several cyber incidents that have occurred at xyz institutions [8]. Despite the wide range of information security technologies and processes available, human resources are the weakest link in cybersecurity. Cyber incidents can occur unnoticed and there is a need for collective awareness in addressing the risk of cyber attacks. Therefore, it is important to conduct regular information security awareness programmes to raise employees' awareness of information security [9],[10]. Employee understanding of information security rules and procedures is anticipated to rise as a result of the information security awareness initiative.

Information security awareness (ISA) is a person's assessment in understanding, committing, and behaving in compliance with the laws, regulations, and policies governing information security [11]. The definition corresponds to the main basis of the HAIS-Q, namely the Knowledge-Attitude-Behaviour (KAB) model. Based on the KAB model, The information security rules and processes that employees are aware of inside the company, their perspective on these policies and procedures, and their information security-related conduct are all factors to consider. [12].

Social engineering is a technique of data theft of a person's valuable information by using focussed social interaction [13]. Another definition is a technique that exploits the weaknesses of human attacks [14]. Frequent examples of social engineering are phishing, malware, spear phishing, pretexting and baiting. Social engineering attacks are different, but they have the same pattern. The phases are similar. The way it works is mostly the same: firstly collecting target information, secondly engaging with the target, then using the available information to carry out the attack and finally leaving no trace [15],[16].

Several previous research have examined information security awareness measurement techniques. Such as measuring information security awareness through information security awareness training in one of the German companies in 2023. The research designed and implemented 3 different information security awareness methods and verified the results based on phishing simulations. The method consists of pre-study, phishing simulation training and awareness campaign, and post-study. The focus of the research was on phishing training, effectiveness of information security awareness and feedback from participants. The results of this study show that information security awareness campaigns can result in a higher success rate in detecting phishing attacks [17].

Next up is a research on information security awareness in one South African organisation in 2023. This study measured the information security awareness of employees participated by 356 respondents. This study uses the Human Aspects of Information Security Questionnaire (HAIS-Q), which is based on the Knowledge, Attitude, Behaviour (KAB) model as a user ISA measurement instrument [12],[18]. The purpose of this research is to determine the level of employee awareness, to make recommendations aimed at increasing awareness within the organisation. The findings of this study indicate that age, language, organisation size and gender are important factors in designing, creating or updating an information security awareness programme for an organisation [19].

In this research, the main focus is to measure the level of information security awareness and improve the ISA level at XYZ institution. The method used is the Human Aspects of Information Security Questionnaire (HAIS-Q) with a focus on 8 areas of modified development results from ISO 27002 with the Knowledge, Attitude, Behaviour approach and also phishing simulations to combine the results of the level of information security awareness with information security awareness training. This is done to see the comparison or effectiveness of providing information security awareness training. In this phising simulation, a social engineering variant is also included to test the weakness of the mindset towards human trust. This research was conducted because there has never been a previous study that developed a questionnaire with 8 focus areas of information security with phishing simulations and evaluated with online information security awareness training in measuring and increasing security awareness at XYZ institutions. The reason for the urgency of the author choosing XYZ Institution as a case study is because in the midst of the increasing number of diverse cyber incidents in government institutions and also one of the important government institutions in Indonesia, which has data on government employees throughout Indonesia that needs to be kept safe, and has digital services that are vulnerable to cyber attacks [5].

2. MATERIALS AND METHOD

The research consisted of an eight-stage procedure intended to ensure the accuracy and reliability of the results. The process consists of the following steps: identifying the problem, searching the literature, choosing research methods, creating research instruments, collecting data, processing and analysing data, Creating Recommendations and Establishing Conclusions. Each step of the process is depicted in Figure 1. The research attempts to make sure that all significant aspects are included and the outcomes can be explained by employing this systematic technique. This methodical approach not only broadens the scope of the study but also promotes accurate and dependable research results, which form a crucial basis for well-informed recommendations and conclusions.

2.1. Research Instruments

The measuring instrument used in this research is the HAIS-Q Model, which measures the level of information security awareness of employees at XYZ Institution. The HAIS-Q Model has seven focus areas. Three dimensions comprise the variables utilised in this research, knowledge, which refers to what the participants know about information security, attitude which describes how the participants feel about information security, and behavioural model which refers to the participants actions towards information security. The KAB model, which combines these characteristics, offers a thorough foundation for comprehending information security awareness.

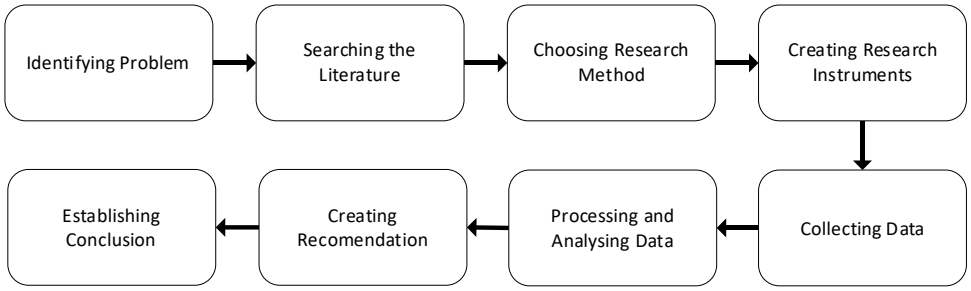

Figure 1. Research Step

Researchers conducted research using 75 questions derived from HAIS-Q and ISO/IEC 27002: 2013. [12],[20]. This method makes it possible to identify and assess eight different focus areas within the domain of information security awareness. These focus areas serve as a theoretical model for understanding different aspects of information security. These focus areas are depicted in Figure 2.

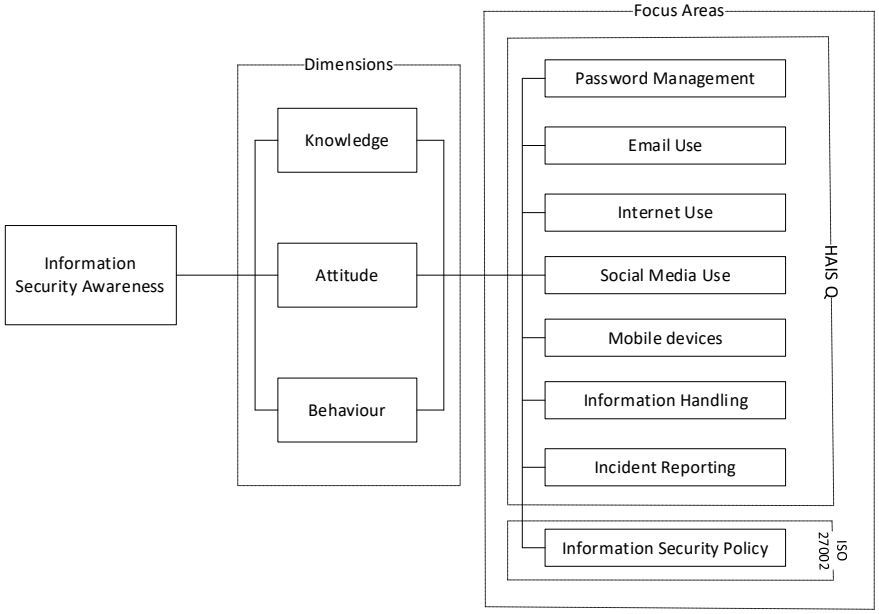

Figure 2. Theoritical Model

Questionnaire method using the three-dimensional approach of the KAB model. The first part of the questionnaire looked at the knowledge dimension, the second part looked at the attitude dimension, and the third part looked at the behavioural factors [21]. The research questions were asked sequentially, and each question received a short answer on a Likert scale from 1 to 5. This scale is shown in Table 1.

Table 1. Answer Scale Value

Scale Value	Description
1	Strongly Disagree
2	Disagree
3	Netral
4	Agree
5	Strongly Agree

The next assessment instrument is a phishing simulation, which uses phishing emails to gauge employees awareness of information security. Phishing simulation training is one of the security education that educates an organisation to prevent phishing in using email [22]. This phishing training system includes mechanisms such as recording user responses and reporting results. As shown in figure 3. Below is an overview of the mechanism of the phishing simulation for employees at XYZ institution.

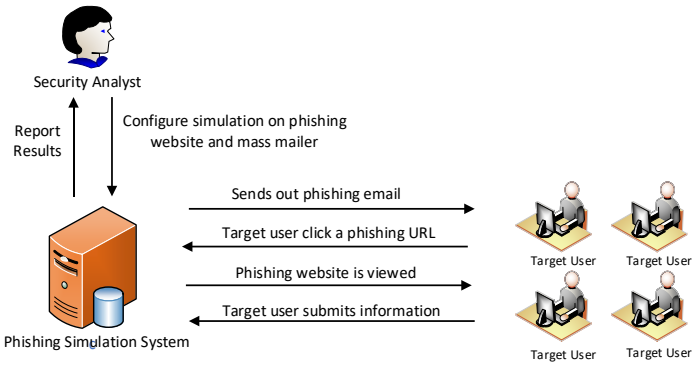

Figure 3. Phishing Simulation Flow

2.2. Data Collection

The researcher conducted a research questionnaire survey at XYZ Institution from March to April 2024. Google Forms was used to create the survey and collect data. Google Forms is an accessible and user-friendly internet form that makes it easy and fast for researchers to create and modify questions.

The next stage is to provide questionnaires to employees of XYZ Institution. We accomplished this by using the whatsapp app, which is a popular communication tool among XYZ Institution employees. By ensuring that the questionnaire is easily available to employees, this approach promotes a higher number of responses. The questionnaire was freely distributed across Institution XYZ offices situated throughout Indonesia in order to guarantee that the data collected in this study accurately reflects the perspectives and experiences of all employees regarding information security awareness. The aim is that the responses collected from this questionnaire are a representative sample of the population from each region of Institution XYZ regarding information security awareness.

After collecting questionnaire data, the next step was to conduct the first phishing simulation training and the second phishing simulation to 200 employees of XYZ institutions in April 2024 and May 2024. The number of 200 employees is a sample that is determined and can represent each population of XYZ Institutions throughout Indonesia. The phishing scenario used is to use a phishing email to XYZ Institution employees in the form of a fake invitation 'zoom Invite' to attend a meeting event. The purpose of this phishing simulation training is to increase the awareness of XYZ Institution employees of information security, especially in phishing.

2.3. Methods / Techniques for Analyzing Data Methods

The validity testing method uses Bivariate Pearson Analysis (Pearson Product Moment Correlation). With a sample size of 150 and a 2-tailed significance value of 0.05, the Pearson values of all the variables are greater than the critical value of 0.159 according to the Pearson Critical Value Table. [23].

The reliability test is carried out using Cronbach's Alpha, the reliability calculation can only be done if the questionnaire is already valid when the validity test is carried out. Thus, you must calculate the validity first before calculating the reliability [24]. The most commonly recognised measure of reliability is the Cronbach Alpha coefficient. This is the most appropriate reliability measure used when the research instrument is structured using a Likert scale. A variable is considered dependable or consistent in measuring the variables if its Cronbach Alpha value is more than 0.70 [25].

The KAB model, which was developed by Kruger & Kearney (2006) to gauge information security awareness, is the model used in this study [12]. This processing uses Microsoft Excel to analyse descriptive statistics that produce average data in each dimension of knowledge, attitude and behaviour. By dividing the total score by the Likert scale's maximum value (Y) and multiplying the result by 100%, as shown in Equation, the index values were achieved (1).

$$Index = \frac{Total\ Score}{Y} \text{ x } 100 \quad (1)$$

After the computation of the mean value for every dimension using the gathered index values. As shown in Table 2, Kruger and Kearney (2006) have categorised information security knowledge into three levels: Good (80 - 100%), Medium (60 - 79%), and Poor (≤59%).

Table 2. Information security awareness assessment scale [12]

Awareness	Measurement (%)
Good	80-100
Average	60-79
Poor	≤ 59

3. RESULTS AND DISCUSSION

After the level of awareness was ascertained by analysis of the questionnaire responses, the outcomes of the phishing simulation were integrated. Furthermore, this information is used to make recommendations regarding information security awareness at XYZ Institution.

3.1. Questionnaire Result Analysis

The questionnaire had previously been distributed to all regions of XYZ Institution and filled in using google form. In total, 150 people filled out the questionnaire that had been distributed from March 2024 to April 2024 from all work units of XYZ Institution in Indonesia. Respondent statistical data can be seen in Table 3.

Table 3. Questionnaire Respondent Demoghrapic

	Categories	Total	Percentage
Gender	Male	71	47 %
	Female	79	53 %
Employee Status	Civil Servant (PNS)	134	89 %
	Government Employee with a Work Agreement (PPPK)	16	11 %
Last Education	≤ SMA (High School)	1	1 %
	D-I, D-II, D-III (Diploma)	20	13 %
	D-IV/S-1 (Bachelor)	103	69 %
	S-2/S-3 (Master/Doctor)	26	1 %
Age Group (years)	≤ 30	48	32 %
	31 - 35	56	37 %
	36 - 40	21	14 %
	41 - 45	10	7 %
	46 - 50	9	6 %
	≥ 51	6	4 %
Length of Service (years)	≤ 5	88	59 %
	6 - 10	30	20 %
	11 - 15	9	6 %
	16 - 20	13	9 %
	21 - 25	4	3 %
	≥ 26	6	4 %
Job Title	Managerial	11	7 %
	Non Managerial	139	93 %
Working Unit	Headquarters	30	20 %
	Regional Offices	120	80 %

The results of measuring the average level of information security awareness of employees of XYZ Institution are shown in Table 4. The value obtained after data processing is 86.54%. According to the categories previously described by Kruger and Kearney, the level of information security awareness of employees of XYZ Institution is at the 'Good' level.

Table 4. Result of Security Awareness Level Measurement

No	Focus Area	Knowledge	Attitude	Behavior	Awareness Level
1	Password Management	93,24	92,98	88,04	91,42
2	Email Use	79,76	88,60	86,03	84,80
3	Internet Use	92,27	89,78	83,87	88,64
4	Social Media Use	81,67	92,13	91,40	88,40
5	Incident Reporting	85,60	87,56	84,80	85,99
6	Mobile Devices	73,07	84,09	76,89	78,01
7	Information Handling	91,13	90,67	85,90	89,23
8	Information Security Policy	84,49	88,71	84,18	85,79
	Average	85,15	89,31	85,14	86,54

According to the table, the attitude dimension has the greatest average value of 89.31%, while the behaviour dimension has the lowest average value of 85.14%, which is nearly equal to the average knowledge dimension of 85.15%. On the other hand, if you look at the focus areas based on the KAB dimension, the lowest level of awareness is found in the focus area of mobile devices at 78.01% and email use at 84.80%. Although scoring in the good category, it does not mean that there are no information security events in the area of concern because humans are the weakest chain in information security that is vulnerable to various types of attacks and psychological manipulation.

3.2. Validity Test

The validity test used analysis with the two-way Pearson Product Moment correlation method (2-tailed), which correlates the factor score to the total score as in Table 5 is data processing using the SPSS application. Based on the study of Hair et al. (2021), a value above 0.159 can be said to be valid and meet the criteria.

Table 5. Result of Validity Pearson

No	Focus Area	Knowledge	Attitude	Behaviour
1	Password Management	.447**	.457**	.452**
2		.434**	.600**	.523**
3		.487**	.446**	.459**
4	Email Use	.526**	.431**	.413**
5		.390**	.660**	.633**
6		.374**	.421**	.343**
7	Internet Use	.428**	.588**	.623**
8		.503**	.613**	.545**
9		.537**	.549**	.581**
10	Social Media Use	.623**	.382**	.589**
11		.596**	.506**	.552**
12		.318**	.502**	.606**
13	Incident Reporting	.439**	.574**	.700**
14		.624**	.537**	.643**
15		.584**	.601**	.604**
16	Mobile Devices	.469**	.394**	.567**
17		.687**	.299**	.682**
18		.459**	.587**	.625**
19	Information Handling	.609**	.494**	.578**
20		.596**	.521**	.615**
21		.644**	.591**	.451**
22	Information Security Policy	.586**	.633**	.636**
23		.653**	.661**	.644**
24		.654**	.608**	.672**
25		.538**	.534**	.624**

3.3. Reliability Test

Reliability testing is conducted as part of testing the reliability of the measurement indicators used in the study. As previously explained, the variable value is considered reliable if the Cronbach's Alpha value is greater than or equal to 0.70. Table 6 displays the Cronbach's alpha value found in this study, where the three variables have a value of more than 0.70 so they are considered reliable.

Table 6. Reliability Statistics

Variable	Cronbach's alpha
Knowledge	.917
Attitude	.917
Behavior	.940

3.4. Phishing Simulation I

Phishing simulation I was conducted in April 2024 by sending phishing emails to employees of XYZ Institution. The results of the phishing simulation I report in Table 5 show that only 65% of XYZ Institution employees clicked the link in the phishing email sent to employees, and 33% of employees submitted data on the phishing web.

Table 5. Phishing Simulation Result I

Email Delivered	Email Opened	Opened (% to Delivered)	Link Clicked	Clicked (% to Opened)	Submitted data	Submited (% to Clicked)
200	60	30%	39	65%	13	33%

3.5. Security Awareness Training

Information security awareness training is one of the strategic approaches taken to educate employees about the importance of cybersecurity and data privacy. In information security awareness training, employees will be educated about information security policies, the dangers of cybercrime, the impact of cyber incidents, mitigating cybersecurity risks and learning from a cyber attack case. The primary goals are to lower the risks related to cyber threats and raise staff understanding of security issues. Employees of XYZ Institution participated in the online information security awareness training at the end of April 2024.

3.6. Phishing Simulation II

Phishing simulation II was conducted in May 2024 after the information security awareness training. The results of the phishing simulation II report in Table 6 show that only 34% of XYZ Institution employees clicked the link in the phishing email sent to employees, and 16% of employees submitted data on the phishing web.

Table 6. Phishing Simulation Result II

Email Delivered	Email Opened	Opened (% to Delivered)	Link Clicked	Clicked (% to Opened)	Submitted data	Submited (% to Clicked)
200	68	34%	12	17%	2	16%

3.7. Comparison of the Phishing Simulation

After phishing simulation I and phishing simulation II, there is a positive comparison of the results of the impact of information security awareness training for employees at XYZ Institution. When comparing Table 5 and Table 6, there is an increase in employees' information security awareness of phishing emails. As in phishing simulation I, the percentage of employees who clicked on the link in the phishing email was 65% and in phishing simulation II the percentage of employees who clicked on the link in the phishing email was 17%. This means that there is a reduction of 53% or a significant increase in employee information security awareness. While the percentage of employees who submit data on the phishing web in phishing simulation I is 33% and in phishing simulation II is 16%. This means that there is a decrease of 17% or an increase in information security awareness of XYZ Institution employees.

4. CONCLUSION

Measurement of the level of information security awareness for employees at XYZ Institution has been completed using HAIS-Q and the KAB model. This measurement is carried out by taking into account the dimensions of knowledge, attitudes, and behaviour of employees. Measurement of employee information security awareness at XYZ Institution has 8 focus areas consisting of password management, email use, internet use, social media use, incident reporting, mobile devices, information handling and information security policy. In addition, there are other measurements using phishing simulation I and phishing simulation II.

Based on the results of research using HAIS-Q and the KAB model, it is found that the average level of information security awareness of XYZ Institution employees from each focus area is in the 'Good' category, namely with a value of 86.54. The lowest focus area in the results of this study is the use of mobile still has a 'Medium' level of awareness and needs to be improved. While the research results in phishing simulation I through phishing emails sent show as in Table 5, namely the percentage comparison of employees who open messages with employees who click on phishing links is 65% and the percentage comparison between employees who click on links and employees who submit data on the phishing web is 33%. Furthermore, in the results of phishing simulation II as in Table 6, the percentage of employees who open messages with employees who click on phishing links is 17% and the percentage comparison between employees who click on links and employees who submit data on phishing webs is 16%.

Following the first phishing simulation, XYZ Institution employees participated in an online training on information security awareness. In this education, employees are given insights related to information security awareness including information security policies, the dangers of cybercrime, the impact of cyber incidents, cyber security risk mitigation to learning from a cyber attack case. The main objective is to increase the information security awareness of XYZ Institution employees. The results of this information security awareness education can be seen from the comparison of the results of the phishing I simulation, which is before the information security awareness education and the results of the phishing II simulation after the information security awareness education. After the education related to information security awareness, employees of XYZ Institution have higher vigilance towards information security.

Despite the results of research with HAIS-Q and KAB in the 'Good' category, it does not mean that there will be no information security events because humans are the weakest chain in information security that is vulnerable to various types of attacks and psychological manipulation. There are still gaps that need to be watched out for such as social engineering techniques carried out on phishing simulations using phishing emails. The recommendation in this research is to create a regular and comprehensive information security

awareness programme. The information security awareness programme must be in accordance with the information security policy and made interesting.

Although research on measuring information security awareness has been done with different methods and objects of research, information security awareness is a dynamic thing and needs to do the latest research in accordance with the developments of the times as cybersecurity incidents are increasing and varied. The results of this study are expected to be a consideration in the formulation of regulations on the obligation of a personal information security awareness index especially for employees in the government sector.

In the mobile devices awareness focus area which has the lowest score, it needs to be improved by increasing the capacity of human resources through intensive education or training. Employees also need to be socialised directly about information security policies, especially in the use of mobile devices, so that they can add insight and vigilance to information security.

Like any other research, this study has limitations. First, it only focuses on the government sector, especially employees of XYZ Institution. Future research is expected to conduct research in the government sector for all employees in Indonesia. Secondly, this research focuses on online information security awareness training, in the future there needs to be further research on the effectiveness of several types of information security awareness programmes used by XYZ Institution.

ACKNOWLEDGMENTS

The author would like to thank the Ministry of Communications and Informatics the Republic of Indonesia for the funding support of this work.

REFERENCES

[1] Perpres, "Presiden Republik Indonesia Peraturan Presiden Republik Indonesia tentang Badan Kepegawaian Negara," *Demogr. Res.*, pp. 4–7, 2013.

[2] BKN, "Buku Statistik Aparatur Sipil Negara," 2023. [Online]. Available: https://satudataasn.bkn.go.id/data-publication

[3] BKN, "Peraturan Badan Kepegawaian Negara Republik Indonesia Nomor 13 Tahun 2022 Tentang Satu Data Bidang Aparatur Sipil Negara," p. 282, 2022, [Online]. Available: https://www.bkn.go.id/unggahan/2023/02/PerBKN-Nomor-13-Tahun-2022.pdf

[4] BKN, "Layanan - Badan Kepegawaian Negara (BKN RI)," BKN.go.id. Accessed: Feb. 05, 2024. [Online]. Available: https://www.bkn.go.id/layanan/

[5] BSSN, "Lanskap Keamanan Siber Indonesia," 2024. [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

[6] B. C. Stahl, N. F. Doherty, and M. Shaw, "Information security policies in the UK healthcare sector: A critical evaluation," *Inf. Syst. J.*, vol. 22, no. 1, pp. 77–94, 2012, doi: 10.1111/j.1365-2575.2011.00378.x.

[7] M. Siponen and A. Vance, "Neutralization: New insights into the problem of employee information systems security policy violations," *MIS Q. Manag. Inf. Syst.*, vol. 34, no. SPEC. ISSUE 3, pp. 487–502, 2010, doi: 10.2307/25750688.

[8] A. Fadhil and S. Yazid, "Measurement of Employee Information Security Awareness: A Case Study of National Civil Service Agency," *Indones. J. Comput. Sci.*, vol. 12, no. 6, pp. 3581–3597, 2024, doi: 10.33022/ijcs.v12i6.3640.

[9] W. Yeoh, H. Huang, W. S. Lee, F. Al Jafari, and R. Mansson, "Simulated Phishing Attack and Embedded Training Campaign," *J. Comput. Inf. Syst.*, vol. 62, no. 4, pp. 802–821, 2022, doi: 10.1080/08874417.2021.1919941.

[10] Q. An, W. C. H. Hong, X. S. Xu, Y. Zhang, and K. Kolletar-Zhu, "How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates," *Int. J. Inf. Secur.*, vol. 22, no. 2, pp. 305–317, Apr. 2023, doi: 10.1007/s10207-022-00637-z.

[11] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, 2017, doi: 10.1016/j.cose.2017.01.004.

[12] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006, doi: 10.1016/j.cose.2006.02.008.

[13] W. Febriyani, D. Fathia, A. Widjajarto, and M. Lubis, "Security Awareness Strategy for Phishing Email Scams: A Case Study One of a Company in Singapore," *JOIV Int. J. Informatics Vis.*, vol. 7, no. 3, pp. 808–814, Sep. 2023, doi: 10.30630/joiv.7.3.2081.

[14] C. M. R. da Silva, E. L. Feitosa, and V. C. Garcia, "Heuristic-based strategy for Phishing prediction: A survey of URL-based approach," *Comput. Secur.*, vol. 88, p. 101613, 2020, doi: 10.1016/j.cose.2019.101613.

[15] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios,"

Comput. Secur., vol. 59, pp. 186–209, 2016, doi: 10.1016/j.cose.2016.03.004.

[16] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "Phishing Happens beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process," *IEEE Access*, vol. 9, pp. 44928–44949, 2021, doi: 10.1109/ACCESS.2021.3066383.

[17] L. Gamisch and D. Pöhn, "A Study of Different Awareness Campaigns in a Company," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2023. doi: 10.1145/3600160.3605006.

[18] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior," *IEEE Access*, vol. 10, pp. 132132–132143, 2022, doi: 10.1109/ACCESS.2022.3230286.

[19] E. Kritzinger, A. Da Veiga, and W. van Staden, "Measuring organizational information security awareness in South Africa," *Inf. Secur. J.*, vol. 32, no. 2, pp. 120–133, 2023, doi: 10.1080/19393555.2022.2077265.

[20] E. Lachapele and M. Bislimi, "Iso/Iec 27002:2013," *Int. Organ. Stand.*, pp. 1–13, 2016, [Online]. Available: www.pecb.com

[21] M. A. Rizal and B. Setiawan, "Information Security Awareness Literature Review: Focus Area for Measurement Instruments," in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 1420–1427. doi: 10.1016/j.procs.2024.03.141.

[22] Y. Shin, K. Kim, J. J. Lee, and K. Lee, "Focusing on the Weakest Link: A Similarity Analysis on Phishing Campaigns Based on the ATT&CK Matrix," *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/1699657.

[23] Statistics Solutions, "Table of critical values: Pearson Correlation - Statistics solutions," Statisticssolutions.com. Accessed: Apr. 18, 2024. [Online]. Available: https://www.statisticssolutions.com/free-resources/directory-of-statistical-analyses/pearsons-correlation-coefficient/table-of-critical-values-pearson-correlation/

[24] C. Busschaert, I. De Bourdeaudhuij, V. Van Holle, S. F. M. Chastin, G. Cardon, and K. De Cocker, "Reliability and validity of three questionnaires measuring context-specific sedentary behaviour and associated correlates in adolescents, adults and older adults," *Int. J. Behav. Nutr. Phys. Act.*, vol. 12, no. 1, pp. 1–14, 2015, doi: 10.1186/s12966-015-0277-2.

[25] H. Taherdoost, "Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research," *SSRN Electron. J.*, vol. 5, no. 3, pp. 28–36, 2018, doi: 10.2139/ssrn.3205040.