Bulletin of Electrical Engineering and Informatics
Vol. 15, No. 4, August 2026, pp. 3356~3364
ISSN: 2302-9285, DOI: 10.11591/eei.v15i4.10199

Role of decision style and knowledge in awareness influence to phishing detection in higher education

Muh. Bafadhal Kurnia Alamsyah, Candiwan
Business Management of Telecommunication and Informatics, Faculty of Economics and Business, Telkom University, Bandung, Indonesia

Article Info

Article history:

Received Mar 3, 2025
Revised Apr 23, 2026
Accepted Jun 19, 2026

Keywords:

Cybersecurity awareness
Information security awareness
Intuitive decision style
Phishing detection
Phishing email knowledge

ABSTRACT

Phishing attacks are a significant cybersecurity threat in higher education, where employees handle sensitive data such as student records, financial transactions, and research information. This study investigates the relationship between information security awareness (ISA), intuitive decision style (IDS), and phishing detection confidence (PDC), while assessing the moderating role of phishing email knowledge (PEK). A quantitative approach was employed, using a structured questionnaire distributed to 120 employees at XYZ University in Indonesia. Data were analyzed using moderated mediation analysis with PROCESS Macro. The findings indicate that ISA positively influences IDS, but an overreliance on intuition negatively impacts PDC. PEK significantly moderates this relationship, reducing the negative effects of intuitive decision-making. The results emphasize the importance of cybersecurity awareness and phishing-specific training programs to enhance detection confidence. Organizations should integrate security awareness programs with phishing simulations and automated detection tools to strengthen their cybersecurity defenses. This study is limited by its focus on a single organization and reliance on self-reported measures. Future research should explore additional cognitive and contextual factors influencing phishing susceptibility to develop more comprehensive security strategies.

Corresponding Author:

Candiwan
Business Management of Telecommunication and Informatics, Faculty of Economics and Business
Telkom University
Bandung, Indonesia
Email: candiwan@telkomuniversity.ac.id

1. INTRODUCTION

The rapid advancement of information and communication technology has transformed many sectors, including education. However, this progress also increases the risks of cybersecurity threats, particularly phishing attacks. Phishing is a cyberattack technique that exploits social engineering to obtain sensitive information via electronic communication by impersonating legitimate entities [1]. In Indonesia, phishing remains one of the most prevalent cybersecurity threats, as recent studies highlight significant cyberattack activities targeting institutional environments [2]. These threats endanger data security, privacy, and institutional integrity, making higher education institutions particularly vulnerable.

In the academic environment, phishing attacks may compromise the personal data of students, faculty, and employees, thereby disrupting institutional operations. Employees are central to maintaining information security, yet their awareness and knowledge of phishing remain limited [2]. Impulsive or intuitive decision-making styles may further exacerbate susceptibility, as phishing attempts are often designed to trigger rapid emotional responses. This highlights the importance of understanding how cognitive processes, awareness, and

knowledge interact in shaping individuals' ability to resist phishing. XYZ University in Indonesia has been selected as the case study for this research due to its recent experiences with cybersecurity incidents, particularly phishing attacks targeting its employees. Several employees at XYZ University have fallen victim to phishing scams, leading to potential security breaches that threaten institutional data. One crucial factor in mitigating this risk is increasing cybersecurity awareness.

Previous studies provide important foundations for this research. Naga *et al.* [3] emphasized that cybersecurity awareness reduces vulnerability by encouraging caution in handling suspicious emails. Sturman *et al.* [4] examined the role of information security awareness (ISA) and intuitive decision-making in influencing behavioral intention and phishing detection, finding that higher awareness improves detection ability but may be moderated by decision style. Brickley [5] noted that phishing detection confidence (PDC) depends not only on awareness and skills but also on subjective factors such as prior experience, knowledge, and self-assessed ability. Moreover, research shows that knowledge of phishing techniques strengthens one's ability to identify fraudulent emails, though it may also generate false confidence if overestimated [6].

Despite these contributions, several research gaps remain. First, most prior studies have focused on behavioral intention or actual detection rather than confidence in detection, even though confidence strongly influences decision-making in real phishing scenarios [5]. Second, the role of intuitive decision style (IDS) as a mediator between awareness and PDC has not been sufficiently examined. Third, limited studies in the Indonesian higher education context have analyzed how phishing knowledge moderates these relationships. Addressing these gaps is critical, as employees in universities face growing cybersecurity threats but are rarely the main focus of empirical investigations.

The objective of this paper is analyze the relationship between ISA, decision-making style, and phishing knowledge in influencing PDC among employees at XYZ University in Indonesia. Specifically, this research examines the mediating role of intuitive decision-making style and the moderating effect of phishing email knowledge (PEK) in the relationship between ISA and PDC. By addressing these aspects, the study seeks to provide insights that contribute to both theoretical advancements and practical applications in cybersecurity awareness and phishing prevention strategies.

The research framework in this study integrates as shown in Figure 1. Insights from Sturman *et al.* [4] regarding the relationship between ISA, IDS, and behavioral intention and phishing detection. However, this study modifies the dependent variable by replacing behavioral intention and phishing detection with PDC. This change is made to better align the research focus with how individuals assess their ability to detect phishing rather than merely their intention to act. This shift aligns with Brickley [5], who emphasizes that confidence in phishing detection can influence detection effectiveness, both positively and negatively. Furthermore, this study retains PEK as a moderating factor, allowing for an exploration of whether increased knowledge about phishing truly enhances confidence in detecting threats or instead fosters false confidence, potentially making individuals more susceptible to sophisticated phishing attacks. By adapting the previous research framework, this research analyses provide deeper insights into the psychological and cognitive mechanisms that shape an individual's confidence in phishing detection.

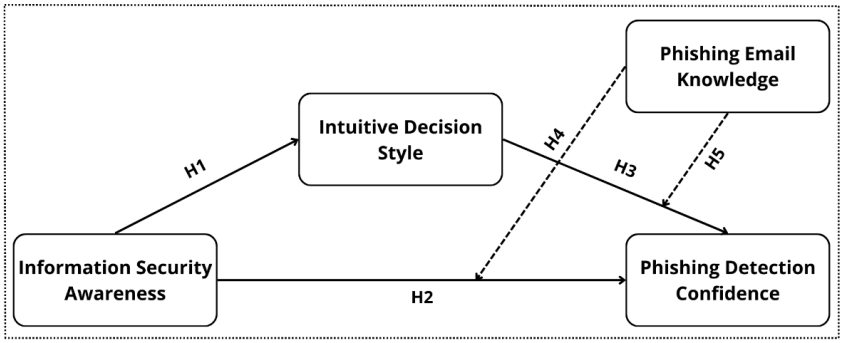

Figure 1. Theoretical model of moderated mediation [4]

Specifically, this study hypothesizes that ISA positively influences IDS among employees at XYZ University in Indonesia (H1) and also has a positive effect on phishing detection confidence (H2). Furthermore, it is expected that IDS positively influences phishing detection confidence (H3). In addition to these direct relationships, this study investigates whether PEK moderates the relationship between ISA and phishing detection confidence (H4) as well as the relationship between IDS and phishing detection confidence (H5). By

testing these hypotheses, this study seeks to provide empirical insights into how these factors interact to enhance PDC among employees in an academic work environment.

2. METHOD

This study examines the relationship between ISA, decision-making styles, and PDC among employees of XYZ University in Indonesia. The population consists of all 120 employees at XYZ University in Indonesia, aligning with Cresswell [7], who define a population as a group of subjects or objects with specific characteristics relevant to research objectives. As noted by Sekaran and Bougie [8], a sample is a subset of the population that represents the entire group, ensuring that the findings reflect broader trends within the target population. Using Cochran's formula, the minimum required sample size for a population of 120, with a 95% confidence level and a 5% margin of error, is approximately 92 respondents. However, given the relatively small population size, this study employs saturated sampling, a non-probability sampling technique where the entire population is included as research participants. Unlike probability sampling, which ensures equal selection opportunities, non-probability sampling does not guarantee equal chances for all individuals [7]. Saturated sampling is particularly useful in this context as it provides a comprehensive understanding of the entire employee group without the need for random selection.

A total of 120 participants were included in the study. As shown in Table 1, the gender distribution is nearly balanced, with 51% male participants (n=61) and 49% female participants (n=59). Regarding generational cohorts, the largest group of participants belongs to the Millennial generation (40%, n=48), followed by Generation Z (33%, n=40) and Generation X (25%, n=30). The Baby Boomer generation accounts for only 2% (n=2), making it the least represented group. In terms of educational background, Table 1 indicates that most participants hold a Bachelor's degree (43%, n=52), followed by Doctorate holders (25%, n=30) and Master's degree holders (22%, n=26). Participants with Diploma 3 (7%, n=8) and Senior High School education (3%, n=4) are the least represented. From the data in Table 1, it can be concluded that the study sample primarily consists of Millennials with a Bachelor's degree. This demographic composition provides a comprehensive representation of cybersecurity awareness across different generations and educational levels.

Table 1. Participant demographics

Category	Subcategory	Percentage (%)	n
Gender	Female	49	59
	Male	51	61
Generation	Generation Z	33	40
	Millennials	40	48
	Generation X	25	30
	Baby Boomers	2	2
Education level	Senior High School	3	4
	Diploma 3	7	8
	Bachelor's degree	43	52
	Master's degree	22	26
	Doctorate	25	30

This study employs a quantitative approach to analyze statistical relationships between variables. According to Brahimi and Leperlier [9], quantitative methods provide a comprehensive understanding beyond individual perspectives. A structured questionnaire is used to assess key research variables, ensuring consistency in data collection and analysis [10]. While primary data offers firsthand insights, it requires significant time and resources (Cresswell [7]). The questionnaire, designed with clear instructions, employs a Likert scale to measure respondents' attitudes toward key indicators [11], enabling a nuanced understanding of security awareness, decision-making styles, and PDC.

In this study, data were collected using a structured questionnaire combined with a practical email sorting task. The questionnaire consisted of four main constructs. ISA was measured using 9 items that assess employees' understanding and vigilance regarding cybersecurity practices. PEK was measured with 15 items designed to evaluate the respondents' ability to recognize the common characteristics of phishing emails, such as suspicious links, sender anomalies, and spelling errors. IDS was measured with 5 items capturing the extent to which individuals rely on intuition and instinct rather than deliberate analysis when making decisions. The primary outcome variable, PDC, was assessed using 15 questionnaire items and complemented by an email sorting task. In this task, participants were presented with a series of email examples, consisting of legitimate and phishing emails. For each email, they were asked to indicate their perceived security level by responding to the statement: "I feel safe clicking on the link in this email." This measurement approach strengthens the validity of the PDC construct by confidence and practical detection performance.

After data collection, data will be analyzed using descriptive statistics to summarize key characteristics and inferential analysis to examine variable relationships and test hypotheses. The data will be coded and processed using statistical software. Methodological challenges include limited generalizability, as the sample is from XYZ University in Indonesia, though the use of saturated sampling minimizes bias. Response rate issues will be addressed through follow-ups and reminders. Additionally, measurement accuracy will be enhanced by using validated measurement scales.

Validity and reliability ensure accurate measurement and consistency in research instruments. Validity testing verifies whether the questionnaire accurately captures research variables [7]. Statements representing each variable were tested using SPSS with 30 respondents, following the recommended sample size for normality. A statement is valid if its r-value exceeds the critical r-table value (0.361). Results confirmed that all items met validity criteria. Reliability testing assesses the instrument's consistency over time using Cronbach's Alpha [7]. An instrument is reliable if $r \geq 0.70$. SPSS results showed that all variables exceeded this threshold: PDC (0.921), PEK (0.925), IDS (0.886), and ISA (0.934). The overall reliability score was 0.966, indicating exceptional reliability.

The data analysis technique in this study employs moderated mediation analysis to evaluate the relationships among the independent variable, mediator, moderator, and dependent variable simultaneously. Huang *et al.* [12] stated that causal explanation helps in identifying complex cause-effect relationships, thereby strengthening the validity of the research model. Hayes [13] explained that moderated mediation is an analytical approach that examines whether the mediating effect of the independent variable (X) on the dependent variable (Y) through a mediator (M) varies depending on the value of a moderator (W). This technique is used to understand complex variable relationships and provide deeper insights into the mechanisms and conditions influencing the indirect effect.

The analysis is conducted using PROCESS Macro version 4.3, developed by Andrew F. Hayes. PROCESS Macro is specifically designed for analyzing mediation and moderation models in linear regression. By using PROCESS, this study can easily estimate direct effects, indirect effects, and interaction effects (moderation). Additionally, PROCESS facilitates the use of the bootstrapping method to enhance the accuracy of confidence interval estimation [13]. This study applies Model 15 in PROCESS Macro, which represents a moderated mediation model where the effect of the independent variable on the dependent variable is mediated by a single mediator, and this mediation relationship is influenced by a single moderator. Sekaran and Bougie [8] noted that analyzing the dependent variable allows researchers to identify the influencing factors and provide answers or solutions to the research problem. This framework guides the moderated mediation analysis employed in this study. This model is chosen because it allows for an in-depth analysis of complex relationships between variables, including how the mediation effect depends on the level of the moderator [13].

The analysis process follows several steps. First, the study identifies the examined variables, including the independent variable (X) as ISA, which reflects respondents' awareness of information security; the mediator (M) as IDS, which represents respondents' preference for intuitive decision-making when evaluating emails; the moderator (W) as PEK, indicating respondents' level of knowledge about phishing characteristics; and the dependent variable (Y) as PDC, which measures the tendency to avoid clicking on malicious email links. Next, data transformation is performed, where the ISA, IDS, and PEK variables are converted into z-scores to obtain standardized effect sizes. Additionally, the moderator variable (PEK is categorized into three levels: low (−1 standard deviation), average (mean), and high (+1 standard deviation).

The analysis process consists of four main steps. First, the direct effect analysis is conducted to measure the direct relationship between ISA (X) and PDC (Y). Second, mediation analysis examines whether the relationship between ISA (X) and Y is mediated by IDS (M). Third, moderation analysis assesses whether the direct and indirect effects are influenced by the level of PEK (W). Lastly, to obtain more accurate results, a bootstrap method with 5,000 samples is used to calculate confidence intervals for direct and indirect effects. Alfons *et al.* [14] stated that the bootstrap method is preferred over traditional methods that assume normality, as it allows for more flexible and accurate estimation of indirect effects and helps determine statistical significance based on confidence intervals.

The decision criteria for this analysis are as follows. The relationships between variables are considered significant if the p-value is less than 0.05. The moderation and mediation effects are deemed significant if the confidence interval does not include zero.

3. RESULTS AND DISCUSSION

3.1. Results

3.1.1. Descriptive statistics and correlation analysis

Prior to hypothesis testing, a descriptive statistical analysis was conducted to examine the mean, standard deviation, and correlation among the study variables. Table 2 presents the regression model for IDS predictors, demonstrating the relationship between ISA and IDS. The results indicate that ISA is positively

correlated with IDS (r=0.637, p<0.01), confirming the positive influence of ISA on IDS. Additionally, the coefficient for ISA→IDS (0.637) is statistically significant (p=0.000), reinforcing the relationship between these variables. The table also includes a control variable (COV), which shows a negative effect (-0.148) on IDS with a significance level of p=0.034. These findings support Hypothesis 1 (H1), which states that ISA positively influences IDS.

Table 2. Regression model for IDS predictor

Variable	Coefficient	SE (HC4)	t	p-value	LLCI	ULCI
Constant	0.441	0.196	2.249	0.026	0.053	0.830
ISA→IDS	**0.637**	0.065	9.772	**0.000**	0.508	0.766
COV	**-0.148**	0.069	-2.145	**0.034**	-0.284	-0.011

3.1.2. Mediation analysis

Next, Table 3 presents the regression model for PDC predictors. The relationship between IDS and PDC was negative and significant (β=-0.300, SE=0.066, p<0.001, 95% CI [-0.431, -0.169]), suggesting that an intuitive approach to decision-making reduces employees' intention to detect phishing attempts. This finding contradicts Hypothesis 3 (H3), which posited a positive effect of IDS on PDC. The direct effect of ISA on PDC was positive and significant (β=0.266, SE=0.099, p=0.008, 95% CI [0.070, 0.462]), supporting Hypothesis 2 (H2).

Table 3. Regression model for PDC predictor

Variable	Coefficient	SE (HC4)	t	p-value	LLCI	ULCI
Constant	3.604	0.211	17.093	0.000	3.186	4.022
ISA→PDC	**0.266**	**0.099**	2.688	**0.008**	**0.070**	**0.462**
IDS→PDC	**-0.300**	**0.066**	-4.540	**0.000**	**-0.431**	**-0.169**
PEK→PDC	0.250	0.134	1.860	0.065	-0.016	0.516
ISA×PEK	0.185	0.153	1.212	0.228	-0.117	0.487
IDS×PEK	-0.305	0.155	-1.971	0.051	-0.612	-0.002
COV	0.051	0.062	0.833	0.407	-0.071	0.174

3.1.3. Moderation analysis

To further explore this moderating effect, Table 4 presents the Johnson-Neyman analysis, which identifies the range of PEK levels at which IDS significantly affects PDC. The results indicate that IDS negatively affects PDC at moderate and high levels of PEK (p<0.05), meaning that individuals with higher PEK are more likely to experience a stronger negative effect of intuitive decision-making on PDC. However, at low levels of PEK (p=0.560), the effect of IDS on PDC becomes non-significant, suggesting that when phishing knowledge is minimal, intuitive decision-making does not significantly impact PDC. These findings confirm that the moderating role of PEK influences how IDS affects PDC, further validating H5.

Table 4. Johnson-Neyman test: significant moderation range of PEK

PEK level	Effect of IDS→PDC	SE (HC4)	t	p-value	LLCI	ULCI
-0.720	-0.081	0.138	-0.585	**0.560**	-0.353	0.192
0.000	-0.300	0.066	-4.540	0.000	-0.431	-0.169
0.720	-0.520	0.121	-4.298	**0.000**	-0.759	-0

3.1.4. Moderated mediation analysis

To further explore the interplay between ISA, IDS, PEK, and PDC, we conducted a moderated mediation analysis using PROCESS Model 15 by Hayes (2022). The analysis examined whether the indirect effect of ISA on PDC via IDS was contingent upon varying levels of PEK. The results confirmed that the indirect effect of ISA on PDC is moderated by PEK at moderate and high levels, supporting H4.

Table 5 highlights the conditional direct effects of ISA on PDC, demonstrating that the direct relationship strengthens as PEK increases. The index of moderated mediation in this finding confirms that PEK significantly moderates the indirect relationship between ISA and PDC via IDS.

The results in Table 6 show that the indirect effect of ISA on PDC through IDS is not significant at low levels of PEK (-0.720) as the confidence interval includes zero. However, the effect becomes significant at moderate (0.000) and high (0.720) levels of PEK, indicating that as employees' PEK increases, the negative influence of IDS on PDC strengthens.

Table 5. Conditional direct effects of ISA on PDC at different levels of PEK

PEK level	Direct effect of IDS→PDC	SE (HC4)	t	p-value	95% CI (LLCI, ULCI)
-0.720	0.133	0.128	1.037	0.302	[-0.121, 0.387]
0.000	0.266	0.099	2.688	0.008	[0.070, 0.462]
0.720	0.399	0.165	2.416	0.017	[0.072, 0.726]

Table 6. Conditional indirect effects of ISA on PDC via IDS at different levels of PEK

PEK level	Indirect effect of IDS→PDC	BootSE	95% CI (BootLLCI, BootULCI)
-0.720	-0.051	0.090	[-0.247, 0.112]
0.000	**-0.191**	**0.052**	**[-0.304, -0.103]**
0.720	-0.331	0.084	[-0.516, -0.188]

3.2. Discussion

The findings provide insights into the interplay between ISA, intuitive decision-making, and phishing detection. The positive relationship between ISA and IDS (H1) aligns with prior research suggesting that individuals with greater security awareness tend to rely more on intuition when making security-related decisions [3]. Similarly, the positive effect of ISA on PDC (H2) is consistent with earlier studies indicating that security awareness enhances phishing threat detection [15]. In quantitative terms, our study found a strong positive effect of ISA on IDS (β=0.637, $p<0.001$) and a significant direct effect of ISA on PDC (β=0.266, p=0.008). These magnitudes are broadly consistent with yet distinctive from prior studies: Sturman *et al.* [4] reported a smaller ISA–PDC effect ($\beta\approx0.18$) in a student sample, while Naga *et al.* [3] found a lower ISA–IDS association (r=0.52) among Filipino employees, suggesting context-dependent variation in effect magnitude.

These results underscore that security awareness training must be complemented by enforcement mechanisms and organizational policies. Alshammari and Al-Mamary [16] similarly highlighted the necessity of integrating awareness with administrative measures, while Sari *et al.* [17] found that awareness of policies did not guarantee compliant behavior without clear sanctions, a pattern echoed in our data where ISA positively influences PDC but requires structural reinforcement.

Contrary to expectations, the IDS–PDC relationship was negative (H3), indicating that intuitive decision-makers may struggle to accurately detect phishing attempts. This finding diverges from literature that associates intuition with efficient risk assessment [18], and suggests that phishing attacks are specifically designed to exploit intuitive thinking through heuristics and psychological triggers such as urgency or familiarity [19], [20]. Zulauf and Wagner [21] note that intuitive decision-making involves unconscious processing without clear reasoning, which may explain susceptibility to misleading phishing cues. Findings from Sirawongphatsara *et al.* [22] reinforce this argument, as their comparative simulation demonstrated that employees without prior cybersecurity training were more susceptible to phishing, and that targeted training interventions significantly reduced susceptibility. Behavioral intention to detect phishing threats can be enhanced by equipping individuals with both technological tools and cognitive skills to identify fraudulent messages [23]. Numerically, the negative IDS–PDC effect (β=-0.300, $p<0.001$) is stronger than Sturman *et al.* [4] ($\beta\approx$-0.19) and markedly different from Brickley [5], who found no significant effect (β=-0.09, p=0.21), suggesting that intuitive bias may be amplified in non-Western, less-institutionalized cybersecurity environments.

The significant moderation of PEK on the IDS–PDC relationship (H5) confirms that employees with higher phishing knowledge are better equipped to counteract the negative influence of intuition [24]. Conversely, the non-significant moderation of PEK on the ISA–PDC relationship (H4) suggests that awareness and knowledge operate as independent predictors rather than interacting constructs, implying that organizations should design distinct training approaches for each, general awareness programs to cultivate vigilance, and knowledge-based interventions to build concrete detection skills [25]. Given the increasing sophistication of phishing tactics, organizations should adopt an integrated approach combining user education with automated detection mechanisms, as mitigating phishing risks requires both human vigilance and advanced threat intelligence systems [26].

Generational analysis revealed that Gen Z and Millennial employees showed higher PDC mean scores (M=3.89, SD=0.61) compared to Generation X and Baby Boomers (M=3.54, SD=0.74), consistent with Sari *et al.* [17]. Respondents with higher phishing knowledge (PEK$\geq$+0.72 SD) also demonstrated stronger mitigation of the negative IDS effect (β=-0.331, 95% CI [-0.516, -0.188]), reinforcing the need for demographically tailored training programs. Several limitations should be noted: the single-site sampling design limits generalizability, self-reported measures introduce common method bias risk, the cross-sectional design precludes causal inference, and environmental factors such as organizational security culture were not controlled. Future studies should employ multi-site, longitudinal, or experimental designs to enhance validity.

Theoretically, the negative IDS–PDC relationship challenges dual-process assumptions in cybersecurity contexts. Practically, organizations should implement multi-layered training, including phishing simulations and demographic-tailored interventions, to counteract intuitive biases and strengthen detection confidence across generational cohorts.

4. CONCLUSION

This study has provided valuable insights into the relationships between ISA, IDS, PEK, and PDC. The results confirm that security awareness positively influences both intuitive decision-making and PDC, reinforcing the need for strong cybersecurity education. However, the negative effect of IDS on PDC suggests that reliance on intuition alone may reduce the accuracy of phishing detection. Additionally, phishing knowledge plays a crucial moderating role, particularly in mitigating the risks associated with intuitive decision-making.

Organizations should adopt a multi-faceted approach to cybersecurity training, combining awareness programs with hands-on phishing simulations to enhance detection skills. Additionally, businesses and institutions should consider integrating phishing detection tools that complement human vigilance, ensuring a holistic defense strategy. Furthermore, differences in generational background and PEK levels suggest that organizations should tailor their cybersecurity training strategies to accommodate different demographic groups. This targeted approach can improve overall awareness and better equip employees to recognize and mitigate phishing threats effectively.

Future research should examine additional psychological and contextual factors that may affect phishing susceptibility, such as cognitive load, stress, or individual risk perception. Expanding the study to different organizational contexts and cultures could also provide broader generalizability. The limitations of this study employed a single-site sampling approach, focusing solely on employees within one institution, which limits the external validity of the findings. Additionally, the reliance on self-reported measures introduces the possibility of response bias. Future studies should incorporate experimental or behavioral observation methods to strengthen the reliability of the results.

ACKNOWLEDGMENTS

The authors would like to sincerely thank XYZ University in Indonesia for providing the necessary support and resources to conduct this research. Special appreciation is extended to all employees who participated in the survey, contributing valuable insights to this study. The authors also acknowledge the guidance and constructive feedback provided by the research supervisors, which greatly improved the quality of this work. Lastly, appreciation is given to family and colleagues for their continuous encouragement throughout this research journey.

FUNDING INFORMATION

Authors state no funding involved. This research did not receive any specific research grant or contract from funding agencies in the public, commercial, or not-for-profit sectors.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Muh. Bafadhal Kurnia Alamsyah	✓	✓		✓	✓	✓		✓	✓					
Candiwan		✓		✓	✓	✓				✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest. The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

DATA AVAILABILITY

The data that support the findings of this study are available from the first author and the corresponding author, MBA, upon reasonable request. The data, which contain information that could compromise the privacy of research participants, are not publicly available due to certain restrictions.

REFERENCES

[1] K. Okokpujie, C. G. Kennedy, K. Nnodu, and E. Noma-Osagha, "Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University)," *International Journal of Sustainable Development and Planning*, vol. 18, no. 1, pp. 255–263, Jan. 2023, doi: 10.18280/ijsdp.180127.

[2] R. B. Permadi and K. Ramli, "Analysis of Measuring Information Security Awareness for Employees at Institution XYZ," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 4, no. 4, pp. 1330–1338, Jul. 2024, doi: 10.57152/malcom.v4i4.1453.

[3] J. F. Naga *et al.*, "Investigating the Relationship Between Personality Traits and Information Security Awareness," *International Journal of Computing and Digital Systems*, vol. 15, no. 1, pp. 1233–1246, Sep. 2024, doi: 10.12785/ijcds/160191.

[4] D. Sturman, J. C. Auton, and B. W. Morrison, "Security awareness, decision style, knowledge, and phishing email detection: Moderated mediation analyses," *Computers & Security*, vol. 148, Jan. 2024, doi: 10.1016/j.cose.2024.104129.

[5] J. Brickley, "What Drives User Retrospective Confidence Levels Towards Phishing Detection Behavior," *ResearchGate*, 2022, doi: 10.13140/RG.2.2.31741.44002.

[6] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Frontiers in Computer Science*, vol. 3, Mar. 2021, doi: 10.3389/fcomp.2021.563060.

[7] J. W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 3rd ed. SAGE Publications, 2009.

[8] U. Sekaran and R. Bougie, *Research Methods for Business: A Skill-Building Approach. 7th Edition*. Wiley & Sons, West Sussex., 2016.

[9] M. A. Brahimi and T. Leperlier, "Quantitative Methods in Intellectual History," The Routledge Handbook of the History and Sociology of Ideas, Routledge, 2023, doi: 10.4324/9781003093046-8ï.

[10] A. L. E. Esquivel, "Operationalization of research variables," *CISA*, vol. 5, no. 5, 2023, doi: 10.58299/cisa.v5i5.35.

[11] C. Andrade, "A Student's Guide to the Classification and Operationalization of Variables in the Conceptualization and Design of a Clinical Study: Part 1," *Indian Journal of Psychological Medicine*, vol. 43, no. 2, pp. 177–179, Mar. 2021, doi: 10.1177/0253717621994334.

[12] J.-H. Huang, C.-H. H. Yang, P.-Y. Chen, M.-H. Chen, and M. Worring, "Causalainer: Causal Explainer for Automatic Video Summarization," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pp. 2630–2636, 2023, doi: 10.1109/CVPRW59228.2023.00262.

[13] A. F. Hayes, "An Index and Test of Linear Moderated Mediation," *Multivariate Behavioral Research*, vol. 50, no. 1, pp. 1–22, Jan. 2015, doi: 10.1080/00273171.2014.962683.

[14] A. Alfons, N. Y. Ateş, and P. J. F. Groenen, "A Robust Bootstrap Test for Mediation Analysis," *Organizational Research Methods*, vol. 25, no. 3, pp. 591–617, Jul. 2022, doi: 10.1177/1094428121999096.

[15] R. Fadlika, Y. Ruldeviyani, Z. T. Butarbutar, R. A. Istiqomah, and A. A. Fariz, "Employee Information Security Awareness in the Power Generation Sector of PT ABC," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, pp. 594–603, 2023, doi: 10.14569/IJACSA.2023.0140465.

[16] M. M. Alshammari and Y. H. Al-Mamary, "Bridging Policy and Practice: Integrated Model for Investigating Behavioral Influences on Information Security Policy Compliance," *Systems*, vol. 13, no. 8, pp. 1-31, Aug. 2025, doi: 10.3390/systems13080630.

[17] P. K. Sari, J. Sutanto, P. W. Handayani, and A. N. Hidayanto, "Information Security Behavior of Healthcare Professionals when There is Poor Health Information Security Policy," in *Proceedings - 28th Pacific Asia Conference on Information Systems (PACIS)*, 2024.

[18] C. Julmi, "When rational decision-making becomes irrational: a critical assessment and re-conceptualization of intuition effectiveness," *Business Research*, vol. 12, no. 1, pp. 291–314, Apr. 2019, doi: 10.1007/s40685-019-0096-4.

[19] K. Darabos, "Intuitive Decision: When to Begin the Succession Process," *Corvinus Journal of Sociology and Social Policy*, vol. 13, no. 2, pp. 79–105, 2022, doi: 10.14267/CJSSP.2022.2.4.

[20] R. Montañez, E. Golob, and S. Xu, "Human Cognition Through the Lens of Social Engineering Cyberattacks," *Frontiers in Psychology*, Sep. 30, 2020, doi: 10.3389/fpsyg.2020.01755.

[21] K. Zulauf and R. Wagner, "Intuitive and Deliberative Decision-Making in Negotiations," *Management Dynamics in the Knowledge Economy*, vol. 9, no. 3, pp. 293–306, Sep. 2021, doi: 10.2478/mdke-2021-0020.

[22] P. Sirawongphatsara, P. Pornpongtechavanich, N. Phanthuna, and T. Daengsi, "Comparative simulation of phishing attacks on a critical information infrastructure organization: an empirical study," *Bulletin of Electrical Engineering and Informatics*, vol. 14, no. 2, pp. 1526–1534, Apr. 2025, doi: 10.11591/eei.v14i2.8020.

[23] N. Pawar and P. A. Tijare, "A Review on Phishing Website Detection Using Machine Learning Approach," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 267–272, Apr. 2023, doi: 10.32628/cseit2390227.

[24] J. S. Tharani and N. A. G. Arachchilage, "Understanding Phishers' Strategies of Mimicking URLs to Leverage Phishing Attacks: A Machine Learning Approach," *Security and Privacy*, vol. 3, no. 5, pp. 1–14, 2020, doi: 10.1002/spy2.120.

[25] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching johnny not to fall for phish," *ACM Transactions on Internet Technology (TOIT)*, vol. 10, no. 2, May 2010, doi: 10.1145/1754393.1754396.

[26] A. E. Schutz and T. Fertig, "The Forgotten Model – Validating the Integrated Behavioral Model in Context of Information Security Awareness," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2023, pp. 6841–6850, doi: 10.24251/hicss.2023.828.

BIOGRAPHIES OF AUTHORS

Muh. Bafadhal Kurnia Alamsyah is an undergraduate student in Business Management of Telecommunications and Informatics at the Faculty of Economics and Business, Telkom University, Bandung, Indonesia. His research interests include information security, information security behavior, and information security management system (ISMS). He can be contacted at email: alamsyahbafadhal@student.telkomuniversity.ac.id.

Candiwan is a Lecturer and Researcher at the Faculty of Economics and Business, Telkom University, Indonesia, where he has been a faculty member since 2013. From 2015-2018, he also served as an Analyst Planning at Yayasan Pendidikan Telkom (YPT). He graduated with a Bachelor's degree in Physical Engineering from Bandung Institute of Technology (ITB) and later obtained his Master's degree in Information and Communication Technology from the University of Wollongong, Australia. From 1991 to 2013, he worked as a practitioner in a telecommunication company. He is also a Certified Lead Auditor for ISO 27001, information security management system (ISMS). His research interests include information security, information security behavior, information security management systems (ISMS), information risk management, technology adoption, and information technology governance. His research works have been published in Scopus-indexed journals, with 30 documents and a Scopus H-index of 8. He received a certificate of best paper award from the 24 IEEE International Conference on Computing conducted on 12th – 14th December 2024 at Kuala Lumpur. He can be contacted at email: candiwan@telkomuniversity.ac.id.