Journal of Soft Computing Exploration
Homepage: htttps://shmpublisher.com/index.php/joscex
p-ISSN: 2746-7686
e-ISSN: 2746-0991

.

Information security awareness among students in eastern indonesia: A HAIS-Q based assessment and intervention priority mapping

Muhammad Fadlan[1], Syarifah[2], Denis Prayogi[3], Suprianto[4]
[1,4]Information System Study Program, STMIK PPKIA Tarakanita Rahmawati, Indonesia
[2]Retail Management Study Program, Universitas Amal Ilmiah Yapis Wamena, Indonesia
[3]Informatics Engineering Study Program, STMIK PPKIA Tarakanita Rahmawati, Indonesia

Article Info

Article history:

Received April 12, 2026
Revised June 15, 2026
Accepted July 4, 2026

Keywords:

Awareness
Information security
Eastern indonesia
HAIS-Q
Intervention mapping

ABSTRACT

The increasing use of digital technology among university students is not always accompanied by adequate levels of information security awareness, especially in Eastern Indonesia, which has its own characteristics and challenges regarding facilities and digital literacy. This study aims to assess students' information security awareness using an adapted HAIS-Q and to provide a soft computing-oriented interpretation for mapping intervention priorities. A quantitative survey was conducted involving students from Universitas Amal Ilmiah Yapis Wamena. The instrument measured three awareness dimensions, namely knowledge, attitude, and behaviour, across five focus areas. The results show that students' information security awareness is generally in the good category, with attitude obtaining the highest score of 81.44, followed by knowledge at 80.10, and behaviour at 75.04. At the focus area level, mobile device security achieved the highest mean score, while email security obtained the lowest. The distribution of awareness levels shows that 60% of respondents were in the good category, 33% in the average category, and 7% in the poor category. From a soft computing perspective, these results can be interpreted as input indicators for mapping intervention priorities, particularly by identifying behaviour-related weaknesses, vulnerable awareness groups, and specific security domains requiring improvement.

Corresponding Author:

Muhammad Fadlan,
Information System Study Program,
STMIK PPKIA Tarakanita Rahmawati,
99 Halmahera Street, Oval Ladang IV, Tarakan, North Kalimantan, Indonesia.
Email: fadlan@ppkia.ac.id
https://doi.org/10.52465/joscex.v7i3.52

1. INTRODUCTION

Digital transformation in higher education has increased the use of academic information systems, e-learning platforms, artificial intelligence, and cloud-based services [1], [2], [3]. Although these technologies support more adaptive academic services, they also increase exposure to information security threats, including hacking, phishing, data breaches, and social engineering [4], [5]. Universities are potential targets because they

manage large volumes of academic and personal student data. Therefore, information security in higher education should not rely only on technical safeguards but also on user awareness and secure behaviour [6], [7], [8]. Information security does not depend solely on technological factors, but also on users' awareness of the technology [9], [10], [11].

Many studies show that the human is the main cause of information security breaches and is considered one of the weakest links in information security [12], [13], [14]. One way to address this threat is to increase user awareness of the importance of information security in today's digital era. Information Security Awareness is a crucial aspect in ensuring information security in the digital era, reflecting individuals' levels of understanding, attitudes, and behaviors in facing various security threats [15]. Low levels of information security awareness can certainly give rise to various risks and threats, such as data leaks and account misuse [16], [17]. Previous studies have shown that human factors remain a critical weakness in information security, making awareness measurement an important step in reducing user-related security risks [18], [19]. Students are characterized by intensive technology use, but this is not always accompanied by adequate security awareness. This underscores the importance of studying information security awareness in higher education, especially among students.

Research on information security awareness in the current era of digital transformation is generally conducted in higher education settings located in urban areas with adequate technological infrastructure [20], [21], [22]. Limited attention has been given to universities located in geographically remote regions where digital literacy levels, technology adoption, and access to information infrastructure may differ significantly. In Indonesia, empirical evidence on students' information security awareness in Eastern regions remains scarce. Therefore, further investigation is needed to assess information security awareness among university students in Eastern Indonesia using a structured measurement instrument such as the Human Aspects of Information Security Questionnaire (HAIS-Q). The HAIS-Q has been widely adopted in various previous studies due to its ability to evaluate user knowledge, attitudes, and behavior toward information security [23], [24], [25], [26], [27]. Furthermore, most studies are conducted in urban contexts and technology-rich environments with adequate digital infrastructure, which indicates that existing findings largely reflect conditions in settings with relatively high levels of digital literacy and access to technology [15], [22], [24], [25], [28], [29].

These studies primarily focus on institutions with relatively mature digital infrastructures. However, in areas with special characteristics, such as Wamena, Jayawijaya Regency, Papua Mountains Province, which is included in the 3T (frontier, outermost, and underdeveloped) category, there are certainly different challenges, both in terms of limited infrastructure, technological access, and variations in the level of digital literacy of its residents. These conditions can affect users' understanding and behavior in maintaining information security. Therefore, research on information awareness in Eastern Indonesia, such as Wamena, is important to provide a more contextual picture and to address the limitations posed by research that has predominantly studied urban areas.

The use of HAIS-Q in this study will provide empirical evidence on student information security awareness in Eastern Indonesia. Different from previous studies that mainly report awareness scores descriptively, this study further positions the awareness results as input indicators for soft computing-oriented intervention mapping. The scores obtained from the knowledge, attitude, and behaviour dimensions, as well as the HAIS-Q focus areas, are interpreted to identify priority areas for improving information security awareness.

2. METHOD

The research flow consisted of six main stages: problem identification, literature review, instrument adaptation, questionnaire development, data collection, and awareness level analysis, as shown in Figure 1. These stages were designed to ensure that the HAIS-Q-based instrument, data collection process, and descriptive analysis were conducted systematically.

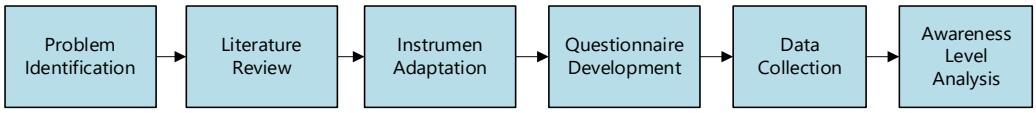

Figure 1. Research methodology

Research Design and Sample

This study used a quantitative survey-based approach to measure information security awareness among university students, as this approach is commonly used to obtain empirical awareness profiles from questionnaire-based data [7], [21], [30]. The population in this study was students at Universitas Amal Ilmiah Yapis Wamena. The sample consisted of 100 students who voluntarily completed the online questionnaire. A convenience sampling technique was used because it allows researchers to collect data from respondents who are accessible and willing to participate, particularly in field-based survey conditions. This approach was selected to obtain a numerical overview of students' awareness based on their responses to the adapted HAIS-Q instrument.

Research Instrument

The instrument was adapted from the HAIS-Q, which measures information security awareness through three dimensions: knowledge, attitude, and behaviour [23], [24], [26]. This study used a simplified version of the HAIS-Q to improve clarity and relevance to the student context while maintaining its core conceptual structure. Five focus areas were included: password management, email security, internet usage, social media usage, and mobile device security, as shown in Figure 2. Each focus area consisted of six statements, comprising two knowledge items, two attitude items, and two behaviour items, resulting in 30 questionnaire items. All items were measured using a five-point Likert scale ranging from strongly disagree (1) to strongly agree (5).

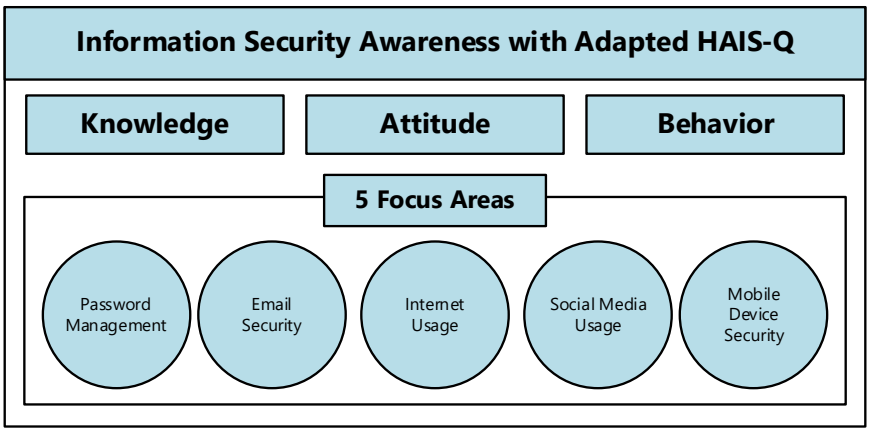

Figure 2. Adapted conceptual HAIS-Q framework

Data Collection Procedure

Data collection was conducted using Google Forms. The questionnaire was distributed to students via social media platforms such as WhatsApp. In this study, respondents were asked to complete the questionnaire voluntarily. Before completing the questionnaire, they were given a brief explanation of the research objectives and assured that the collected data would be anonymous and used solely for academic purposes. This was done to increase respondents' trust in the questionnaire and encourage more honest responses.

Data Analysis

The collected data were analyzed using descriptive statistics. Validity testing was conducted using item-total correlation, while reliability was assessed using Cronbach's Alpha. After the instrument was considered valid and reliable, mean scores were calculated for the knowledge, attitude, and behaviour dimensions and for each HAIS-Q focus area. Awareness scores were then converted into three categories: poor (0–59), average (60–79), and good (80–100) [15]. This analysis aimed to provide a clearer picture of respondents' overall awareness.

Soft Computing-Oriented Awareness Mapping

The descriptive awareness results were further interpreted using a soft computing-oriented rule-based perspective to map intervention priorities. The knowledge, attitude, and behaviour dimensions, the five HAIS-Q focus areas, and the awareness level categories were treated as input indicators. Intervention priorities were determined by identifying the lowest KAB dimension, the lowest focus area, and the proportion of respondents in each awareness category. Conceptually, the mapping represents awareness indicators as linguistic categories such as low, moderate, and high, which are then linked to intervention priorities. Although this study does not implement a complete fuzzy inference or predictive model, this interpretation provides an initial basis for future fuzzy logic, clustering, classification, or recommendation-based awareness models.

3. RESULTS AND DISCUSSIONS

Respondent Characteristics

This study involved 100 students from UNAIM Yapis Wamena who completed the questionnaire. Respondent characteristics were analysed by gender, academic year, internet usage, and experience with digital security training. This analysis was conducted to provide an initial overview of the respondents' conditions, representing students in Eastern Indonesia. The results of the analysis of these respondent characteristics are shown in Table 1.

Table 1. Respondent characteristics

Characteristics	Category	Frequency	Percentage (%)
Gender	Male	62	62%
	Female	38	38%
Year of Enrollment	< 2022	20	20%
	2022	11	11%
	2023	25	25%
	2024	20	20%
	2025	24	24%
Internet Usage	< 2 hours	16	16%
	2-4 hours	28	28%
	5-7 hours	22	22%
	> 7 hours	34	34%
Security Training	Ever attended	16	16%
	Never attended	84	84%

Table 1 shows that most respondents were male (62%), while the largest enrollment group came from the 2023 cohort (25%). Most respondents used the internet for more than seven hours per day (34%), but 84% had never attended digital security training. This indicates a potential gap between intensive technology use and formal exposure to information security training.

Reliability and Validity Test

Based on the test results, a Cronbach's Alpha reliability value of 0.963 was obtained for 30 statement items, as seen in Table 2.

Table 2. Reliability test result

Variable	Cronbach's Alpha	Number of Items
Information Security Awareness	0.963	30

This value indicates that the instrument has a very high level of reliability. This indicates that all items in the questionnaire have good consistency in measuring respondents' information security awareness, making it suitable for further analysis. Furthermore, the validity test was conducted by comparing each item's correlation value with the r-table value, as shown in Table 3. Based on the number of respondents (100), the r-table value was 0.197. The test results showed that all items had correlation values higher than the r-table, with a range of 0.417 to 0.838, as shown in Table 3. These results indicate that all items in the questionnaire are valid and can be used for further analysis, namely, information security awareness.

Table 3. Validity test summary

Indicator	Minimum r-value	Maximum r-value	r-table	Result
All Items (P1–P30)	0.417	0.838	0.197	Valid

Information Security Awareness Analysis by K-A-B Dimension

The analysis of information security awareness was conducted across three main dimensions: knowledge, attitude, and behaviour. The calculation results for each dimension are presented in Figure 3. Based on the results in Figure 3, the attitude dimension has the highest score of 81.44, followed by knowledge at 80.10, and behaviour at 75.04. From these results, all three dimensions show a relatively high level of awareness, with scores ranging from 0 to 100. However, there is a significant difference between the attitude and behaviour dimensions, indicating that a positive attitude towards information security has not been fully reflected in daily behaviour. This finding indicates that respondents tend to have a good level of knowledge and attitude, but this has not been fully reflected in consistent behaviour to maintain information security. This

difference indicates a gap between understanding and implementation in daily practice, so more targeted efforts are needed to encourage changes in behaviour towards awareness of information security, rather than simply increasing knowledge and attitudes.

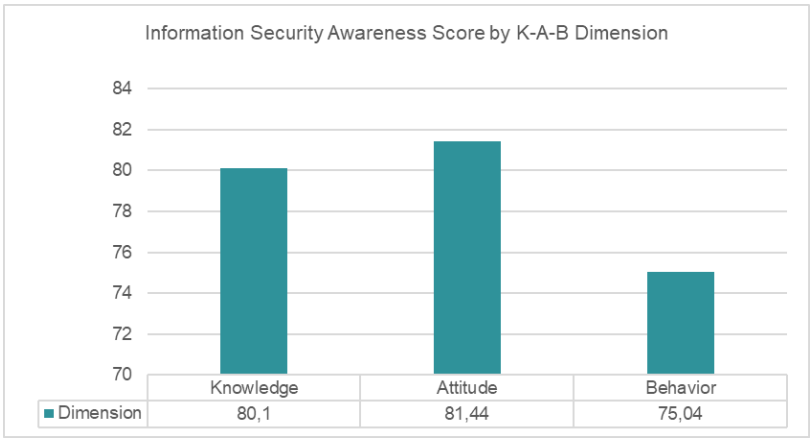

Figure 3. Information security awareness score by K-A-B dimension

Information Security Awareness Analysis by Focus Area

In addition to the dimensions, analysis was also conducted on the five main areas of the HAIS-Q: password management, email security, internet usage, social media usage, and mobile device security. The measurement results for each area are presented as a profile, as shown in Figure 4.

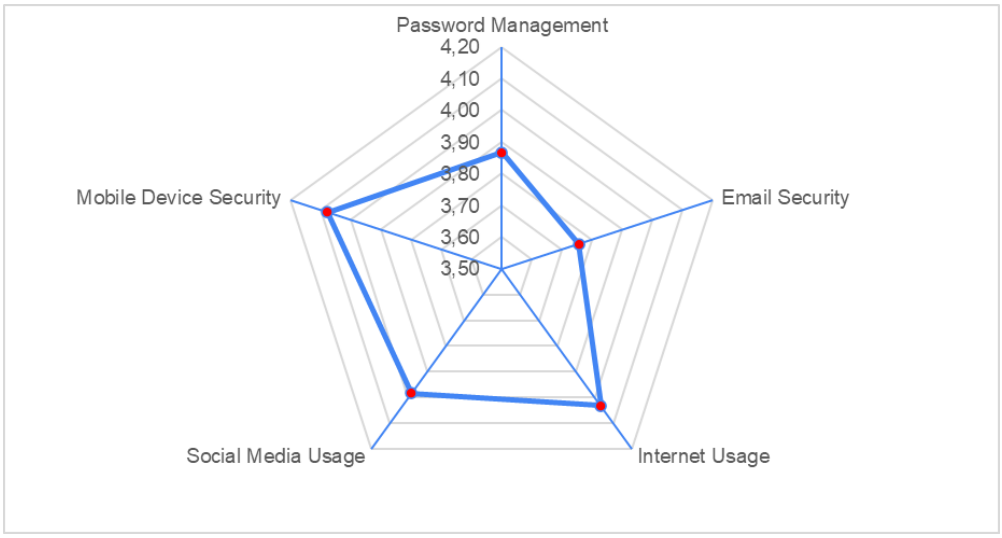

Figure 4. Information security awareness profile by 5-focus area

Based on Figure 4, all areas show average values in the high category. Mobile device security has the highest average value of 4,077, followed by internet usage at 4,032 and social media usage at 3,983. Meanwhile, password management has a value of 3,867, and email security has the lowest value at 3,757. The pattern shown in Figure 4 indicates that students' information security awareness is uneven across all HAIS-Q aspects. A low score on email security indicates potential vulnerabilities, particularly against threats such as phishing and social engineering-based emails. Conversely, a high score on mobile device security indicates that students are more aware of and apply security practices when using their mobile devices. The high intensity of mobile device use in daily activities likely influences this. These findings indicate that students in Eastern Indonesia generally have a high level of awareness. However, there are still certain areas that require more attention, especially those related to digital communication security.

Information security awareness levels were also analysed by classifying respondents into three categories: poor, average, and good, based on scores converted to a scale of 0-100. The distribution of respondents' awareness levels is presented in Figure 5. Based on the results in Figure 5, the majority of respondents are in the good category, at 60%. Meanwhile, 33% of respondents are in the average category, and another 7% are in the poor category. These findings indicate that although the majority of students have a good level of information security awareness, a significant proportion falls into the average category. Furthermore,

the presence of respondents in the poor category indicates a potentially highly vulnerable group to information security risks. For students in Eastern Indonesia, these results indicate that information security awareness is not yet fully distributed. Therefore, more targeted improvement efforts are needed, particularly to encourage a shift from the average to the good category and reduce the number of groups with low levels of awareness.

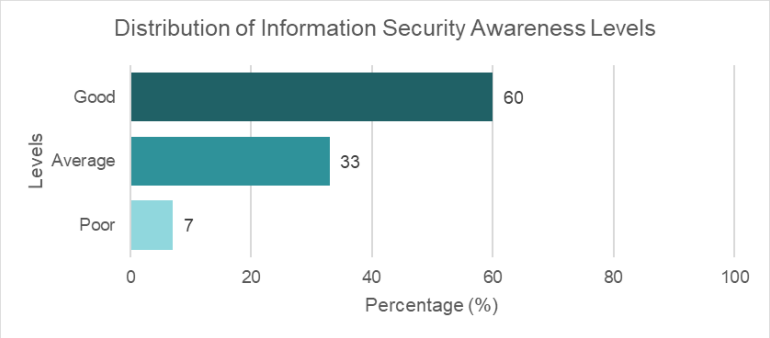

Figure 5. Distribution of levels

Soft Computing-Oriented Interpretation of Awareness Results

The awareness results were further interpreted using a soft computing-oriented perspective to identify intervention priorities. As summarized in Table 4, the lowest score in the behaviour dimension indicates a gap between students' knowledge and attitudes and their actual security practices, suggesting a high priority for behaviour-oriented awareness programs. Similarly, email security obtained the lowest score among the HAIS-Q focus areas, indicating the need for targeted interventions related to phishing awareness, suspicious links, social engineering, and secure email usage.

Table 4. Soft computing-oriented intervention mapping based on HAIS-Q results

Finding	Soft Computing-Oriented Interpretation	Intervention Priority
Behaviour obtained the lowest KAB score	An awareness-practice gap exists because positive knowledge and attitude are not fully reflected in daily security behaviour	High
Email security obtained the lowest focus area score	Students may be more vulnerable to phishing, suspicious links, unsafe attachments, and social engineering-based email attacks	High
33% of respondents were in the average category	Students need reinforcement programs to improve consistency in applying secure practices	Medium
7% of respondents were in the poor category	Students need intensive, practical, and targeted awareness training	High
Mobile device security obtained the highest score	Awareness in this area is relatively established and can be maintained through periodic reminders	Low

The distribution of awareness levels also provides useful input for intervention mapping. Students in the average and poor categories represent priority groups for reinforcement and intensive awareness programs, whereas students in the good category mainly require maintenance activities. In contrast, the relatively high score for mobile device security suggests that awareness in this area is already well established. Overall, the intervention mapping presented in Table 4 highlights three main priorities: improving security behaviour, strengthening email security awareness, and focusing awareness programs on students with average and poor awareness levels. These findings demonstrate how HAIS-Q-based descriptive results can be extended into a soft computing-oriented decision-support perspective and provide a foundation for future fuzzy rule-based or machine learning-based awareness models.

Discussion

The results of this study indicate that students' information security awareness is generally in the good category, across the dimensions of knowledge, attitude, and behaviour. However, several important patterns emerged that warrant further attention. The first finding is a clear gap between the attitude and behaviour dimensions. Although respondents expressed a positive attitude toward the importance of information security, this attitude did not fully translate into their actual behaviour. This finding indicates that understanding and awareness do not automatically lead to the implementation of information security awareness practices in their daily lives. Students tend to know and agree with information security principles, but do not consistently apply

them. This phenomenon aligns with the idea that increased knowledge does not always translate into behavioural change, particularly in the context of information security, which is heavily influenced by individual habits.

The second finding, analysis based on focus areas, shows that awareness levels are uneven across all aspects. This is evident in the focus areas of mobile device security and internet usage, which scored higher than other areas, while email security scored lowest across several other aspects. This situation indicates that students are more familiar with security practices on devices frequently used in daily activities, such as smartphones, but pay less attention to the security aspects of email-based communications. Yet, email is a key vulnerability in frequent information security attacks, such as phishing and social engineering. Low awareness in this area is a potential weak point that irresponsible parties could exploit.

The third finding, the distribution of awareness levels, shows that although the majority of respondents fall into the good category, significant proportions are in the average and poor categories. This indicates that information security awareness levels are not evenly distributed across the student population. The presence of groups with lower levels of awareness indicates potential vulnerabilities that cannot be ignored, especially in an academic environment that is increasingly dependent on digital systems and technology. For students in Eastern Indonesia, this finding becomes even more relevant. The high intensity of digital technology use, unbalanced by an equitable understanding and practice of information security, can increase the risk of various cyber threats.

From a soft computing perspective, the HAIS-Q results can be used as decision-support indicators for identifying intervention priorities. The lower behaviour score indicates a need for behaviour-focused programs, while the lower email security score highlights a priority area for improvement. Although no AI or machine learning model was implemented, these findings provide a foundation for future fuzzy logic, clustering, classification, or recommendation-based approaches to support more adaptive information security awareness programs. Furthermore, limited access to formal training or education related to information security may also be a contributing factor. The implications of this research confirm that efforts to increase information security awareness should not focus solely on improving knowledge and attitudes, but also on actual behavioural changes in each individual. Education and training programs need to be designed in a more practical, context-specific manner, emphasising hands-on practice and relevant threat simulations, particularly in areas of weakness, such as email security. Furthermore, a more targeted approach is needed to reach student groups with average and poor levels of awareness, thus creating a more equitable level of awareness among students.

4. CONCLUSION

This study shows that information security awareness among students in Eastern Indonesia is generally in the good category. The attitude dimension achieved the highest score (81.44), followed by knowledge (80.10), while behaviour recorded the lowest score (75.04), indicating an awareness-practice gap. Across HAIS-Q focus areas, mobile device security obtained the highest score, whereas email security scored the lowest, highlighting the need for greater attention to phishing and social engineering threats. Overall, 60% of respondents were in the good category, 33% in the average category, and 7% in the poor category. From a soft computing-oriented perspective, behaviour weaknesses, low email security awareness, and the presence of average and poor awareness groups can serve as indicators for intervention priorities. These findings provide empirical evidence of information security awareness in Eastern Indonesia and offer a foundation for future fuzzy logic, clustering, classification, or machine learning-based awareness models.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge STMIK PPKIA Tarakanita Rahmawati and Universitas Amal Ilmiah Yapis Wamena for their support of this research. The authors also extend their sincere thanks to the respondents from Universitas Amal Ilmiah Yapis Wamena for their participation and valuable contribution to this study.

REFERENCES

[1] Helmiatin, A. Hidayat, and M. R. Kahar, "Investigating the adoption of AI in higher education: a study of public universities in Indonesia," *Cogent Education*, vol. 11, no. 1, 2024, doi: 10.1080/2331186X.2024.2380175.

[2] Q. Aini, A. Kurniawan, and T. Bina Sulistiyowati, "Digital Transformation: Best Practices of Educational Platform in Indonesia," *Jurnal Transformative*, vol. 10, no. 1, pp. 42–59, Mar. 2024, doi: 10.21776/ub.transformative.2024.010.01.3.

[3] Suwendi, Mesraini, C. B. Gama, H. Rahman, T. Luhuringbudi, and M. Masrom, "Adoption of Artificial Intelligence and Digital Resources among Academicians of Islamic Higher Education Institutions in Indonesia," *Jurnal Online Informatika*, vol. 10, no. 1, pp. 42–52, Apr. 2025, doi: 10.15575/join.v10i1.1549.

[4] N. Hakiem *et al.*, "ASSESSING CYBERSECURITY READINESS AMONG HIGHER EDUCATION INSTITUTIONS IN INDONESIA USING MANAGEMENT PERSPECTIVES," *ICIC Express Letters*, vol. 17, no. 10, pp. 1151–1158, Aug. 2023, doi: 10.24507/icicel.17.10.1151.

[5] B. Wibowo, N. Ibrahim, A. Yuswanto, and T. Hidayat, "Cyber Resilience to Digital Threats for Education Institutions 4.0," *International Journal of Management Science and Application*, vol. 4, no. 1, pp. 35–45, Jun. 2025, doi: 10.58291/ijmsa.v4i1.370.

[6] Y. Evitha, "Leading Digital Transformation: Strategies for Higher Education Leaders in Navigating Online Platforms, Administrative Services, and Cybersecurity," *Jurnal Pendidikan*, vol. 16, no. 2, pp. 2645–2656, 2024, doi: 10.35445/alishlah.v16i2.5614.

[7] Y. Kurniawan, S. I. Santoso, R. R. Wibowo, N. Anwar, G. Bhutkar, and E. Halim, "Analysis of Higher Education Students' Awareness in Indonesia on Personal Data Security in Social Media," *Sustainability (Switzerland)*, vol. 15, no. 4, Feb. 2023, doi: 10.3390/su15043814.

[8] G. M. W. Tangka and E. Y. Putra, "Classification of Indonesian Undergraduate Students' Awareness Level of Phishing Attacks using Decision Tree Algorithm," *Journal of Information System Research (JOSH)*, vol. 6, no. 4, pp. 1911–1919, Jul. 2025, doi: 10.47065/josh.v6i4.7859.

[9] K. Hughes-Lartey, M. Li, F. E. Botchey, and Z. Qin, "Human factor, a critical weak point in the information security of an organization's Internet of things," *Heliyon*, vol. 7, no. 3, Mar. 2021, doi: 10.1016/j.heliyon.2021.e06522.

[10] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, and H. Thapliyal, "A systematic literature review of cybersecurity scales assessing information security awareness," *Heliyon*, vol. 9, no. 3, Mar. 2023, doi: 10.1016/j.heliyon.2023.e14234.

[11] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review," May 01, 2022, *Elsevier B.V.* doi: 10.1016/j.compind.2022.103614.

[12] N. T. Mai and I. Khalid, "Human Error vs. System Security: Evaluating the Weakest Link in Digital Business Information Systems," *Journal of Management and Informatics*, vol. 4, no. 3, pp. 981–997, Dec. 2025, doi: 10.51903/jmi.v4i3.305.

[13] N. S. Sulaiman, M. A. Fauzi, W. Wider, J. Rajadurai, S. Hussain, and S. A. Harun, "Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review," Sep. 01, 2022, *MDPI*. doi: 10.3390/socsci11090386.

[14] M. Salam, K. A. Abu Bakar, A. T. Abdul Ghani, and A. H. Mohd Aman, "Cybersecurity in Higher Education Institutions Digitalisation: Addressing Threats and Vulnerabilities," Jan. 01, 2026, *SAGE Publications Inc.* doi: 10.1177/21582440251413473.

[15] 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.

[16] I. Hwang, R. Wakefield, S. Kim, and T. Kim, "Security Awareness: The First Step in Information Security Compliance Behavior," *Journal of Computer Information Systems*, vol. 61, no. 4, pp. 345–356, 2021, doi: 10.1080/08874417.2019.1650676.

[17] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, 2022, doi: 10.1080/08874417.2020.1712269.

[18] L. W. Wong, G. W. H. Tan, J. J. Hew, K. B. Ooi, and L. Y. Leong, "Mobile social media marketing: a new marketing channel among digital natives in higher education?," *Journal of Marketing for Higher Education*, vol. 32, no. 1, pp. 113–137, 2022, doi: 10.1080/08841241.2020.1834486.

[19] G. Janschitz and M. Penker, "How digital are 'digital natives' actually? Developing an instrument to measure the degree of digitalisation of university students – the DDS-Index," *BMS Bulletin of Sociological Methodology/ Bulletin de Methodologie Sociologique*, vol. 153, no. 1, pp. 127–159, Jan. 2022, doi: 10.1177/07591063211061760.

[20] Nurbojatmiko, A. Fajar Firmansyah, Q. Aini, A. Saehudin, and S. Amsariah, "Information Security Awareness of Students on Academic Information System Using Kruger Approach," in *2020 8th International Conference on Cyber and IT Service Management, CITSM 2020*, Institute of Electrical and Electronics Engineers Inc., Oct. 2020. doi: 10.1109/CITSM50537.2020.9268795.

[21] B. Setiawan and M. A. Rizal, "Measurement of Information Security and Privacy Awareness in College Students after the Covid-19 Pandemic," in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 1396–1403. doi: 10.1016/j.procs.2024.03.138.

[22] D. A. Perkasa and B. Setiawan, "Measuring Information Security Awareness Level of High School Students," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 4, no. 4, pp. 1301–1308, Jul. 2024, doi: 10.57152/malcom.v4i4.1461.

[23] S. F. Arum, A. Zubaidi, and R. B. Huwae, "Measuring Information Security Awareness Using HAIS-Q: Revealing the Gap between Students' Attitudes and Knowledge," *Jurnal Bumigora Information Technology (BITe)*, vol. 7, no. 2, pp. 83–94, 2025, doi: 10.30812/bite.v7i2.5430.

[24] F. N. Shakti and A. N. Hidayanto, "MEASUREMENT OF EMPLOYEE INFORMATION SECURITY AWARENESS: CASE STUDY AT FINANCIAL INSTITUTION," *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, vol. 9, no. 2, pp. 172–179, Feb. 2024, doi: 10.33480/jitk.v9i2.4163.

[25] Y. Adhi Styoutomo and Y. Ruldeviyani, "Information Security Awareness Raising Strategy Using Fuzzy AHP Method with HAIS-Q and ISO/IEC 27001:2013: A Case Study of XYZ Financial Institution," *CommIT Journal*, vol. 17, no. 2, pp. 133–149, 2023.

[26] A. L. Fadhilah, Y. Ruldeviyani, R. Prakoso, and K. F. Arisya, "Measurement of Information Security Awareness Level: A Case Study of Digital Wallet Users," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1077, no. 1, p. 012003, Feb. 2021, doi: 10.1088/1757-899x/1077/1/012003.

[27] 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.

[28] I. G. A. Sukariana Yasa, I. M. E. Listartha, and I. M. A. Pradnyana, "MEASUREMENT OF INFORMATION SECURITY AND PRIVACY AWARENESS USING THE MULTIPLE CRITERIA DECISION ANALYSIS (MCDA) METHOD," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 4, pp. 759–768, Aug. 2023, doi: 10.52436/1.jutif.2023.4.4.692.

[29] G. Bonggal, N. Alvito, F. Setiadi, and M. Irsan, "Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa Fakultas Informatika Menggunakan Human Aspect of Information Security Questionnaire (HAISQ) di Universitas Telkom Bandung," *Jurnal Penelitian Informatika*, vol. 3, pp. 98–107, 2025, doi: 10.25124/logic.v3i2.6467.

[30] L. Bognár and L. Bottyán, "Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students," *Educ. Sci. (Basel).*, vol. 14, no. 6, Jun. 2024, doi: 10.3390/educsci14060588.

.