Jurnal Ekonomi, Teknologi dan Bisnis (JETBIS)
Volume 5, Number 4 April 2026
p-ISSN 2964-903X; e-ISSN 2962-9330

Measurement and Strategy to Improve Information Security Awareness with The Hais-Q (Human Aspect Information Security Questionnaire) and AHP Case of E-Commerce Users

Romy Aziz Risaldi[1]*, Catur Edi Widodo[2], Bayu Surarso[3]
Universitas Diponegoro, Indonesia[1,2,3]
Email: romyrisaldi@students.undip.ac.id[1]*, caturediwidodo@lecturer.undip.ac.id[2],
bayus@lecturer.undip.ac.id[3]
Email: romyrisaldi@students.undip.ac.id

ABSTRACT

Rapid growth in e-commerce has made information security awareness (ISA) increasingly critical, particularly following major breaches such as the 2020 Tokopedia incident, which compromised the personal data of approximately 91 million Indonesian users. This vulnerability is compounded by the sharp rise in e-commerce transactions since the Covid-19 pandemic, widening the attack surface for threats such as phishing and account takeover. This study aims to measure the level of ISA among e-commerce users in Purwokerto City and to formulate a strategy for improving it. A quantitative descriptive survey was conducted using the HAIS-Q instrument, assessing users' Knowledge, Attitude, and Behavior (KAB) across seven focus areas, combined with the Analytic Hierarchy Process (AHP) to prioritize those areas through expert comparison. Data were collected from 71 active users of Tokopedia, Shopee, Blibli, and Lazada using a 70-item questionnaire. The overall ISA score was 78.12, classified as "Average," with knowledge scoring highest and behavior lowest. Two focus areas reached the "Good" category, while five remained "Average," indicating that improving ISA requires strategies targeting behavioral change, offering an empirical, priority-based basis for platform providers, regulators, and users.

Keywords: information security awareness; e-commerce; KAB; HAIS-Q; AHP

INTRODUCTION

Information is data that has been processed and used for decision-making. Because information is highly valuable, its protection is crucial through information security that maintains its confidentiality, integrity, and availability (Nadji, 2024). Cyber threats such as hacking are increasing as organizations and individuals become more dependent on technology. This trend is reflected in national-level figures: Indonesia's National Cyber and Encryption Agency (Badan Siber dan Sandi Negara/BSSN) recorded approximately 361 million traffic anomalies indicative of cyberattacks between January and October 2023 alone, dominated by malware (42.79%) and trojan activity (35.40%) (Arkyasa, 2023). Low information security awareness among technology users is a major contributor to this trend and can lead to data leaks, operational disruptions, and a diminished organizational reputation. A concrete illustration of this risk in the Indonesian e-commerce sector is the 2020 Tokopedia data breach, in which the personal data of approximately 91 million user accounts including usernames, email addresses, hashed passwords, and dates of birth (Putra, Y. G., & Rahmahani, 2025).

Incidents of this kind show that individual users, not only organizational systems, are frequently the weakest link in information security, and that technical safeguards alone are insufficient without adequate user awareness of secure online behavior (Imtiaz, 2025). This concern is amplified in e-commerce, where transaction volumes have grown rapidly since the Covid-19 pandemic, widening the potential attack surface for phishing, account takeover, and data theft targeting individual users (Adeniya, 2025). Beyond the direct financial and privacy harm to affected

users, such incidents erode public trust in digital platforms and, at an aggregate level, threaten the continuity of Indonesia's digital economy, underscoring the urgency of understanding and strengthening user-level information security awareness rather than relying solely on platform-side technical controls.

The Human Aspects of Information Security Questionnaire (HAIS-Q) is an instrument designed to measure information security awareness using the Knowledge, Attitude, and Behavior (KAB) model (Mokhsen et al., 2025). In this study, the questionnaire results are combined with the Analytic Hierarchy Process (AHP) to prioritize security awareness areas within seven distinct focus domains. The AHP method supports decision-makers by organizing complex problems and ensuring that all relevant criteria and alternatives are taken into account (Bugingo et al., 2024). HAIS-Q and AHP have each been validated and applied in prior information-security research (Utama, F. et.al, 2023), providing methodological grounding for their combined use in this study. Several studies have measured information security awareness (ISA) in Indonesian contexts using KAB-based instruments (Munir, 2024), but none has specifically examined active e-commerce users while combining HAIS-Q with AHP-based prioritization.

Ramadhan & Idea, (2023) measured the ISA of digital banking application users in Indonesia using HAIS-Q and reported an overall "good" awareness level, although behavioral compliance remained an area for improvement. Kusumaningrum et al., (2022) assessed the cybersecurity awareness of students during remote learning using the Multiple Criteria Decision Analysis (MCDA) method and found a "moderate" awareness level. Utama, F. et.al, (2023) measured the information security awareness of civil registration service employees in Bengkulu City using MCDA combined with AHP weighting and reported an overall "average" score of 79%, with the knowledge dimension identified as the weakest. While these studies confirm that KAB-based instruments are effective across institutional settings, none of them targeted e-commerce users specifically, and none combined HAIS-Q with AHP to derive an expert-weighted priority ranking across ISA focus areas. In practice, treating all seven HAIS-Q focus areas as equally important, as most prior studies implicitly do, does not reflect the fact that some information-security risks (e.g., account credential misuse) Heesuk, (2022) carry more severe consequences for e-commerce users than others (e.g., minor privacy inconvenience) a gap this study addresses by incorporating AHP-based expert weighting.

The novelty of this study lies in integrating two complementary methods: HAIS-Q, which measures ISA through the KAB model across seven focus areas, and AHP, which derives expert-weighted priorities among those seven focus areas through pairwise comparison. This combination allows the resulting ISA score not only to describe users' current awareness level but also to indicate which focus areas warrant the most urgent intervention (Armstrong et al., 2020), offering a more actionable basis for improvement strategies than a HAIS-Q measurement alone. To the authors' knowledge, this HAIS-Q–AHP combination has not previously been applied to e-commerce users in an Indonesian city-level context.

This study aims to measure the level of Information Security Awareness (ISA) of e-commerce application users in Purwokerto City using the HAIS-Q instrument, and to determine the priority ranking of ISA focus areas using AHP, in order to formulate a strategy for improving information security awareness among e-commerce users. The results are expected to help e-commerce users recognize gaps in their own security practices, to provide e-commerce platform providers with an

empirical, priority-based foundation for designing more targeted security education and features, and to support regulators and other stakeholders in developing cybersecurity literacy policies that address the specific behavioral gaps identified in this study.

RESEARCH METHODS

This research employs a quantitative descriptive research design, using a cross-sectional online survey to measure e-commerce users' Information Security Awareness (ISA) and an expert pairwise-comparison survey (AHP) to prioritize ISA focus areas. There are six stages in this research procedure, as depicted in Figure 1 Literature Review, Problem Identification and Formulation, Research Instruments, Data Collection, Data Processing and Analysis, and Conclusion Drawing.

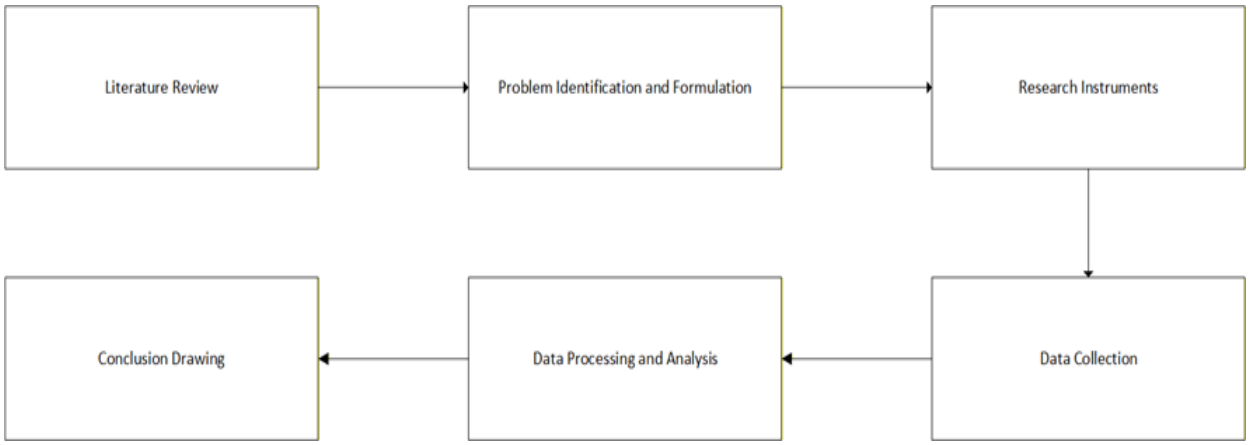

Figure 1. Research Procedures

Research Instruments

The Instruments needed in this study are respondent data obtained from the information security awareness research questionnaire using the HAIS-Q (Human Aspect Information Security Questionnaire) method. Respondents are active users of e-commerce applications domiciled in Purwokerto City of all ages and education levels. There are 4 e-commerce application products used as research materials for measuring information security awareness, namely Tokopedia, Shopee, Blibli, and Lazada. Respondents are only allowed to submit their answers once. The questionnaire consists of 70 questions with 63 statements referring to specific statements regarding information security awareness of the use of e-commerce applications as well as internet usage and smartphone usage and 7 statements referring to general statements such as the duration of daily use of e-commerce applications along with personal data.

Each respondent answers questions related to information security using a Likert scale consisting of 5 scales, namely 1 = (Strongly Disagree), 2 = (Disagree), 3 = (Neutral), 4 = (Agree), and 5 (Strongly Agree).

Data Collection

After the research instrument development stage, quantitative data collection was conducted by distributing an online questionnaire to e-commerce application users in Purwokerto City using a non-probability (convenience) sampling approach, obtaining 71 respondents. Furthermore, a statement form related to the pairwise comparison matrix was sent to cybersecurity experts to

compare the priority levels of the predetermined focus areas. The output of this stage was respondent response data and the pairwise comparison matrix data.

Data Processing and Analysis

The seven focus areas of the HAISQ method in this research such as; source application, information handling & privacy, internet use & message, consequences, account & password management, security incident, and mobile devices describing below.

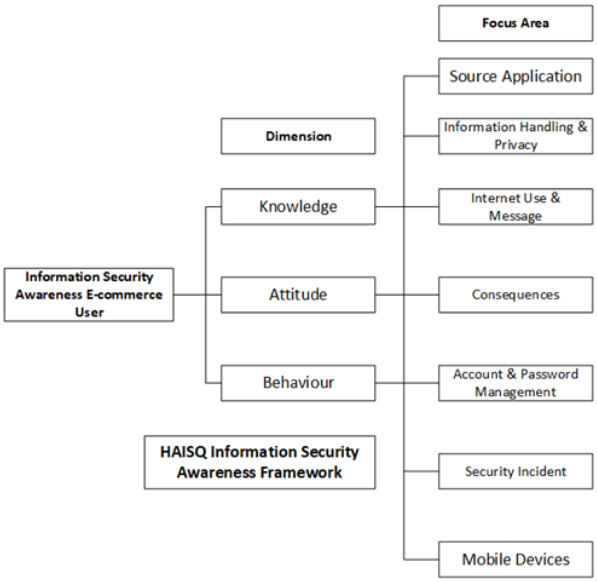

Figure 2. E-commerce User Information Security Awareness Framework Adopted from HAIS-Q

After the focus area is described, sub-focus areas are determined for each focus area, with 3 sub-focus areas for each focus area based on previous research journals.

Table 1. Determining Sub Focus Area

No.	Focus Area	Sub Focus Area	Reference
1	Source Application	Untrusted Source	HAIS-Q : Mokhsen et al., (2025); Pandia, (2024)
		Review & Rating	
		Unsigned Application	
2	Information Handling & Privacy	Secure Sensitive Information	
		Privacy	
		Perceived Intrusion	
3	Internet Use & Message	Unknown Sender Message	
		Link Phising	
		Social Engineering	
4	Consequences	Using Ilegal Application	
		Using Free VPN in Public	
		Using Wifi Public for	
		Transaction	
5	Account & Password Management	Using a Strong Password	
		2 FA Authentification	

No.	Focus Area	Sub Focus Area	Reference
		Using a Same Password	
6	Security Incident	Awareness Fraud Incident	
		Awareness about Skimming	
		Reporting Security Incident	
7	Mobile Devices	Root (Jailbreak)	
		OS and Security update	
		Security Feature	

Source: Data Processed

The level of information security awareness will be calculated using different priority scales and weights for each focus area. Priority scales for focus areas are determined using the AHP method using scale 1-9. AHP helps decision makers find the most appropriate solution by structuring the problem and ensuring that all criteria and alternatives have been identified. The following is an example of an AHP priority scale table and a priority scale for focus areas.

Table 2. AHP Scale Matrix Pairwise Comparison

Numerical Value	Description
1	Equal Importance
3	Slighty more Importance
5	Moderate importance of one over another
7	Very strong importance
9	Extreme importance of one over another
2,4,6,8	Intermediate values between two adjacent values

Source: Data Processed

Table 3. Determining AHP Scale Matrix Pairwise Comparison for Focus Area

Criteria A	Criteria B	More Importance A/B?	Scale (1-9)
Source Application	Information Handling & Privacy	A	7
	Internet Use & Message	A	5
	Consequences	A	5
	Account & Password Management	A	3
	Security Incident	A	3
	Mobile Devices	A	5
Information Handling & Privacy	Internet Use & Message	B	2
	Consequences	B	3
	Account & Password Management	B	2
	Security Incident	B	3
	Mobile Devices	A	5
Internet Use & Message	Consequences	A	6
	Account & Password	B	7

Criteria A	Criteria B	More Important A/B?	Scale (1-9)
	Management		
	Security Incident	A	6
	Mobile Devices	A	5
Consequences	Account & Password Management	B	4
	Security Incident	B	3
	Mobile Devices	A	5
Account & Password Management	Security Incident	A	3
	Mobile Devices	A	7
Security Incident	Mobile Devices	A	5

Source: Data Processed

After outlining the focus areas with the weighting of the AHP scale given, the next step is to create a list of questions based on the focus area and sub focus area table, based on literature references from previous research. Each focus area has 9 questions, 3 of which are from the KAB concept (knowledge, attitude, behavior) and the next 3 are from the sub-focus area. To assess the questionnaire questions, a Likert scale of 1-5 is used (1 = Strongly disagree - 5 = Strongly agree).

Table 4. Questionnaire Focus Area Internet Use & Message

	Sub Focus Area	Dimension			Reference
		Knowledge	Attitude	Behaviour	
Focus Area: Internet Use & Message	Unknown Sender Message	I sometimes worry about unknown message senders.	I think we need to be more careful when looking at SMS/Chats that suddenly come into our cell phones and we don't know who sent them.	I need to be careful if there is a message sender who doesn't have a contact name and if necessary, trace it in the GetContact application.	HAIS-Q: Parsons et al. (2017)
	Link Phishing	I think links with the URL prefix https:// are safe.	I rarely click on links containing product advertisements from e-commerce apps when I'm on social media, chat apps, or email.	I need to be careful if there is a URL link where when I open it there is a security notification.	
	Social Engineering	You need to be careful if someone claims to be from the bank	If I get a gift message from an e-commerce application, I	If I get a WhatsApp message to update my account	

Sub Focus Area	Dimension			Reference
	Knowledge	Attitude	Behaviour	
	and asks for identity information.	would rather ignore it.	information and password via the link specified by the e-commerce customer service, I ignore it.	

Source: Data Processed

Next step, based on the Krueger and Kearney weighting scale, each attribute of *knowledge*, *attitude*, and *behavior* is given a certain weight (refer to the table below).

Table 4. Weighting of Knowledge, Attitude, Behavior Dimensions

Dimension	Weight
Knowledge	30
Attitude	20
Behaviour	50

Source: Data Processed

Then the next step is to calculate the awareness score by multiplying the results for each focus area (vi) and the weight for each focus area (wi) that have been made by previous research using the formula calculation below.

$$V(a) = \sum_{i=1}^{n} vi\ (a)\ wi$$

Figure 3. ISA Measurement Formula Adopted from Kruger (Kruger, H., and Kearney, 2006)

V(a) is the value of all alternatives or the value of the level of information security awareness, vi is the score value that represents the performance of the alternative or the quantitative value from the calculation results of the Likert scale questionnaire, and wi is the value to represent the level of importance. The weight of wi is determined using the AHP method (Kruger, H., and Kearney, 2006)**.**

Then there is a scale of action criteria from the final value of information security awareness with each scale having its own follow-up, as in the example below.

Table 5. Information Security Awareness Action Criteria Scale

Category	Persentage (%)	Action Plan
Good	80 - 100	No need for action
Average	60 – 79	Action potentially required
Poor	<59	Action Required

Source: Data Processed

The table above, quoted from Kruger, indicates that each level of security awareness requires different follow-up actions. For the awareness level, "*Poor*" means that information security awareness is still very low and requires significant improvement. For the awareness level, "*Medium*" means that information security awareness is quite good, but there are still some areas that need improvement. Meanwhile, "Good" means that security awareness is very good. The necessary follow-up may only involve reinforcement activities or reminders that can be carried out periodically, or other activities aimed at increasing information security awareness.

RESULTS AND DISCUSSION

After the research method stage, the next step is to calculate the obtained questionnaire data and use it to determine the level of information security awareness of e-commerce application users. After that, a strategy was concluded to improve information security awareness.

Questionnaire Result Analysis

Based on the research results, it is known that the majority of respondents using e-commerce services have a high school/vocational high school/Islamic high school education, namely 31 people or 43.7 percent. Then respondents with a bachelor's degree are 19 people or 26.8 percent, Diploma as many as 13 people or 18.3 percent, junior high school/Islamic junior high school as many as 5 people or 7.07 percent, then 2 people or 2.8 percent have elementary school education and only 1 person or 1.4 percent have postgraduate education. This data indicates that e-commerce users are dominated by the middle-educated group (SMA/SMK/MAN), while participation from the higher-educated group (Postgraduate) is very low. The data also shows that the middle-educated level (SMA/SMK/MAN) dominates in the use of e-commerce services, perhaps due to age factors, access to technology, or higher online shopping needs among these groups compared to college graduates.

Table 6. Respondents Based on Frequently Used E-commerce Application Products

	Frequently used e-commerce application products	Amount	Persentage
1	Blibli	6	8.5
2	Lazada	15	21.1
3	Shopee	35	49.3
4	Tokopedia	15	21.1
	Total	**71**	**100.0**

Source: Data Processed

The results of the study showed that the majority of respondents who use e-commerce services prefer Shopee as an online shopping platform, with the number of users reaching 35 people (49.3 percent). The next ranking is occupied by Lazada and Tokopedia, each used by 15 people (21.1 percent), while Blibli is the choice for 6 people (8.5 percent) of respondents. These findings indicate that Shopee dominates the e-commerce market among respondents, perhaps due to massive promotions, competitive prices, or ease of use compared to other platforms. Meanwhile, Lazada and Tokopedia have almost equal market share, while Blibli is still relatively less popular among the users surveyed.

Table 7. Description of Respondents Based on Last Education

No	Last Education	Amount	Persentage
1	Diploma	13	18.3
2	Post Graduate	1	1.4
3	Bachelor	19	26.8
4	Elementary	2	2.8
5	Senior High School	31	43.7
6	Junior High School	5	7.0
	Total	**71**	**100.0**

Source: Data Processed

Based on the research results, it is known that the majority of respondents using e-commerce services have a high school/vocational high school/Islamic high school education, namely 31 people or 43.7 percent. Then respondents with a bachelor's degree are 19 people or 26.8 percent, Diploma as many as 13 people or 18.3 percent, junior high school/Islamic junior high school as many as 5 people or 7.07 percent, then 2 people or 2.8 percent have elementary school education and only 1 person or 1.4 percent have postgraduate education. This data indicates that e-commerce users are dominated by the middle-educated group (SMA/SMK/MAN), while participation from the higher-educated group (Postgraduate) is very low. The data also shows that the middle-educated level (SMA/SMK/MAN) dominates in the use of e-commerce services, perhaps due to age factors, access to technology, or higher online shopping needs among these groups compared to college graduates.

Information Security Awareness Score for each Focus Area

The following table shows the final score for measuring e-commerce users' information security awareness based on focus areas and KAB (knowledge, attitude, behavior) dimensions.

Table 8. ISA score description for each focus area

Focus Area	K	A	B	Total Awareness (Focus Area)
Source Application	73,62	84,79	75,40	76,74
Information Handling & Privacy	76,62	76,34	80,09	78,30
Internet Use & Message	80,38	71,83	84,23	80,59
Consequences	76,81	81,97	72,49	75,68
Account & Password Management	81,22	81,88	71,64	76,56
Security Incident	81,88	80,09	72,96	77,06
Mobile Devices	83,19	72,02	83,10	80,91

Source: Data Processed

In the Source Application focus area, the knowledge (K) score was 73.62, attitude (A) was 84.79, and behavior (B) was 75.40, resulting in a total awareness of 76.74. This indicates that although user attitudes towards source application security are already high, user understanding and behavior still need to be improved to align with their attitudes. The Information Handling & Privacy focus area achieved a total awareness of 78.30, with a K score of 76.62, an A score of 76.34, and a B score of 80.09. These findings indicate that users have relatively implemented good behavior in

handling and maintaining information privacy, although the knowledge and attitude aspects still need to be strengthened. In Internet Use & Messaging, a total awareness score of 80.59 was obtained, which is one of the highest scores.

The K score of 80.38 and B score of 84.23 indicate that users have a good understanding and behavior in using the internet and messaging, although the relatively lower attitude (A) score of 71.83 indicates potential risks if caution is not continuously improved. The Consequences focus area has a total awareness of 75.68, with a K value of 76.81, an A value of 81.97, and a B value of 72.49. These results indicate that users have a positive attitude towards the consequences of information security breaches, but actual behavior in anticipating and avoiding risks is still relatively low compared to other dimensions. In Account & Password Management, total awareness was recorded at 76.56. Knowledge scores (81.22) and attitudes (81.88) were relatively high, but the behavior score (71.64) indicated a gap between understanding and attitudes and the implementation of secure account and password management practices.

Furthermore, the Security Incident focus area showed a total awareness of 77.06, with a K score of 81.88, an A score of 80.09, and a B score of 72.96. This indicates that users have a good understanding and attitude towards security incidents, but are still less than optimal in their incident reporting and handling behavior (Pandia, 2024). Meanwhile, Mobile Devices achieved the highest total awareness of 80.91. The K score of 83.19 and B score of 83.10 indicate a very good level of understanding and behavior in using mobile devices, although the lower attitude (A) score of 72.02 indicates the need to increase awareness of attitudes towards security risks on mobile devices.

Analytic Hierarchy Process (AHP) Priority Weighting and Overall ISA Score

Using the expert pairwise-comparison matrix in Table 3 and Applying the formula $V(a) = \Sigma vi \cdot wi$ to the total awareness scores (vi) in Table 8 and the AHP weights (wi) above yields an overall ISA score of approximately 77.5, which closely approximates the overall ISA score of 78.12 reported in the Conclusion (the small difference reflects rounding and the specific eigenvalue-approximation method used). This derivation makes explicit, and reproducible, the link between the individual focus-area scores in Table 8 and the headline ISA score, which was previously stated only in the Conclusion without supporting calculation. Under this AHP weighting, Source Application and Account & Password Management jointly account for more than half of the overall ISA score's weighting (Edwards, 2024), meaning that improvement efforts targeting these two focus areas would have the largest impact on the overall ISA score.

Comparison with Prior Studies and Interpretation

The overall ISA score of 78.12 ("Average") obtained in this study is broadly consistent with the pattern observed in prior Indonesian ISA research: Ramadhan & Idea, (2023) reported a "good" level among digital banking users, Kusumaningrum et al., (2022) reported a "moderate" level among students studying from home, and Utama, F. P. et.al, (2023) reported an "average" score of 79% among civil registration employees in Bengkulu City. Together with the present findings, this suggests that awareness levels among Indonesian technology users generally cluster in the moderate-to-average range (Gavana et al., 2024), with e-commerce users in this study performing comparably to public-sector employees but behind banking-application users, possibly reflecting more mature security messaging in the financial sector than in general e-commerce .

Within the KAB dimensions, the consistent pattern of knowledge exceeding attitude, which in turn exceeds behavior, indicates that respondents largely understand what constitutes safe practice and even hold favorable attitudes toward it, but do not consistently translate this into action. This knowledge behavior gap is plausibly explained by the convenience driven, habitual nature of e-commerce use (Liu et al., 2025), where the perceived cost of, for example, enabling two-factor authentication or verifying an application's source is weighed against the immediate friction it adds to a purchase, and by optimism bias, whereby users judge a breach as more likely to happen to others than to themselves. This interpretation is consistent with the lowest total-awareness focus area in this study, Consequences (75.68), where users reported favorable attitudes (81.97) toward the seriousness of information-security breaches but comparatively weak behavior (72.49) in actually avoiding risky actions.

Strategy to Improve Information Security Awareness

Combining the AHP priority weights with the KAB gap identified above yields a targeted, rather than generic, strategy to improve ISA (Donati et al., 2023). Because Source Application carries the highest AHP weight (33.41%) yet has the lowest total awareness score among the top-weighted areas (76.74, driven by its comparatively low behavior score of 75.40), e-commerce platform providers and regulators should prioritize interventions that make safe application-source verification easier and more habitual, for example through in-app warnings before installing unofficial extensions or before entering credentials on unfamiliar interfaces.

Because Account & Password Management is the second most heavily weighted area (22.38%) and shows the largest internal K/A–B gap (knowledge 81.22 and attitude 81.88 versus behavior 71.64), platforms should prioritize default, low-friction security features (e.g., enforced two-factor authentication, password managers, and breach notifications) rather than relying on user-initiated adoption. At the user level, e-commerce users are advised to consistently apply strong, unique passwords, verify application sources before installation, and report suspected security incidents. At the policy level, these findings support the design of behavior-focused cybersecurity literacy campaigns, rather than knowledge-only campaigns, since knowledge was consistently the strongest KAB dimension across nearly all focus areas.

CONCLUSION

Based on the measurement of Information Security Awareness (ISA) among e-commerce application users using the HAIS-Q method with the Knowledge, Attitude, and Behavior (KAB) approach, respondents came from diverse backgrounds and routinely used e-commerce applications. The instrument was adapted from the validated HAIS-Q, though sample-specific reliability testing was not conducted, a limitation for future replications. The overall ISA score was 78.12, an "Average" category indicating fairly good but not optimal awareness, especially in behavior. Knowledge scored highest, followed by attitude, with behavior lowest, revealing a gap between understanding, attitude, and actual practice.

Weighted by AHP, Source Application and Account & Password Management were the highest-priority areas, though this ranking is indicative given the Consistency Ratio exceeded the recommended threshold. Two focus areas reached "Good," while five remained "Average." Users

should apply strong passwords and verify application sources; providers should strengthen security features; and regulators can use these findings for policy.

BIBLIOGRAPHY

Adeniya, F. A. (2025). *Exploratory Analysis Of Cyberattack Patterns On E-Commerce Platforms Using Statistical Methods*. Https://Arxiv.Org/Pdf/2511.03020

Arkyasa, M. (2023). *Bssn Records 361 Million Cyber Attacks In Indonesia - En.Tempo.Co*. Https://En.Tempo.Co/Read/1797753/Bssn-Records-361-Million-Cyber-Attacks-In-Indonesia

Armstrong, L. L., Watt, E., St. John, E., & Desson, S. (2020). The Interactive Symptoms Assessment: I.S.A. – Development And Validation Using A Knowledge Translation-Integrated Model. *Current Psychology 2020 41:5*, *41*(5), 3038–3054. Https://Doi.Org/10.1007/S12144-020-00801-5

Bugingo, E., Leone Ndimubenshi, E., Tshimanga Kamanga, C., Xavier Rugema, F., Habimana, O., & Batamuliza, J. (2024). *Application Of Ahp In Decision-Making: Case Studies And Practical Implementation*. Https://Doi.Org/10.5772/Intechopen.1006966

Donati, I. I. M., Viaggi, D., Srdjevic, Z., Srdjevic, B., Di Fonzo, A., Del Giudice, T., Cimino, O., Martelli, A., Dalla Marta, A., Henke, R., & Altobelli, F. (2023). An Analysis Of Preference Weights And Setting Priorities By Irrigation Advisory Services Users Based On The Analytic Hierarchy Process. *Agriculture 2023, Vol. 13, Page 1545*, *13*(8), 1545. Https://Doi.Org/10.3390/Agriculture13081545

Edwards, D. J. (2024). Account Management. *Critical Security Controls For Effective Cyber Defense*, 127–154. Https://Doi.Org/10.1007/979-8-8688-0506-6_5

Gavana, G., Gottardo, P. (2024). Related Party Transactions And Earnings Management In Family Firms: The Moderating Role Of Board Characteristics. *Emerald.Com*. Https://Doi.Org/10.1108/Jfbm-07-2022-0090

Heesuk Lee Ahmad Mostafa, By, Mentor, F., Myles Vogel, C., Member Kondo Litchmore, C., & Member Jennifer Straub, C. A. (2022). *The Relationship Between The Frequency Of Respective Cybersecurity Training Types And Information Security Awareness In The U. S. Technology Industry*.

Imtiaz, U. (2025). Investigating The Impact Of Phishing Attacks On Organizational Cybersecurity Posture. *Spectrum Of Engineering Sciences*, 1758–1780. Https://Doi.Org/10.5281/Zenodo.19912244

Kruger, H., And Kearney, W. (2006). *A Prototype For Assessing Information Security Awareness*. Computers & Security.

Kusumaningrum, A., Sinus, H. (2022). Pengukuran Tingkat Kesadaran Keamanan Siber Di Kalangan Mahasiswa Saat Study From Home Dengan Multiple Criteria Decision Analysis (Mcda). *Researchgate.Neta Kusumaningrum, H Wijayanto, Bd Raharjajurnal Ilmiah Sinus, 2022•Researchgate.Net*. Https://Www.Researchgate.Net/Profile/Hendro-Wijayanto/Publication/357834285_Pengukuran_Tingkat_Kesadaran_Keamanan_Siber_Di_Kalangan_Mahasiswa_Saat_Study_From_Home_Dengan_Multiple_Criteria_Decision_Analysis_Mcda/Links/61e1a73970db8b034c941ba2/Pengukuran-Ti

Liu, K. J., Chen, S. L., Huang, H. C., & Gan, M. L. (2025). From Theory To Practice: Key Factors Influencing User Shopping Behavior On Cross-Border E-Commerce Platforms. *Springer*,

44(19), 15994–16009. Https://Doi.Org/10.1007/S12144-025-08151-W

Mokhsen, M., -, R. U., Informatics, Undefined, Cybersecurity, And, & 2025, Undefined. (2025). Enhancement Of The Human Aspects Of Information Security Questionnaire (Hais-Q): For Indonesia Educational Institutions. *Ieeexplore.Ieee.Org*, *26*(1–2), 24–49. Https://Doi.Org/10.1080/15228886.2025.2541178

Munir, N. (2024). *The Impact Of Iso 27001 Compliance On Employees' Information Security Awareness And Behaviors In Medium Sized Enterprises (Mses)*. Https://Www.Diva-Portal.Org/Smash/Get/Diva2:1874341/Fulltext01.Pdf

Nadji, B. (Brad). (2024). Data Security, Integrity, And Protection. *Signals And Communication Technology*, *Part F3121*, 59–83. Https://Doi.Org/10.1007/978-3-031-61117-9_4/Save-Research

Pandia, H. (2024). Role Of Knowledge And Attitudes In Shaping Incident Reporting Behaviors In Mobile Banking. *Teika*, *14*(2), 199–209. Https://Doi.Org/10.36342/Teika.V14i2.3758

Putra, Y. G., & Rahmahani, A. (2025). *Legal Protection For Victims Of Personal Data Leakage (Case Study On Victims Of Pt Tokopedia In 2020)*. 600–612.

Ramadhan, T., & Idea, B. P. (2023). Analisis Tingkat Kesadaran Keamanan Informasi: Studi Kasus Pengguna Aplikasi Perbankan Digital Di Indonesia Guna Mencegah. *Pdfs.Semanticscholar.Orgt Ramadhan, B Purwandarisyntax Idea, 2023•Pdfs.Semanticscholar.Org*. Https://Doi.Org/10.36418/Syntax-Idea.V3i6.1227

Utama, F. P., Prasetyo, D. Y., & Coastera, F. F. (2023). *Penerapan Mcda Untuk Meningkatkan Kesadaran Keamanan Informasi Publik Pada Dinas Dukcapil Kota Bengkulu*. Https://Scholar.Google.Co.Id/Scholar?Hl=Id&As_Sdt=0%252c5&As_Ylo=2022&Q=Utama%252c+F.+P.%252c+Prasetyo%252c+D.+Y.%252c+%2526+Coastera%252c+F.+F.+%2528 2023%2529.+Penerapan+Mcda+Untuk+Meningkatkan+Kesadaran+Keamanan+Informasi+Publik+Pada+Dinas+Dukcapil+Kota+Bengkulu.+Jsai+%252

Yusuf, A. L., Nugraha, D., Wahlanto, P., Indriastuti, M., Indri Lestari Prodi, N. D., Stikes Muhammadiyah Ciamis, F., Kunci, K., Bakar Ringan, L., Luka Bakar Bakar Ringan, P., & Ekstrak Kulit Lidah Buaya, G. (2020). *Uji Aktivitas Gel Ekstrak Kulit Lidah Buaya (Aloe Vera) Untuk Penyembuhan Luka Bakar Ringan Pada Kelinci (Oryctolagus Cuniculus) Activity Test Of Aloe Vera Peel Extract (Aloe Vera) Gel With Rabbit's (Orycctolagus Cuniculus) Combustio (Minor Burns)*.