Journal of Emerging Information Systems and Business Intelligence
ISSN: 2774-3993
Journal homepage: https://ejournal.unesa.ac.id/index.php/JEISBI/

Analysis of Information Security Awareness Level Using Multiple Criteria Decision Analysis

Fauzan Ali Ghofur[1], I Kadek Dwi Nuryana[2]
[1,2]*Universitas Negeri Surabaya, Surabaya, Indonesia*
fauzan.19041@mhs.unesa.ac.id, *dwinuryana@unesa.ac.id*

ABSTRACT

The rapid growth of digital transaction applications has transformed financial activities and increased reliance on electronic payment systems. However, the widespread use of these platforms also exposes users to various information security threats, including phishing, malware, and social engineering attacks that often exploit human vulnerabilities. Despite the increasing adoption of digital financial services, the level of information security awareness among users remains a critical issue that requires systematic evaluation. This study aims to measure and analyze the level of information security awareness among digital transaction application users in Surabaya. This research employs a quantitative approach using Multiple Criteria Decision Analysis (MCDA) integrated with the Knowledge, Attitude, and Behavior (KAB) model. The assessment framework is based on the Human Aspects of Information Security Questionnaire (HAIS-Q), which includes seven focus areas: password management, email usage, internet usage, social media usage, device usage, information handling, and incident reporting. Data were collected through an online questionnaire distributed to digital transaction users in Surabaya, resulting in 102 valid respondents. The results indicate that most focus areas fall into the low awareness category, including password management (53.73%), email usage (23.44%), internet usage (15.99%), social media usage (47.34%), device usage (47.63%), and incident reporting (45.57%). Only the information handling dimension reached a moderate awareness level with a score of 78.17%. These findings highlight the need for improved cybersecurity education and awareness programs to encourage safer digital transaction practices.

Keyword: Information Security Awareness, Digital Transaction Security, Multiple Criteria Decision Analysis, HAIS-Q, Cybersecurity.

Article Info:
Article history:
Received March 17, 2026
Revised March 24, 2026
Accepted May 25, 2026

Corresponding Author
Fauzan Ali Ghofur
Univeritas Negeri Surabaya, Surabaya, Indonesia
Fauzan.19041@mhs.unesa.ac.id

1. INTRODUCTION

The rapid advancement of technology has profoundly impacted global business operations and societal structures. From the industrial revolutions to the present digital age, technology has consistently been leveraged to address complex challenges. This technological evolution has also significantly influenced governmental operations, with information technology (IT) increasingly employed to streamline administration and public services. Indonesia has embraced this transformation, evidenced by the establishment of task forces to accelerate digitalization and the development of thousands of government applications to support online administration and

transactions[1]. The widespread adoption of digital payments, facilitated by mobile banking and other online platforms, has become a norm, particularly accelerated by the COVID-19 pandemic. This shift has led to a surge in digital economic transactions, with Bank Indonesia reporting trillions of rupiah in electronic money transactions in 2022 alone[2].

Despite the convenience and efficiency offered by digital transactions, a critical concern emerges: the vulnerability of users to cyber threats. Small and Medium Enterprises (SMEs) in Surabaya, for instance, are identified as targets for cyber-attacks due to a general lack of awareness and understanding of cybersecurity measures[3]. This knowledge gap makes individuals susceptible to social engineering attacks, a prevalent method used by threat actors to gain unauthorized access to sensitive information and systems. Reports from IDADX and BSSN highlight social engineering as a common vector for malware dissemination through modified software applications and phishing emails [4], [5]. Phishing, in particular, involves attackers impersonating legitimate institutions to solicit personal and sensitive data, with over 22,000 reported attacks in 2022 [5]. Sectors like finance in Surabaya have experienced frequent attacks including hacking, phishing, and malware, underscoring the urgent need for enhanced cybersecurity literacy [6].

Information Security Awareness (ISA) is a crucial aspect of cybersecurity, focusing on an individual's understanding and perception of information security principles and practices. It involves a process of changing individual perceptions, values, attitudes, culture, norms, and work activities related to securing information [10]. ISA is considered a discipline that emphasizes the human factor in protecting information assets [11]. Consequently, a lack of awareness can create opportunities for cybercriminals, leading to a high incidence of cybercrime, often by exploiting human vulnerabilities [7].

To address this growing concern, measuring and understanding information security awareness (ISA) is paramount. This study proposes the use of Multiple Criteria Decision Analysis (MCDA) to quantify ISA among digital transaction users in Surabaya. MCDA allows for the evaluation of complex decisions with multiple conflicting criteria, making it suitable for assessing a multi-faceted concept like security awareness. The research integrates the Knowledge-Attitude-Behavior (KAB) model, a psychological framework that posits the interplay between an individual's knowledge, attitudes, and behaviors in shaping their actions. This integration is grounded in established research and aims to provide a comprehensive understanding of ISA[8]. The HAIS-Q (Human Aspects of Information Security Questionnaire) will serve as a robust instrument for measuring ISA across seven key focus areas: password management, email usage, internet usage, social media usage, device usage, information handling, and incident reporting.

This research aims to answer the following questions:

1. How can MCDA be utilized to measure the level of information security awareness among digital transaction users in Surabaya?
2. What are the key criteria that influence the level of information security awareness?
3. How do knowledge, attitude, and behavior collectively influence information security awareness in the context of digital transactions?
4. What actionable recommendations can be derived from the MCDA results to enhance information security awareness among digital transaction users?

The study's objectives are to:

- Determine the level of information security awareness among digital transaction users.
- Identify the weakest focus areas, which represent potential vulnerabilities.
- Analyze the relationship between KAB dimensions and ISA measurement through MCDA.

- Propose effective interventions to improve ISA among digital transaction application users.

This research contributes to the growing body of literature on cybersecurity awareness by providing a quantitative assessment using a robust methodological framework. The findings are expected to inform educational programs and policy development aimed at enhancing digital security literacy among users in Surabaya and potentially beyond.

2. METHODS

This study adopted a quantitative research design employing a cross-sectional survey approach. The primary objective was to measure and analyze the information security awareness of digital transaction application users in Surabaya at a specific point in time. The research integrated the Multiple Criteria Decision Analysis (MCDA) as the overarching analytical framework, with the Knowledge, Attitude, and Behavior (KAB) model serving as the evaluative criteria within the MCDA. The research utilizes seven focus areas derived from the Human Aspects of Information Security Questionnaire (HAIS-Q), as established by Parsons et al. [9], password management, email usage, internet usage, social media usage, device usage, information handling, and incident reporting. These focus areas are deemed critical for assessing ISA in the context of digital transactions. The HAIS-Q has been validated through multiple studies [9], [10]. For instance, 'Password Management' included sub-areas such as using the same password across multiple accounts, sharing passwords, and using strong passwords. 'Email Usage' covered aspects like opening links from unknown senders and downloading attachments indiscriminately. The research process involved designing and administering a questionnaire, collecting data, performing quantitative analysis using statistical software, and drawing conclusions based on the empirical findings. The questionnaire comprised 60 items, with each item formulated as a statement related to security practices. Respondents were asked to rate their agreement with these statements using a Likert scale (e.g., 1 = Strongly Disagree to 5 = Strongly Agree). To mitigate response bias and ensure data accuracy, some statements were phrased negatively (reverse-coded items). Data were collected through an online questionnaire distributed to digital transaction users in Surabaya, resulting in 102 valid responses.

3. RESULTS AND DISCUSSION

This section presents the empirical findings derived from the questionnaire survey and subsequent data analysis. It begins with the validation of the research instrument, followed by a description of the respondent demographics and the core results of the MCDA and KAB analysis.

3.1 Research Design

This study employs a quantitative research design to measure and analyze the level of information security awareness among digital transaction users. The primary methodology is Multiple Criteria Decision Analysis (MCDA), integrated with the Knowledge-Attitude-Behavior (KAB) model. The HAIS-Q instrument, adapted for the context of digital transactions, will be used to collect data across seven focus areas. The research process involves designing and developing a questionnaire, sampling, data collection, data analysis using statistical software (SPSS), and drawing conclusions.

3.2 Sampling and Participants

The target population for this study comprises individuals residing in Surabaya who have engaged in digital transactions using digital transaction applications. A random sampling

technique was employed to select participants. The minimum sample size was calculated using Lemeshow's formula:

$$n = \frac{Z^2 \times P \times (1 - P)}{E^2}$$

where Z is the Z-score for the desired confidence level (1.96 for 95% confidence), P is the estimated proportion of the population (assumed to be 0.5 for maximum sample size), and E is the margin of error (0.05). Based on the population data from the Surabaya Central Statistics Agency (BPS) for 2023 (3,009,286 individuals), the required minimum sample size was calculated to be 385 respondents [11]. However, due to practical constraints during data collection, 102 valid responses were obtained

3.3 Validity and Reliability

The validity and reliability tests were conducted on the 60 questionnaire items. The results of the validity test, presented in Table 10, indicate that all 60 items are valid, as their r-calculated values exceeded the r-table value (0.193), and the significance values were below 0.05. The reliability test, performed using Cronbach's alpha, yielded a value of 0.934 (Table 1). This value is significantly above the threshold of 0.7, indicating that the questionnaire is highly reliable and suitable for data collection.

Table 1 Reliability Statistic

Reliability Statistics	
Cronbach's Alpha	N of Items
0,934	60

3.4 Demographic Profile of Respondents

A total of 102 valid responses were collected from participants in Surabaya. The demographic breakdown is as follows:

- Age: The majority of respondents were aged 16-25 years (66.7%), followed by 26-35 years (19%), 36-45 years (7.6%), and smaller proportions in other age groups (Figure 1).

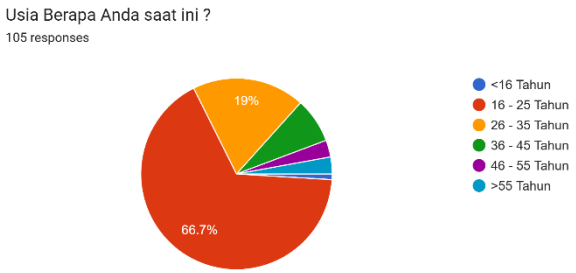

Figure 1 Age Group Respondent

- Gender: There was a near-even distribution, with 54 female respondents and 51 male respondents.

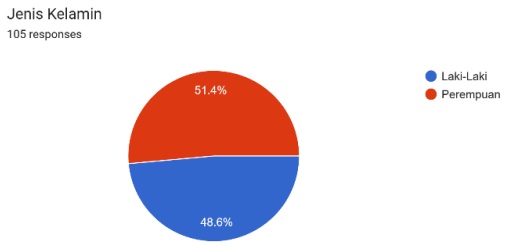

Figure 2 Gender

- Domicile: Respondents were distributed across various districts in Surabaya, with Gubeng, Wonokromo, Benowo, and Sukolilo having the highest number of participants.

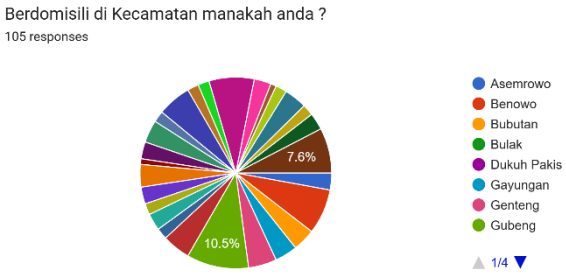

Figure 3 Respondent Domicile

- Occupation: The most common occupations reported were private employees (43 respondents) and students/university students (20 respondents), followed by entrepreneurs (17 respondents).
- Type of Digital Transaction Application Used: E-wallets were the most frequently used type (85 respondents), followed closely by mobile banking (84 respondents) and internet banking (29 respondents). Respondents could select multiple categories.
- Specific Applications Used: GoPay (69 respondents), ShopeePay (79 respondents), and Dana (70 respondents) were the most popular e-wallet applications. BCA Mobile (50 respondents) was also widely used.

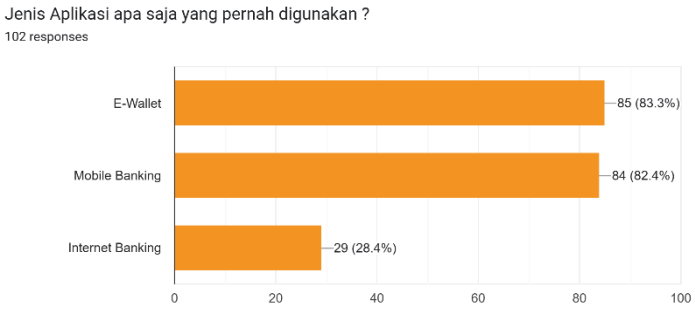

Figure 4 Specific Application Used

- Frequency of Use: Most respondents reported using digital transaction applications more than twice a week, indicating regular engagement with digital payment methods.

3.5 Performance Values and MCDA Calculation

The performance values for each sub-area within the Knowledge, Attitude, and Behavior dimensions were calculated by averaging the responses. These values were then aggregated to represent the performance for each of the seven focus areas across the KAB dimensions. The weights for each focus area were adopted from previous research [12] :

Table 2 Focus Area Weight

Focus Area	Performance Value
Password Management	17,36%
Email Usage	7,69%
Internet Usage	5,22%
Information Handling	25,30%
Device Usage	15,40%
Social Media Usage	15,40%
Incident Reporting	13,63%

Using these weights and the calculated performance values, the MCDA was applied to determine the overall awareness score for each focus area. The formula was used to calculate the weighted scores for each KAB dimension within each focus area.

$$V(a) = \sum_{i=1}^{n} v_i(a) w_i$$

Subsequently, the total awareness score for each focus area was computed based on the KAB proportions (Knowledge: 30%, Attitude: 20%, Behavior: 50%) [13].

Table 3 KAB Value

Focus Area	Knowledge	Attitude	Behavior
Password Management	48,89%	53,67%	56,67%
Email Usage	21,66%	23,48%	24,50%
Internet Usage	14%	17,69%	16,51%
Information Handling	44,33%	50,32%	47,96%
Device Usage	46,80%	49,97%	47,20%
Social Media Usage	73,17%	81,10%	80%
Incident Reporting	44,23%	42,35%	47,67%

The resulting overall awareness scores for each focus area are presented in Table 4:

Table 4 Measurement of Information Security Awareness Level

Focus Area	Awareness Score (%)	Level
Password Management	53,736	Low
Email Usage	23,444	Low
Internet Usage	15,993	Low
Information Handling	47,343	Low
Device Usage	47,634	Low
Social Media Usage	78,171	Average
Incident Reporting	45,574	Low

3.6 Interpretation of Results

Based on the calculated awareness scores and the classification scale (Good: 80–100%, Average: 60–79%, Low: <59%) [13], the findings reveal varying levels of information security awareness among digital transaction users in Surabaya.

- Low Awareness: Six out of the seven focus areas—Password Management, Email Usage, Internet Usage, Social Media Usage, Device Usage, and Incident Reporting—fall into the "Low" awareness category. This indicates significant vulnerabilities in these critical aspects of digital security among the surveyed population.
- Average Awareness: Only the "Information Handling" focus area achieved an "Average" awareness level, with a score of 78.17%. This suggests that while users demonstrate a relatively better understanding and practice regarding handling sensitive information, there is still room for improvement to reach a "Good" level.

3.7 Discussion

The results of this study provide a clear picture of the information security awareness landscape among digital transaction users in Surabaya. The predominantly low awareness levels across most focus areas are a significant cause for concern, highlighting a critical gap between the widespread adoption of digital technologies and users' preparedness to secure themselves against evolving cyber threats.

The "Low" awareness in Password Management (53.74%), indicating that users likely employ weak or reused passwords, making their accounts vulnerable to brute-force attacks and credential stuffing. This aligns with global observations where poor password hygiene remains a primary entry point for cybercriminals.

The extremely low score in Email Usage (23.44%). This suggests a high susceptibility to phishing and malware attacks delivered via email. Users may be clicking on suspicious links or opening malicious attachments without adequate caution, potentially compromising their devices and personal data. The prevalence of social engineering tactics leveraging email makes this finding particularly alarming.

Internet Usage also shows a significantly low awareness score (15.99). Users may be inadvertently accessing risky websites or downloading unverified files, exposing themselves to malware or data theft. The lack of awareness regarding website authenticity and safe information input practices poses a considerable risk.

The findings for Social Media Usage (47.34%) and Device Usage (47.63%) indicate a moderate level of vulnerability. While not as critically low as email or internet usage, these scores suggest that users may not be fully utilizing privacy settings on social media platforms or exercising sufficient caution when handling their devices. This could lead to privacy breaches or the compromise of sensitive information shared on these platforms.

The Incident Reporting score (45.57%), the low score suggests that users may not be reporting suspicious activities or security breaches effectively. This lack of reporting can hinder timely responses from authorities or service providers, allowing threats to persist and potentially spread. It also deprives researchers and organizations of valuable data for threat intelligence.

The only area demonstrating an "Average" awareness level is Information Handling (78.17%). This suggests that users are relatively more aware of the importance of protecting physical and digital information, aligning with the need for secure data management in transactions. However, even this score indicates that complete adherence to best practices is not universal, and there is still potential for vulnerabilities.

The overall low scores across multiple domains underscore the effectiveness of social engineering tactics as described by [4], [5]. Threat actors can exploit these awareness gaps by impersonating legitimate entities or creating deceptive scenarios to trick users into divulging sensitive information or performing actions that compromise their security. The study's findings are consistent with previous research that has highlighted similar awareness deficits in various user populations [3], [8], [14], [15].

3.8 Implications and Recommendations

The findings have significant implications for cybersecurity strategies in Surabaya. The prevalent low awareness necessitates targeted and comprehensive educational interventions. Based on the results, the following actionable recommendations are proposed:

1. Password Management:
    i. Promote the use of strong, unique passwords for all accounts, especially for digital transaction applications. This should involve combining uppercase and lowercase letters, numbers, and symbols.
    ii. Educate users against sharing passwords, even with trusted individuals.
    iii. Emphasize the importance of using different passwords for social media accounts versus financial and transaction applications.
    iv. Encourage the adoption of password managers as a tool to manage multiple complex passwords securely.
2. Email Usage:
    i. Conduct awareness campaigns on identifying phishing attempts and suspicious email content. Users should be cautioned against clicking on unknown links or downloading attachments from unfamiliar senders.
    ii. Highlight the risks associated with responding to unsolicited emails requesting personal or financial information.
3. Internet Usage:
    i. Advise users to employ Virtual Private Networks (VPNs) when using public Wi-Fi to encrypt their traffic.

ii. Educate users about the dangers of clicking on unexpected website redirects and the importance of verifying website legitimacy before entering sensitive data.

iii. Reinforce the principle of not sharing personal information easily, whether online or offline.

4. Social Media Usage:

i. Encourage regular review and adjustment of privacy settings on social media platforms.

ii. Advise users to be mindful of the information they share publicly, especially regarding financial activities or personal routines that could be exploited.

iii. Promote understanding of how social media interactions can be leveraged for social engineering attacks.

5. Device Usage:

i. Emphasize the importance of downloading applications only from official and trusted sources (e.g., Google Play Store, Apple App Store).

ii. Promote vigilance when entering PINs or passwords, advising users to be aware of their surroundings to prevent shoulder surfing.

iii. Educate users about securing their devices with screen locks and keeping their operating systems and applications updated.

6. Information Handling:

i. While this area showed relatively better awareness, continuous reinforcement of procedures for handling sensitive documents and information is necessary. This includes secure disposal of physical documents and avoiding leaving sensitive items unattended.

7. Incident Reporting:

i. Establish clear and accessible channels for reporting cyber incidents.

ii. Educate users on the importance of reporting even seemingly minor privacy violations or suspicious activities to relevant authorities or service providers. This feedback loop is crucial for improving overall security.

3.9 Limitation

This study acknowledges several limitations. Firstly, the sample size (102 respondents) did not meet the statistically determined minimum requirement of 385 respondents. This limits the generalizability of the findings to the entire digital transaction user population in Surabaya. Secondly, the research was confined to the geographical area of Surabaya. Future research could expand the scope to cover other regions in Indonesia. Thirdly, while the HAIS-Q and KAB models provide a robust framework, the self-reported nature of questionnaire data is subject to social desirability bias.

CONCLUSION

This study successfully employed MCDA integrated with the KAB model to assess the information security awareness level among digital transaction users in Surabaya. The findings reveal a concerning landscape of generally low awareness across most critical areas, including

password management, email usage, internet usage, social media usage, device usage, and incident reporting. Only information handling demonstrated an average level of awareness.

The predominant vulnerabilities highlight the significant risks users face from cyber-attacks, particularly social engineering. The low scores underscore the urgent need for targeted educational initiatives and awareness campaigns tailored to the specific challenges faced by digital transaction users.

The actionable recommendations provided—focusing on secure password practices, cautious email and internet usage, mindful social media engagement, secure device handling, proper information management, and proactive incident reporting—aim to empower users and mitigate identified risks.

Despite its limitations, particularly the sample size, this research provides valuable insights into the cybersecurity awareness landscape in Surabaya. Future research should aim to replicate these findings with a larger, more representative sample to achieve greater generalizability and further explore effective intervention strategies for enhancing digital security across Indonesia.

REFERENCES

[1] P. Agustini, "Kominfo Siapkan Super Apps, 24.700 Aplikasi Siap Dilebur – Ditjen Aptika," https://aptika.kominfo.go.id/2022/08/kominfo-siapkan-super-apps-24-700-aplikasi-siap-dilebur/.

[2] "Transaksi Uang Elektronik Melejit," https://indonesia.go.id/kategori/indonesia-dalam-angka/6855/transaksi-uang-elektronik-melejit?lang=1.

[3] I. Made Suartana, R. E. Putra, R. Bisma, and A. Prapanca, "PENGENALAN PENTINGNYA CYBER SECURITY AWARENESS PADA UMKM," *Abadimas Adi Buana*, vol. 5, no. 02, pp. 197–204, 2022, [Online]. Available: http://jurnal.unipasby.ac.id/index.php/abadimas

[4] A. Nugroho, "Tiga Serangan yang Dipakai untuk Bobol Dompet Digital." Accessed: Oct. 29, 2024. [Online]. Available: https://cyberthreat.id/read/4643/Tiga-Serangan-yang-Dipakai-untuk-Bobol-Dompet-Digital

[5] BSSN, "ANNUAL REPORT," 2023.

[6] N. Shafa Azzahra, A. Micael Tambunan, N. Nayra Aulia, A. Binarsih, and T. Hedi Saepudin, "TINJAUAN LITERATUR TENTANG ANCAMAN CYBERCRIME DAN IMPLEMENTASI KEAMANAN SIBER DI INDUSTRI PERBANKAN | HUMANITIS: Jurnal Homaniora, Sosial dan Bisnis," *Humanitis: Jurnal Humaniora, Sosial, dan Bisnis*, vol. 2, no. Vol. 2 No. 7 (2024): Juli, pp. 692–700, Jul. 2024.

[7] CrowdStrike, "2023 GLOBAL THREAT REPORT," 2023.

[8] T. Ramadhan and B. Purwandari, "ANALISIS TINGKAT KESADARAN KEAMANAN INFORMASI: STUDI KASUS PENGGUNA APLIKASI PERBANKAN DIGITAL DI INDONESIA GUNA MENCEGAH SOCIAL ENGINEERING," *Syntax Idea*, vol. 5, no. 1, pp. 86–98, Jun. 2023, doi: 10.36418/syntax-idea.v3i6.1227.

[9] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, “Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q),” *Comput. Secur.*, vol. 42, pp. 165–176, 2014, doi: 10.1016/j.cose.2013.12.003.

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

[11] Badan Pusat Statistik (BPS) Kota Surabaya, “Surabaya Dalam Angka 2023.”

[12] 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.

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

[14] R. Akraman, C. Candiwan, and Y. Priyadi, “Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia,” *JURNAL SISTEM INFORMASI BISNIS*, vol. 8, no. 2, p. 115, Oct. 2018, doi: 10.21456/vol8iss2pp115-122.

[15] M. Amin, “Pengukuran Tingkat Kesadaran Keamanan Informasi PENGUKURAN TINGKAT KESADARAN KEAMANAN INFORMASI MENGGUNAKAN MULTIPLE CRITERIA DECISION ANALYSIS (MCDA) INFORMATION SECURITY AWARENESS LEVEL MEASUREMENT USING MULTIPLE CRITERIA DECISION ANALYSIS (MCDA),” vol. 5, no. 1, pp. 15–24, 2014.