Measurement of Information Security Awareness Level: A Case Study of Digital Wallet Users

A L Fadhilah¹, Y Ruldeviyani², R Prakoso³ and K F Arisya⁴

¹,³,⁴Magister of Information Technology, Faculty of Computer Science, Universitas Indonesia
²Department of Information Technology, Faculty of Computer Science, Universitas Indonesia, Jl. Kenari 2 Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta, Indonesia

E-mail: amanda.lailatul@ui.ac.id

Abstract. Awareness of a person is an important factor in maintaining information security and reducing the fraud gap. The existence of various types of digital wallet application fraud requires someone to have an awareness of information security. This study was conducted to measure the information security awareness of digital wallet users. The research was conducted by distributing questionnaires to 156 respondents of digital wallet users. These respondents represented users of digital wallet applications in Indonesia. Information security was measured based on the user's knowledge-attitude-behavior. The assessment of information security awareness level was calculated using the Analytic Hierarchy Process (AHP) method. The results showed that the score was at the awareness level of good (80.78%). However, several focus areas still showed score at the average level which was one of the reasons why there are still many information security breaches against users of the digital wallet.

1. Introduction

The development of information technology has led to various innovations in various sectors. These innovations have brought significant changes to the way of living, working and communicating. No wonder these changes have led to a digital lifestyle. The technology-based financial sector or fintech also contributes to changes to a digital lifestyle. Nowadays, the digital wallet is one of the trending technology.

The popularity of digital wallet among the public is also high, this is showed by Dailysocial research that digital wallets (82.7%) were the most popular fintech product category according to respondents, followed by investment (62.4%), pay later (56.7%), and p2p lending that accommodated personal needs (40%). The same source also stated that 81.6% of the considerations for using digital wallets were based on respondents' trust in the product itself. 72.2% of respondents also tend to use it because of its suitability to their needs. Besides, 72.9% of respondents chose that digital wallets have the appropriate functionality. Then, 66.2% of respondents also stated that digital wallets were easy to use and 32.8% of using digital wallets could save time [1].

The continued growth of digital wallets and high popularity among the public has led to the rise of various types of fraud and deception mode on behalf of these service providers. This is evidenced by the Police report which stated that the high number of cases received in 2019 was online fraud. However, the police did not specifically mention the number of online deception figures, especially deception that occurred on digital wallet service. The mode of deception that is carried out can be in the form of
suspicious messages, phone calls and so on. From these messages or call, deceiver usually asks for OTP from customers, ask for personal data even ask for a balance transfer. Apart from deception, there are also cybercrimes in the form of digital wallet burglary. These cybercriminals usually perform these 3 types: impersonate and take over SIM cards (SIM Swab), Man-in-the-middle (MiTM) attacks and phishing and also malware attack [2].

The rise of various types of fraud and cybercrime modes related to digital wallet service shows the importance of public awareness of security in the cyberspace. In the research conducted by Ogutcu, et al., stated that security issues are not just a technological problem, but also human attitudes and behavior towards the use of information technology [3]. Therefore, public awareness of information security needs to be properly assessed and evaluated. This is useful to find out more about the scope of information security which still needs to be improved as a preventive measure and self-protection towards various types of fraud and data theft.

Kruger and Kearney have developed a model for measuring information security awareness, namely the Knowledge-Attitude-Behavior (KAB) model. This model is the most commonly used as a basic model for measuring information security [4]. Several studies have adopted the KAB model as a basis for measuring information security awareness, such as a study written by Parsons, et al. [5]. However, there is no specific research that discusses measuring the level of information security awareness for digital wallet users.

The purpose of this research is to find out the security awareness of Indonesians in cyberspace by testing their security level when using a digital wallet. The population of digital wallet users in this study represented the majority of Indonesian users.

2. Literature Review

2.1. Information Security

Information security is defined as the protection of information and information systems from unauthorized access, use, disclosure, interference modification, or destruction [6]. The concept of information security according to Andress is known as the CIA Triad, namely Confidentiality, Integrity, and Availability. Confidentiality is an important component of privacy and refers to an organization’s ability to protect the data of unauthorized persons. Integrity refers to the ability to prevent to not change illegally. Availability refers to the ability to access data when needed.

Meanwhile, according to Whitman and Mattord, Information Security is an organization that must have several layers of security to protect its operations. The security in question is as follows [7]:

- Physical security generally protects physical items or objects and areas from illegal access and abuse
- Personnel security generally protects an individual or group of individuals who have the authority to access the organization and its operation
- Operation security generally protects the details of a particular operation or series of activities.
- Communication security generally protects communication media, technology and content.
- Network Security generally protects network component, connection, and their contents.
- Information security generally protects confidentiality, integrity and availability of information assets, whether in terms of storage, processing or transmission. This is achieved through the application of policies, education, training and awareness, as well as technology.

2.2. Information Security Awareness

Information security awareness is characterized by understanding security policy, procedure and practice so that when security problems occur, the public can make appropriate judgments. Improve information security awareness is like implementing a security policy, taking preventive measures, improving user security behavior patterns, or changing routines so that they can implement habits related to information security [8].
Building a level of information security awareness is important because human behavior is considered to be the biggest threat of information security. Various types of information security threats arise due to human behavior such as carelessness and negligence in safeguarding information, unwise mobile use, access unsafe sites and handle the data that does not comply with security policies. This behavior can be risky internally and externally. It caused cybercrime and deception to steal confidential data [9].

2.3. Measurement of Information Security Awareness
Measuring information security awareness is a dynamic process. Risk and threat are constantly changing so that the measurement of information awareness needs to be continuously measured and updated to reflect changes in the risk profile.

The most popular information security awareness measurement model used is the model proposed by Kruger and Kearney. 3 dimensions serve as benchmarks for assessing information security awareness, namely Knowledge, Attitude, Behavior. Knowledge to measure what users know about information security. Having insights related to information security is an initial step in creating information security awareness. Attitude is to measure how users feel or think about the known risk of information security. Behavior is to measure what users do or actions regarding information security [4]. Table 1 is a scale of the level of awareness that is used to help define the level of awareness of the object studied.

| Table 1. Level of Awareness |
|-----------------------------|
| Level          | Result    |
| Good           | 80-100    |
| Average        | 60-79     |
| Poor           | <59       |

In the dimensions of Knowledge, Attitude and Behavior, it is focused on the variable focus area which refers to the variable developed by Parsons, namely Human Aspects of Information Security (HAIS-Q) [5]. Each dimension variable is measured to the 7 HAIS-Q variables, namely password management, email usage, use of the internet, use of social media, mobile device, information handling, and incident reporting.

2.4. Analytic Hierarchy Process Method
In this study, 3 area dimension variables and 7 focus area variables are used so that need a method that can calculate the validity up to the tolerance level for inconsistencies of various criteria and alternatives chosen by decision-makers that is Analytic Hierarchy Process (AHP). AHP is decision support using a basic approach. This approach is used to select the best number of alternatives that are evaluated based on several criteria [10]. It describes a complex multi-factor or multi-criteria problem into a hierarchy. Hierarchy is defined as a representation of a complex problem in a multilevel structure where the first level is the goal, then the factor level, criteria, sub-criteria, and so on until the last level of alternatives [11]. Data quality from respondents takes precedence over quantity data when applying the AHP method. The sample size in the AHP method does not have a specific formula or standard [12], there is a general consensus that the AHP does not require a very large sample [13]. Figure 1 shows the hierarchy of AHP.

3. Methodology
This section discussed the research stages, research instruments, data collection, hierarchical structure design, and data analysis techniques. The detail of each point explained below.

3.1. Research Stages
This section shows the stages taken in this study. Each stage explained below:
Determine the problem. The first thing to do was to determine the problem that was researched. In this case, it also looked for facts about the problem and determined the research objectives.

- Literature study. At this stage, looking for various things or information that was relevant in the research, including searching for several previous studies that have similar topics or were related to this research.
- Make a research design. The research design made was compiling a hierarchical structure for the implementation of the AHP. In this hierarchical structure, the KAB (knowledge, attitude and behavior) model acted as a criterion and the HAIS-Q (human aspect information security questionnaire) acted as an alternative.
- Create questions and distribute questionnaires. After determining the research design, the next step was to create a questionnaire question. The questionnaire refers to two variables, namely the dimensional variable and the focus area variable. Furthermore, the questionnaire was distributed online by having predetermined criteria for respondents.
- Processing data and analysis. The next stage was processing the data from the questionnaire and analysis. The data processing technique used was AHP. After getting the research results, the results were analyzed.
- Conclude. In this stage, conclusions can be drawn based on the data that has been collected and analyzed. At this stage, several recommendations were also given that could be made to improve information security awareness.

![Hierarchy of AHP](image)

**Figure 1. Hierarchy of AHP**

| Scale | Category                                     |
|-------|----------------------------------------------|
| 1     | Strongly disagree / very negative / very never |
| 2     | Disagree / negative / almost never            |
| 3     | Neutral / hesitant / sometimes                |
| 4     | Agree / positive / syringe                    |
| 5     | Strongly agree / very positive / always       |

**Table 2. Likert Scale**

3.2. Research Instrument

The questionnaire was created using Google form and consisted of 55 questions consisting of 51 questions regarding information security and 4 questions which represent the criteria for respondents such as age, latest education, occupation and gender. The 51 questions regarding information security relating to 3-dimensional variables and 7 focus area variables. The questionnaire was translated into the Indonesian to ensure broader coverage. Google form is also set to only accept one response to prevent duplicate respondents. Respondents were asked to fill out the questionnaire using a Likert Scale with a
scale of 1 to 5. The Likert Scale was designed to measure attitudes in a scientifically accepted way and validated in 1932 [14]. Table 2 is the Likert Scale table used.

3.3. Data Collection
The questionnaires were distributed randomly online using random sampling techniques and met the requirements of using a digital wallet application in Indonesia. According to Arif Rahman, random sampling has several assumptions that the population is known as a whole, the sample is drawn randomly from the population, and each member of the population has an equal chance of being sampled [14]. The respondent's data were then processed using the Analytic Hierarchy Process and the results could be drawn a conclusion and analysis.

3.4. Hierarchical Structure Design
AHP has a hierarchical structure which is one of the stages to use in this method. The top hierarchical structure is the purpose of the decisions taken, then the next level is the criteria and the lowest level is the alternative [4]. Figure 2 is the hierarchical structure used in this study.

![AHP Hierarchy Structure](image)

The highest level of the structure is knowing the level of information security, the next level is the criteria that is filled with 3-dimensional variables (knowledge, attitude, behavior) and the lowest level is 7 focus area variables (password management, email usage, use of the internet, use of social media, mobile device, information handling, and incident reporting).

3.5. Data Analysis Technique
After the respondent's data collected, Kruger and Kearney measure the weight of the dimensions and focus areas using AHP. The value of the dimensional variable weight that is used in this study refers to the weight that has been made by Kruger and Kearney [4]. Table 3 represents the weight that was used in the dimensional variable.

| Table 3. Dimensional Weight |
|-----------------------------|
| Dimension | Weight (%) |
| Knowledge   | 30          |
| Attitude    | 20          |
| Behavior    | 50          |

Determining the weight of the focus area variable requires expert consideration to fill the pairwise of the comparison matrix [10]. An expert in information security from the University of Indonesia was
interviewed to get a priority scale between the focus area variables. Table 4 is the weight of the focus areas used in this study.

The score of each focus area per dimension was calculated and normalized to the sum of one. The total score, \( v(a) \), was determined using the formula below [4]:

\[
V(a) = \sum_{i=1}^{g} v_i(a) w_i \tag{1}
\]

| Focus Area             | Weight (%) |
|-----------------------|------------|
| Password Management   | 17.36%     |
| Email Usage           | 7.69%      |
| Use of Internet       | 5.22%      |
| Information Handling  | 25.30%     |
| Mobile Device         | 15.40%     |
| Use of Social Media   | 15.40%     |
| Incident Reporting    | 13.62%     |

After obtained the value from the awareness level of the digital wallet application users, the value was grouped into 3 categories of information security awareness level [4]. Table 5 represents the value categories that are used and the colors used in the results table. The function of giving color to the table is to make it easier to read the table and provide detailed information so that it can make it easier to take action for each dimension and focus area.

| Score (%) | Information                              | Colour          |
|-----------|------------------------------------------|-----------------|
| 80-100    | Satisfactory, does not require action/improvement |                 |
| 60-79     | Monitor, potentially requiring action/improvement |                 |
| 0-59      | Not satisfactory, requires action/improvement |                 |

4. Result and Discussion

The questionnaire was distributed online to the general public but the respondent has used a digital wallet application. The number of respondents was 156, representing users of digital wallet applications in Indonesia.

The results of measuring the average information security awareness of digital wallet application users can be seen in Table 6. The total score is 80.78%. The result of the measurement is categorized into the good category according to the metering of the level of information security awareness used by Kruger and Kearney [4]. This showed that the information security awareness of digital wallet application users was satisfactory so that no action is needed to improve information security awareness.

Although the overall showed the good category, several focus areas need attention. The focus area of "use of social media" had the lowest average level of awareness of 73.35%. Some respondents still considered that displaying a phone number on social media was an action that would not interfere with their information security. Although this action is quite risky. When other people know someone's phone number, this will be a fraud gap to be able to log in by getting an OTP number from the victim.

The focus area of "use of internet" and "information handling" also still needs attention because each dimension is categorized into an average level and has the potential to take action to improve information awareness. The lowest value in the focus area of "use of internet" was on the knowledge dimension, which was 70.67%. It may some respondents were not aware that there could be a fake application that
acts on behalf of the digital wallet service so that they provide their data to the fake application. Many respondents also might access digital wallet applications with a free VPN from the application store. Besides, respondents were also not aware that entering personal data on online sites that lured digital wallet balance vouchers that could compromise their personal data. Meanwhile, the lowest value in the focus area of “information handling” was on the behavior dimension, which was 75.32%. Many respondents still stored important information about digital wallet accounts such as PINs on their phones without providing protection. This is quite risky when someone accesses their phone and accidentally opens information about a digital wallet account.

### Table 6. Measurement Results of Information Security Awareness

| Focus Area            | Dimension  | Total Awareness |
|-----------------------|------------|-----------------|
|                       | K          | A               | B           |
| Password Management   | 89.26%     | 87.98%          | 76.92%      | 82.84% |
| Email Usage           | 71.15%     | 77.56%          | 85.58%      | 79.65% |
| Use of Internet       | 70.67%     | 76.92%          | 78.85%      | 76.01% |
| Information Handling  | 77.24%     | 79.17%          | 75.32%      | 76.67% |
| Mobile Device         | 92.31%     | 90.06%          | 86.22%      | 88.81% |
| Use of Social Media   | 76.37%     | 79.12%          | 69.23%      | 73.35% |
| Incident Reporting    | 90.97%     | 90.38%          | 83.33%      | 87.03% |
| **Total**             | **82.69%** | **83.75%**      | **78.44%**  | **80.78%** |

The last focus area that needs to be considered was “email usage”, because the score of the knowledge and attitude dimensions still showed the category of needing supervision, 71.15% for the knowledge dimension and 77.56% for the attitude dimension. There were still many respondents who deliberately entered their data because they were lured with reward through fake email notifications on behalf of the digital wallet service. They also might not understand the threat of email containing malware.

Although none of the dimensions and focus areas showed the poor category, digital wallet service providers need to make some improvements in several focus areas with the average category by the following recommendations:

- Based on focus area of information handling and email usage that has an average score and needs some improvements, so that digital wallet service providers need to provide education to users periodically. This is important to do because unconsciously users tend to do things that can threaten the security of their digital wallets. This education can be in the form of an appeal not to put a phone number on social media, then not to store important information about digital wallets on phone, and an appeal to only trust the official website or email of a digital wallet service provider. The hopes that digital wallet users always remember to keep their data security.
- Based on focus area use of internet that the score still on average and needs an action such as the digital wallet service providers may add policies for digital wallet users. One of the policies that need is to prohibit users from accessing digital wallet applications using a free VPN from the application store. Cybersecurity observers said that using a free VPN can be risky. The types of risks are also varied, such as VPN traffic can easily spread advertisements or malware, the other risk is robbery and data leaks [16]. So that digital wallet providers need to strictly prohibit their users from accessing digital wallets using a free VPN.

5. Conclusion
The measurement of information security awareness to digital wallet application users using the KAB model has been successfully delivered. The KAB model assessed 3 dimensions that are Knowledge,
Attitude, Behavior and 7 focus areas that are password management, email usage, use of the internet, and use of social media, mobile device, information handling, and incident reporting. The results showed that the total score of the respondents' category of awareness was at the good. However, focus areas such as “use of social media”, “use of internet”, “information handling”, and “email usage” still showed average scores or require supervision.

Although there are no dimensions and focus areas that indicate a poor category, these actions are still needed to increase the level of user awareness in several focus areas with an average score. Such as an action to provide education to users regarding appeal not to carelessly display a phone number and reminding them to properly store valuable information, then not easily trusting fake sites and emails. It can also create policies that strictly prohibit the use of free VPN when opening digital wallet applications.

Acknowledgments
This research was supported by PUTI Q2 grant “Measurement of Information Security Awareness Level: A Case Study of Digital Wallet Users” (NKB-850/UN2.RST/HKP.05. 00/ 2020). We would express our gratitude to the Faculty of Computer Science and Directorate of Research and Community Engagement, Universitas Indonesia.

References
[1] DSresearch 2019 Moving towards a New Era in Indonesia's Financial Industry (Electronic Materials) (Jakarta: Daily Social)
[2] Nugroho A 2020 Three Attacks Used to Break Digital Wallets (Electronic Materials) (Jakarta: cyberthreat.id) [in Indonesian]
[3] Öugütçü G, Testik Ö Z and Chouseimoglu O 2016 Analysis of personal information security behavior and awareness Comput. Secur. 56 pp 83–93
[4] Kruger H A and Kearney D W 2006 A prototype for assessing information security awareness Computers & Security pp 289–96
[5] Parsons K, McCormac A, Butavicius M, Pattinson M and Jerram C 2014 Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q) Comput. Secur. 42 pp 165–76
[6] Andress J 2011 The Basics of information security: understanding the fundamentals of infosec in theory and practice (Amsterdam: Elsevier)
[7] Whitman M E and Mattord H J 2012 Principle of Information Security 4th Edition (Boston: Thomson Course Technology)
[8] Fakeh S K W, Zulhemay M N, Shahibi M S, Ali J and Zaini M K 2012 Information security awareness amongst academic librarians J. of Applied Sciences Research 8(3) pp 1723–35
[9] Bauer S, Bernroider E W N, and Chudzikowski, K. 2017 Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks Computers and Security 68 pp 145–59
[10] Saaty T L and Vargas L G 2012 Models, Methods, Concepts & Applications of the Analytic Hierarchy Process 2nd ed (New York: Springer)
[11] Saaty T L 2008 Decision Making with the Analytic Hierarchy Process Int. J. Services Sciences pp 83–98
[12] Saaty T L 2012 Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in A Complex World 5th ed (Pittsburgh: RWS Publication)
[13] Schmidt K, Aumann I, Hollander I, Damk K and Von Der Schulenburg J M G 2015 Applying the Analytic Hierarchy Process in healthcare research: A systematic literature review and evaluation of reporting BMC Med. Inform. Decis. Mak. 15 p 112
[14] Edmondson D R 2005 Likert scale: a history Conf. on Historical Analysis and Research in Marketing pp 127–33
[15] Rahman A 2013 Randomized random sampling with an inverse-transform random variate generator approach based on the hypergeometric distribution Seminar Nasional TEKNOIN 4 pp 106–11 [In Indonesian]

[16] Jakartapost 2019 Risks of using VPN and why it’s difficult to stop (Electronic Materials) (Jakarta: thejakartapost.com)