Journal of Computer Science, Information Technology and Telecommunication Engineering (JCoSITTE)
Vol. 6, No. 2, September 2020, pp. 916~922
ISSN: 2721-3838, DOI: 10.30596/jcositte.v6i2.26050

Measurement of Security Awareness Level in the Implementation of Quick Response Code Indonesian Standard

Milda Safrila Oktiana[1*], Avinanta Tarigan[2]
[1]Master in Information Systems Management, Universitas Gunadarma, Depok, Indonesia
[2]Faculty of Computer Science and Information Technology, Universitas Gunadarma, Depok, Indonesia

ABSTRACT

Quick Response Code Indonesian Standard (QRIS) is a QR code standard adopted in Indonesia as an electronic payment method. QRIS allows users to make payment transactions easily using mobile phones. Although QRIS provides many benefits regarding ease and efficiency of transactions, there are some security risks from payment methods using QR codes. A lack of public awareness regarding the safety of using QRIS can open the risk of misuse by irresponsible parties. This study aims to measure the level of security awareness in using QRIS Merchants in the DKI Jakarta areaThe research data was collected using questionnaires based on the Kruger and Kearney models involving 3 (three) dimensions, namely knowledge, attitudes, and behavior, as well as 6 (six) focus areas. The number of samples obtained was 110 respondents. The results showed that the safety awareness of QRIS use in the DKI Jakarta area was 91, in the average value category. With an average score of 91, most respondents realize the importance of paying attention to security aspects in transacting using QRIS.

Keyword: Electronic Payment; QRIS Merchant; Security Awareness; User Behavior

Corresponding Author:
Milda Safrila Oktiana
Master in Information Systems Management
Universitas Gunadarma
Margonda Raya street, Depok, Indonesia
Email: mildaokt21@gmail.com

Article history:
Received Jul 25, 2025
Revised Aug 20, 2025
Accepted Aug 26, 2025

1. INTRODUCTION

Bank Indonesia has formulated three primary strategies for the payment system in the digital economy era to support the growth of the digital economy as a new driver of economic expansion. One of these strategies involves the electronification of financial transactions, which refers to the shift from cash-based to non-cash payment methods. The adoption of non-cash payments has become increasingly prevalent among Indonesian communities, spanning both urban and rural areas (Setiyono, 2020; Utami, 2024). Non-cash money is considered more effective as a means of payment transactions and is the primary driver of economic growth today. This is marked by an increase in the provision of the QR Code Indonesian Standard (QRIS) as a merchant transaction tool (Sriekaningsih, 2020).

The use of QRIS as a digital payment method has seen significant growth and widespread adoption among both merchants and users. According to Bank Indonesia, by February 2023, the number of merchants utilizing QRIS had reached 24.9 million, while the total number of users stood at 30.87 million. In addition, the value of QRIS transactions recorded up to February 2023 amounted to IDR 12.28 trillion, with a total transaction volume of 121.8 million (Bank Indonesia, 2023). Although it provides many benefits regarding efficiency and ease of transactions, QRIS carries security risks such as fraud and cyber attacks, so QRIS users need to understand the risks of using this payment method. New fraud modes using QRIS occur in several places. The perpetrators forged QR codes on mosque charity boxes, shopping centers, public fuel filling stations, and airport areas and raised around Rp. 13 million from April 1-10, 2023 (Saskia and Pertiwi, 2023). User awareness of QRIS security involves understanding related security issues. In facing these security challenges, efforts to increase public awareness must be carried out through education, security certification, technology improvement, and security reporting.

Security Awareness has been a widely discussed topic, including Information Security Awareness. Many factors influence a person in applying security awareness correctly, such as the person's habits or characteristics, traits, and behavior (Lebek, et al., 2014). Until recently, the human aspect of information security research typically focused on understanding human vulnerability at the individual level by exploring specific characteristics that may relate to and influence information

security behavior (McCormac, et al., 2017). Taufiq and Betty (2023) emphasizes that security awareness is not only influenced by individual traits but also by the level of knowledge and understanding of specific technologies or systems. In line with this, Nabila, et al. (2025) highlight that strengthening system security and user trust plays a crucial role in encouraging the adoption of secure digital payment platforms.

Building on this foundation, the current study seeks to measure the level of awareness among QRIS Merchant users regarding the safety of QRIS usage. Additionally, it aims to explore the relationship between users' knowledge, awareness, and their QRIS usage habits. The research will also investigate potential differences in QRIS awareness levels and usage habits based on demographic factors such as gender, age, educational background, and monthly income, and how these factors influence the overall level of security awareness. This comprehensive approach aims to provide insights into how demographic variables and individual characteristics shape security awareness and behaviors in the context of QRIS usage.

2. RESEARCH METHOD

The research conducted is a quantitative research using a survey approach. The survey is conducted by distributing questionnaires to a sample of a predetermined population. The questionnaire has 36 questions arranged based on the Kruger & Kearney Model with three dimensions of research: knowledge, attitude, and behavior. Each dimension has six common focus areas: password management, internet usage, mobile devices, software, information handling, and incident reporting (Kruger & Kearnet, 2006). Each dimension will be represented by 12 questions arranged based on six focus areas.

Validity and reliability testing will be conducted against the questionnaire. Validity is the degree of accuracy between the data that occurs in the research object and the data that researchers can report [4]. A validity test is carried out on each question item; the r-count result is compared with the r-table (where df = n – 2 with significance = 5%); if the r-table is less than the r-count, then the question item on the questionnaire is declared valid. Reliability refers to the stability and consistency of respondents' answers to questions that represent specific constructs; these constructs are dimensions of a variable organized within a questionnaire form (Hardani, et al., 2020). Reliability tests are carried out jointly on all question items; if Cronbach's Alpha value is more significant than 0.70, all question items are considered reliable.

The research questionnaire was created using the Google Form platform and will be shared with respondents either directly or via social media and other communication channels. Respondents are expected to provide answers to all questions included in the questionnaire. The data collection process is conducted in a single stage or within a designated timeframe.

The population in this study is people in DKI Jakarta province who own or work in micro, small, or medium enterprises and use the QRIS payment method to receive payments. The determination of this province is based on the province with the highest number of QRIS merchants in Indonesia. The sample size is determined using Roscoe's theory, which suggests that for multivariate analyses, such as correlation or multiple linear regression, the number of samples should be at least ten times the number of variables being analyzed (Sugiyono, 2018). The follow-up analysis in this study involved five variables, with one dependent variable and four independent variables. Therefore, the minimum number of sample members required is 50 respondents.

The questionnaire results will be processed by calculating the security awareness score for each respondent based on answers from the instrument used to measure the level of security awareness. The weighting is determined using the Analytical Hierarchy Process (AHP) (Akraman, et al., 2018). The AHP employs pairwise comparisons to generate subjective assessments of various factors, relying on the judgments and perspectives of management professionals (Fauzi, et al., 2020). Each dimension will have its weight used in the calculation of consciousness. The division of weights for dimensions can be seen in Table 1.

Table 1. Dimension Weight Division (Kruger & Kearney, 2006)

Dimension	Weight
Knowledge	30%
Attitude	20%
Behavior	50%

The calculation of the level of security awareness is divided into five stages, namely the summation of the value of questions filled in by respondents for each focus area in each dimension, the calculation of the awareness value for each focus area in each dimension, the calculation of the total value of awareness of the focus area, the calculation of the total value of dimensional awareness and the calculation of the overall awareness value.

1. The first stage, namely the sum of the question values filled in by respondents for each focus area in each dimension, can be calculated through equation (1).

$$JNJ = NJ_1 + NJ_2 + NJ_3 + \cdots + NJ_n \quad (1)$$

2. The second stage calculates the value of consciousness for each focus area in each dimension through the following equations (2) and (3).

$$TJNJ = \left(\frac{JNJ_1}{JBP_i}/10\right) + \left(\frac{JNJ_2}{JBP_i}/10\right) + \left(\frac{JNJ_3}{JBP_i}/10\right) + \ldots + \left(\frac{JNJ_n}{JBP_i}/10\right) \quad (2)$$

$$NKAF = \frac{TJNJ}{JR} x\ 100 \quad (3)$$

3. The third stage is calculating the total value of consciousness for each focus area through equation (4). The total value of consciousness ranges from 0 – 100 (in percent).

$$TNKAF = (NKAF_1\ x\ 0{,}3) + (NKAF_2\ x\ 0{,}2) + (NKAF_3\ x\ 0{,}5) \quad (4)$$

4. The fourth stage is calculating the total value of consciousness for each dimension through equation (5). The total value of consciousness ranges from 0 – 100 (in percent).

$$TNKD = (NKD_i + NKD_i + \ldots + NKD_i)/i \quad (5)$$

5. The fifth stage is the calculation of the value of consciousness as a whole as the final result of the value of consciousness through equations (6), (7), and (8). The total value of consciousness ranges from 0 – 100 (in percent).

$$RTNKAF = (TNKAF_i + TNKAF_i + \ldots + TNKAF_i)/i \quad (6)$$

$$RTNKD = (TNKD_1\ x\ 0{,}3) + (TNKD_2\ x\ 0{,}2) + (TNKD_3\ x\ 0{,}5) \quad (7)$$

$$NKS = \frac{RTNKAF}{RTNKD} \quad (8)$$

From the calculation of the level of awareness obtained, a representative value of the level of security awareness of QRIS use will be accepted, which will be evaluated according to the criteria listed in Table 2.

Table 2. Criteria of Awareness (Kruger & Kearney, 2006)

Criteria	Scores (%)	Description
Good	95 – 100	It's been good, it needs to be maintained.
Average	80 – 94	Good enough, but still open opportunities for improvement.
Bad	Less than 80	It needs special attention to improvement efforts.

3. RESULTS AND DISCUSSION

The results of research instrument testing are conducted to test the validity and reliability of measurement tools used in research. This test is carried out to ensure that the research questionnaire can produce accurate and reliable data. Validity and reliability tests are two important aspects of research instrument tests that aim to ensure that the research questionnaires are of good quality and reliability.

The test was conducted on 36 questions in a questionnaire filled out by 30 respondents, using the RStudio Application for data processing. If all questions are declared valid and reliable, the questionnaire will be distributed to respondents in the research sample. In the validity test, Pearson's product-moment correlation relates each question to the total value of each question category. The accepted standard Pearson or r-count value for the validity test must be greater than the r-table value. For a validity test with 30 respondents and a significance level of 5%, the accepted r-table value was 0.361. The test results found that 36 questions on the questionnaire had an r-count value more significant than the r-table so that all questionnaire questions could be declared valid.

In reliability testing, the value to be taken is Cronbach's Alpha (α), an internal consistency index of the overall measurement scale. The accepted standard Cronbach's Alpha (α) score so that the questions on the questionnaire are said to be reliable or reliable is > 0.70. From the reliability test results, it was found that 36 questions on the questionnaire received a Cronbach's Alpha (α) score of 0.787, so all questions were declared reliable or reliable. Based on the results of the validity test and reliability test, it can be concluded that all questions in the questionnaire are declared valid and reliable so that the questionnaire can be distributed to respondents in the research sample.

A. Characteristics of Respondents

This study's total number of respondents was 110 after the data cleaning process. Table 3 contains respondents' characteristics in various categories according to demographic information, including gender, age, education, income, and business fields.

Table 3. Characteristics of Respondents

Characteristics	Total	Percentage
Gender		
Male	47	42,73%
Female	63	57,27%
Age		
21 – 25 years old	32	29,09%
26 – 30 years old	33	30,00%
31 – 40 years old	23	20,91%
Above 40 years old	22	20,00%
Education		
Graduated Senior High School	52	47,27%
Graduated Diploma	19	17,27%
Graduated Bachelor	39	35,46%
Monthly Income		
Rp. 1.000.000 - Rp. 2.999.999	19	17,27%
Rp. 3.000.000 - Rp. 4.999.999	51	46,36%
Rp. 5.000.000 - Rp. 9.999.999	34	30,91%
Rp. 10.000.000 - Rp. 14.999.999	6	5,46%
Business Field		
Electronic	13	11,82%
Fashion	10	9,09%
Furniture	6	5,46%
Health	8	7,27%
Food	73	66,36%

B. Questionnaire Processing Results

The process of processing the questionnaire consists of two stages. The first stage involves processing the data from disseminating questionnaires to generate a security awareness level score. After that, in the second stage, an analysis will be carried out to determine the effect of different demographic factors of respondents on the level of security awareness in using QRIS.

a. Security Awareness Score Results

The security awareness score calculation results can be seen in Table 4. This security awareness score includes scores from each dimension and area of focus, which then generates an overall security awareness final score.

Table 4. QRIS Usage Security Awareness Level Score

	Knowledge (30)	Attitude (20)	Behavior (50)	Total Awareness Score/Area Focus
Password Management	84	88	77	83
Internet Usage	86	94	91	91
Mobile Devices	99	95	95	96
Software	91	91	92	91
Information Handling	87	88	87	87
Incident Reporting	95	99	99	98
Total Awareness Score/Dimension	90	93	90	91

In this study, the overall score of security awareness of using QRIS Merchant as a payment recipient transaction reached 91, which was categorized into the average value. Each dimension, namely knowledge, attitude, and behavior, has a security awareness score in the average value category of 90 to 93. Of the six focus areas, two have good value categories, namely Mobile Devices and Incident Reporting, with a range of 95 to 99. This shows that security awareness related to these two focus areas is good enough and needs to be maintained, while other focus areas, such as Password Management, Internet Usage, Software, and Information Handling, even though they are already in the average value category, still have the opportunity to be able to increase the value of security awareness.

b. Multiple Linear Regression Results

In Table 5, we can see the results of multiple linear regression, which aims to find demographic factors that affect the different levels of security awareness of QRIS usage.

Table 5. Multiple Linear Regression Results

Gender	-3.1531
(Female)	-0.1966
Age	0.4763
(> 30 Years old)	0.0291
Education	2.2923
(Graduated Diploma/Bachelor)	0.1435
Monthly Income	-0.3099
(≥ Rp. 5.000.000,-)	-0.0185
Constant/Intercept	91.756
	-2.197e-16
R^2	0.058
Highest VIF	1.111158
Mean VIF	1.065608
Ramsey RESET Test	0.097876
Observation	106

From the diagnosis results in the initial iteration, five outliers were not included in the next iteration, leaving 106 respondents who became the final regression analysis model. The factor that has the most significant influence is gender and followed by the last education. If all factors are equal, QRIS Merchant users who are female will have a score of 3.1 points lower than the male gender, while for the last education, QRIS Merchant users who are at the Graduated Diploma/Bachelor level have a score of 2.3 points higher than QRIS Merchant users who are at the Graduated Senior High School.

Meanwhile, the security awareness score remained the same regarding other factors, such as age and monthly income. Regarding age, QRIS Merchant users over 30 have scored 0.5 points higher than QRIS Merchant users under or equal to 30 years old. In the monthly income factor, QRIS Merchant users with a monthly income of more than or equal to Rp. 5.000.000,- of 0.3 points lower than QRIS Merchant users with a monthly income of less than Rp. 5.000.000,-.

The value of R Squared (R^2) is the value of influence given by the independent variable to the dependent variable simultaneously or together. The VIF value is obtained from each independent variable for the multicollinearity test. The Ramsey RESET Test value is the value of a statistical test known as the Ramset Regression Equation Specification Error Test. Finally, the observation value is the amount of respondent data processed in multiple linear regression analysis.

c. Visualization of Demographic Factors Results

Based on the results of multiple linear regression of four demographic factors on the safety awareness of QRIS Merchant use, the visualization results will be presented in the form of plots to show the effect. The visualization of four demographic factors can be seen in Figure 1.

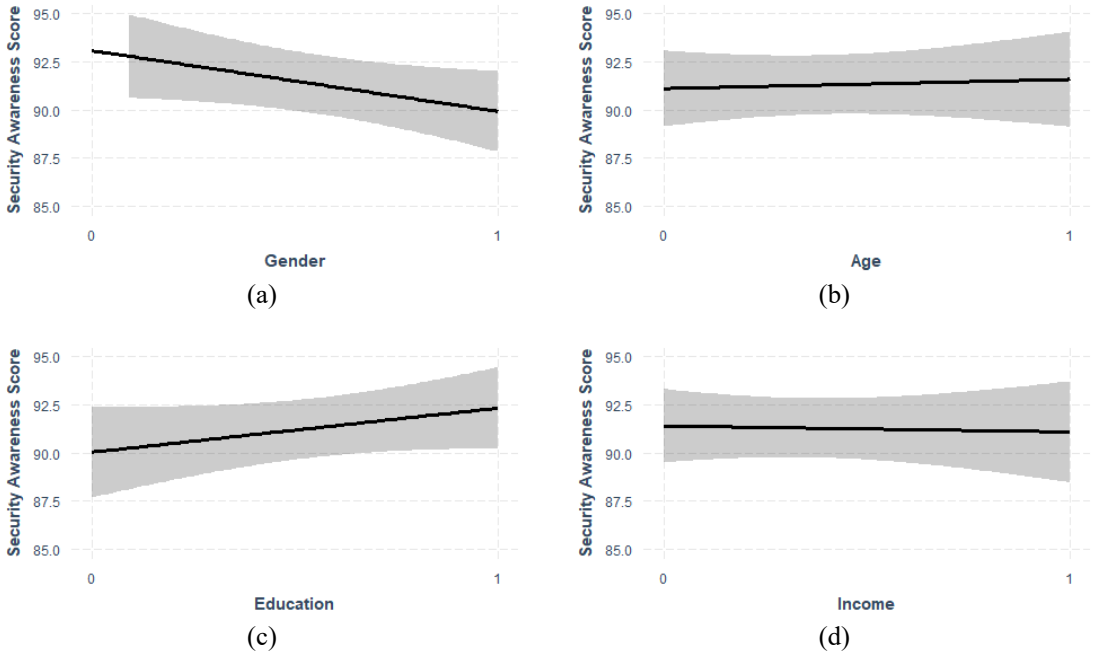

Figure 1. Visualization of the influence of factors against (a) Gender; (b) Age; (c) Education; and (d) Income

Based on the visualization results, it is known that of the four demographic factors, two factors significantly influence security awareness scores, there are gender and education. In contrast, the factors that less influence security awareness of QRIS Merchant use are age and income. There are several reasons why gender and recent education have a more significant influence on QRIS safety awareness.

Differences in safety awareness between the sexes can be due to differences in behavior and preferences regarding technology and safety. Research shows that male respondents are more cautious and concerned about QRIS security. A person's education level can also influence security awareness and understanding of security threats and practices in using QRIS. Users with higher education tend to have access to more information. They can better understand the risks and recommended security practices, so they are more likely to be better able to implement appropriate security measures in using QRIS as a means of payment acceptance transactions.

4. CONCLUSION

Based on the research that has been conducted, it is known that the knowledge score about security awareness of QRIS use is 90, which is in the average value category. The attitude score about security awareness of QRIS use is 93, which is in the average value category, and the behavior score about security awareness of QRIS use is 90, which is in the average value category. From the total security awareness score of QRIS use, it is known that the security awareness of QRIS Merchant use in the DKI Jakarta area is 91, which is in the average value category. The score results that show the average score category conclude that the user habits assessed are good enough based on the questions answered on the questionnaire.

From the six focus areas, four focus areas still need to increase security awareness in using QRIS, namely in terms of Password Management, Information Handling, Internet Usage, and Software. In these four areas, efforts need to be made in the form of user education to increase security awareness in avoiding threats that can occur.

Then, this study also discusses and finds differences in the level of security awareness of QRIS use based on demographic factors such as gender, age, education, and monthly income. QRIS Merchant female users have a lower level of security awareness than male users. QRIS Merchant users over 30 years old have a higher security awareness than users under or equal to 30 years old. QRIS Merchant users at the Graduated Diploma/Bachelor level have a higher security awareness than users with Graduated Senior High School levels. Finally, QRIS Merchant users with a monthly income above or equal to Rp. 5.000.000,- have a lower level of security awareness than users with income below Rp. 5.000.000,-

REFERENCES

Akraman, R., Candiwan, C., & Priyadi, Y. (2018). Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia. Jurnal Sistem Informasi Bisnis, 8(2), 115-122, doi: 10.21456/vol8iss2pp115-122

Bank Indonesia. (2023). *Bank Indonesia Edukasi Masyarakat dan Pedagang/Merchant Agar Terhindar dari Upaya Penyalahgunaan QRIS* [Online]. Available at: https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_259323.aspx

Fauzi, F., Al-Khowarizmi, A. K., & Muhathir, M. (2020). The e-Business Community Model is Used to Improve Communication Between Businesses by Utilizing Union Principles. *JITE (JOURNAL OF INFORMATICS AND TELECOMMUNICATION ENGINEERING)*, *3*(2), 252-257.

Hardani, et al, (2020). *Metode Penelitian Kualitatif & Kuantittif*. Yogyakarta: CV Pustaka Ilmu Grup.

Kencana Sari, P., & Candiwan. (2014). Measuring information security awareness of Indonesian smartphone users. *Telkomnika (Telecommunication Computing Electronics and Control)*, 12(2), 493–500, doi: 10.12928/TELKOMNIKA.v12i2.2015

Kruger, H. A., and Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, 25(4), 289-296, 2006, doi: 10.1080/10691898.2019.1665485

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M., H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, 37(12): 1049-1092.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151-156. doi: 10.1016/j.chb.2016.11.065

Nabila, A. P., Raharso, S., Tiorida, E., (2025). The Influence of Trust and Transaction Security on Interest in Using The QRIS Payment System. *Airlangga Journal of Innovation Management*, 06(2), 248-260. doi: https://doi.org/10.20473/ajim.v6i2.72597

Saskia, C., & Pertiwi, W., K. (2023). *Modus Penipuan QRIS Palsu, Pengamat Usulkan Standar Keamanan Perbankan* [Online]. Available at: https://tekno.kompas.com/read/2023/04/13/17370087/modus-penipuan-qris-palsu-pengamat-usulkan-peningkatan-standar-keamanan

Setiyono, T., A. (2020). Indonesian's Acceptance of Non-Cash Transaction Using QRIS. *Economics, Business and Management Research,* 169, 141-144.

Sriekaningsih, A. (2020). *QRIS dan Era Baru Transaksi Pembayaran 4.0*. Yogyakarta: ANDI.

Sugiyono. (2018). *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta.

Taufiq, R., & Betty, P. (2023). Measurement of Information Security Awareness Level: A Case Study of Mobile Banking App Users to Prevent Social Engineering, *Journal of Syntax Idea*, 5(1), 86-98.

Utami, B. (2024). The Impact of the QRIS Payment System on the Digital Economy Development. *Jurnal Ekonomi dan Bisnis*, 1(3), 141-148.