

Mitigating the Risk of Quishing Threats (QR Phishing) using the Security Behavior Intentions Scale (SeBIS) in supporting digital economic security

A. We Tenri Fatimah Singkeruang ^{1*}, Setya Ega Susanto ² Nuraeni Saeni ³
wetenrifatimah@gmail.com ^{1*}, setyaegasusanto@gmail.com², enysaeni565@gmail.com ³

Bisnis Digital, Institut Bisnis dan Keuangan Nitro, Indonesia^{1*}.
Perdagangan Internasional, Institut Bisnis dan Keuangan Nitro, Indonesia².
Manajemen, Institut Bisnis dan Keuangan Nitro, Indonesia³

Abstract

The object of research is the risk mitigation of Quishing (QR Phishing) in financial transactions using the Security Behavior Intentions Scale (SeBIS). The study focuses on how user behavior, financial security awareness, and technological adoption influence the ability to detect and mitigate Quishing threats. One of the most problematic areas is the growing vulnerability of digital payment users to fraudulent QR codes, which cybercriminals exploit to redirect users to malicious websites and steal sensitive financial information. Despite the rapid adoption of QR-based payments, primarily through Quick Response Indonesia Standard (QRIS) and e-wallets, there is a lack of comprehensive risk mitigation models that integrate user awareness, behavioral factors, and security technologies. The study used a quantitative approach with Structural Equation Modeling (SEM) to analyze the relationships between security behavior, user awareness, and Quishing risk mitigation. Data was collected from 100 respondents in Makassar, Indonesia, to evaluate their digital security practices and susceptibility to Quishing attacks. The results indicate that password management and user awareness significantly influence Quishing risk mitigation, whereas device security alone does not guarantee protection. The study confirms that digital financial resilience can be enhanced through targeted education, stronger authentication mechanisms, and AI-driven fraud detection. This is because the proposed integration of SeBIS-based behavioral assessment and security interventions addresses multiple vulnerabilities in digital transactions. This ensures that it is possible to improve the overall security of digital payments by enhancing user behavior and implementing proactive security measures. Compared to similar known models, this approach combines behavioral insights with technological solutions, leading to more effective mitigation strategies for financial cybersecurity risks.

Kata Kunci: *digital economy; security behavior; Quick Response Indonesia Standard (QRIS); Quishing; QR Code.*

 This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

Introduction

In today's digital era, the digital economy has become one of the main drivers of growth and innovation. Initially developed for high-speed tag scanning, QR codes are not an entirely new design. However, they were not widely used before the requirement for touchless interactions, namely the COVID-19 pandemic (tai-wei, 2011). Surnames and names of the authors of the sources used are not mentioned directly in the text; references to the number of their work in the list of references are sufficient. However, with the rapid development of technology, various security threats have emerged that can disrupt this ecosystem. One of the increasingly disturbing threats is Quishing (QR Phishing), where phishing attacks use QR codes to deceive users and direct them to fake or malicious websites. This threat poses a serious risk to individuals and organizations in the digital economy. To address this risk, it is essential to understand individual behavior when dealing with digital security threats. More effective risk mitigation strategies can be developed by

understanding individual intentions in adopting digital security behaviors. The Security Behavior Intentions Scale (SeBIS) is used to help understand and measure individual intentions regarding digital security (Egelman, 2015). The practice of “squishing” or phishing with malicious QR codes (i.e., QR codes that embed malicious URLs) is not new but has so far affected a small number of victims and has never received much attention (Chouinard, 2021). However, quishing became popular when QR codes became an important intermediary for sharing information (Federal Bureau of Investigation, 2022). In Indonesia, the potential for Quishing can be seen from several cases published in online media (Fig. 1, 2).



Fig. 1. The perpetrator attached a fake QRIS sticker (CNN Indonesia)



Fig. 2. Alleged fraud stickers appear containing an invitation to scan barcodes to get free E-Toll (Jasamargatollroadoperator)

Figure 1. The results of the police investigation stated that the perpetrator had been secured, and the police also found 38 fake QRIS points attached by the perpetrator with a total fund of around IDR 13 million since April 1-10, 2023. (CNN Indonesia). Figure 2 Based on the follow-up from the Area, the management of PT Jasamarga Tollroad Operator emphasized that this was an irresponsible act (jasamargatollroadoperator). The description above provides researchers with an overview of the Quishing Threat Risk. This is also why researchers are interested in researching the Mitigation of Quishing Threat Risk (QR Phishing) using the Security Behavior Intentions Scale (SeBIS) in supporting digital economy security.

Therefore, it is important to understand the factors influencing users' susceptibility to Quishing attacks, particularly in digital financial transactions. By examining the behavioral aspects of security, financial literacy, and technological adoption, this study aims to


identify effective strategies for mitigating Quishing risks. Developing a comprehensive risk mitigation framework is crucial to enhancing digital financial security and protecting users from fraudulent QR codes.

Thus, the study's purpose is to analyze the impact of cyber-security behavior, password usage, proactive awareness, updating behavior, and technological security measures on the mitigation of Phishing risks in digital transactions. By integrating behavioral analysis through the Security Behavior Intentions Scale (SeBIS) with digital financial security frameworks, this study seeks to develop an effective model for improving user resilience against QR-based phishing threats.

Cybersecurity behavior research has evolved over the past decade. Amoah (2022) researched QR code security, reducing the Quishing problem, and found that users should be careful when scanning QR codes provided by advertisements and payment options. It is recommended that only QR codes be scanned from trusted sources. Scanning codes for curiosity is not recommended (Godwin, 2022). Filipo (2022) Researched Dangerous QR Phishing and found that people's alertness, or the ability to detect anomalies over a long period, was very poor regarding phishing, making it unlikely that positive changes would occur when faced with malicious QR codes. Females and younger users used weaker passwords and showed lower software update behavior. Additionally, the study found that participants who reported being proficient in cybersecurity exhibited worse behaviors than those who were not. Cain et al. (2018). Furthermore, some of these studies used cybersecurity instruments that only partially examined security behaviors and lacked a holistic measure of the phenomenon, Sawaya et al. (2017). Another multi-national study from seven countries reported on the cybersecurity behavior of 3500 participants using the Security Behavior Intention Scale (SeBIS) instrument. Five hundred participants (from China, France, Japan, Russia, South Korea, the United States, and the UAE) showed differences in their security behavior, with Japan showing the least secure behavior. Another empirical study measuring the cybersecurity behavior of healthcare professionals showed that older participants showed more secure behavior in several aspects of cybersecurity. Solic et al. (2019). Another empirical evidence on the cybersecurity behavior of 355 high school students was reported by Velki et al. (2017), who showed that younger school students showed the least secure password-sharing behavior. Similarly, preliminary results from a national sample (Velki & Romstein, 2019) of school students and employees from Croatia reported that cybersecurity behavior increases as people reach middle age.

Analysis Method

The approach used in this study is quantitative. This study aims to determine the level of public understanding of the threat of Quishing in the digital economy. The research location was conducted in Makassar City in 2024. The population in this study was the Makassar City community with a productive age range of 15-65, amounting to 1,014,628 people, BPS 2023. Because the population used was quite large and aimed to facilitate the research, the researcher conducted random sampling, which was expected to represent the entire target population. In simple random sampling, each subject in the population has an equal chance of being selected or not selected as a research sample (Sastroasmoro, 2012). The sample size calculation was carried out using the sample size calculator feature via the website www.raosoft.com. In the calculation, the number of populations is filled in the population size column with a confidence level of 95%, a response distribution of 50%, and a margin of error of 10%.



Raosoft®

What margin of error can you accept? <small>5% is a common choice</small>	10 %
What confidence level do you need? <small>Typical choices are 90%, 95%, or 99%</small>	95 %
What is the population size? <small>If you don't know, use 20000</small>	1014628
What is the response distribution? <small>Leave this as 50%</small>	50 %
Your recommended sample size is	97

Fig. 3. Sample size (www.raosoft.com)

The number of samples obtained was 97. However, the researchers used a sample of 100 subjects. The type of data used in this study is primary data, which is distributed by questionnaires, which will then be filled out by respondents who are obtained directly as a source of information sought. The primary data source taken in this study was obtained directly from the productive age community in Makassar City.

This is a survey research where the information is obtained from respondents who fill out the questionnaire. After the data is collected, the data will be analyzed. However, before the data is analyzed, the author needs to test whether the data is valid and reliable with a reliability test and validity test of the research instrument, namely the Egelman and Peer's Security Behaviors Intentions Scale questionnaire (2015). This survey has 16 questions and asks users about their attitudes towards security behavior. The questionnaire was chosen because it is more efficient in terms of time, energy, and research costs and has a high level of accuracy. The scale used is the Likert scale. The questionnaire used in this study is a questionnaire with five alternative answers with scoring:

- 1) STS (Strongly Disagree) answers are scored 1.
- 2) TS (Disagree) answers are given a score of 2.
- 3) N (Neutral) answers are given a score of 3.
- 4) S (Agree) answers are given a score of 4.
- 5) SS (Strongly Agree) answers are given a score of 5

Hypothesis Development

- H1: A person's cyber-security behavior regarding securing devices affects mitigating quashing risks.
- H2: A person's behavior related to password usage (Password Generation) affects mitigating quashing risks.
- H3: The level of user awareness (Proactive Awareness) when browsing different websites affects mitigating quashing risks.
- H4: A person's behavior in responding to software updates to secure devices (Updating Behavior) affects mitigating quashing risks.
- H5: The level of public understanding and awareness of the threat of quashing in the digital economy affects mitigating quashing risks.
- H6: Implementing this risk mitigation strategy can support the overall security of the digital economy.

Results and Discussion

Result

This study used the Structural Equation Model (SEM) with SmartPLS V3.0 for data analysis. SEM can test the relationship between variables. There are two main steps in analyzing data: evaluation, known as the measurement model. This analysis is carried out to ensure the validity and reliability of the research instrument and conduct a structural model analysis that aims to validate the research model. Second, namely, hypothesis testing.

3.1. Respondents

Respondents in this study were people who had used QRIS as a payment method in their daily lives. The survey results came from filling out the questionnaire. Table 1 shows the profile of respondents who participated in this study.

Table 1. Demography Characteristic

Variable	Measurement	n
Gender	Man	28
	Woman	72
Age (Years)	18-25	71
	26-35	27
	>40	2
Education Level	Undergraduate	66
	Graduate	54
	Worker	55
Job Status	(have own income)	
	Student	45

Source: data processing results, 2024

The research sample was dominated by women, with an average sample age entering productive age of 18–39 and 66 people with a Bachelor's degree.

3.2. Validity and Reliability Test

Table 2. Cross Loadings

Variable	DS	PG	PA	QA	QRM	WEB
DS1	0,740	0,465	0,437	0,395	0,424	0,446
DS2	0,725	0,567	0,662	0,490	0,474	0,617
DS3	0,788	0,603	0,511	0,500	0,493	0,528
DS4	0,809	0,573	0,469	0,361	0,421	0,414
PA1	0,540	0,513	0,665	0,482	0,548	0,599
PA2	0,390	0,571	0,720	0,535	0,512	0,483
PA3	0,425	0,508	0,731	0,813	0,526	0,516
PA4	0,544	0,818	0,852	0,882	0,593	0,614
PA5	0,711	0,506	0,641	0,461	0,397	0,595
PG1	0,784	0,718	0,507	0,440	0,583	0,457
PG2	0,564	0,723	0,533	0,511	0,606	0,535
PG3	0,518	0,804	0,599	0,578	0,781	0,604
PG4	0,478	0,815	0,786	0,840	0,563	0,573
QA1	0,492	0,607	0,775	0,871	0,646	0,609
QA2	0,532	0,820	0,850	0,889	0,608	0,611
QRM1	0,484	0,639	0,567	0,568	0,848	0,593
QRM2	0,593	0,647	0,560	0,552	0,851	0,640
QRM3	0,451	0,733	0,637	0,653	0,819	0,571
QRM4	0,526	0,745	0,659	0,648	0,899	0,737
UB1	0,550	0,666	0,681	0,626	0,626	0,876
UB2	0,581	0,567	0,678	0,587	0,605	0,904
UB3	0,643	0,650	0,656	0,624	0,739	0,874

Source: data processing results, 2024

Based on the outer loading analysis, all indicators of the variables Device Securement (DS), Password Generation (PG), Proactive Awareness (PA), Updating Behavior (UB), User Awareness and Quishing Knowledge (UAQK), and Quishing Risk Mitigation (QRM) have values of more than 0.5, thus meeting the indicator validity criteria (Table 2). In addition, each variable's Average Variance Extracted (AVE) value is also more than 0.5, indicating good discriminant validity.

In terms of reliability, the Cronbach Alpha, Composite Reliability, and rho-A values for all variables are more significant than 0.7, indicating that the research construct has high internal consistency (Table 3). This indicates that the instrument used has met the valid and reliable measuring criteria.

Table 3. Construct Reliability and Validity

Variable	Cronbach's Alpha	Rho_A	Composite Reliability	Average Variance Extracted (AVE)
DS	0,766	0,770	0,850	0,587
PG	0,773	0,818	0,850	0,587
PA	0,779	0,819	0,846	0,526
QA	0,708	0,710	0,872	0,774
QRM	0,877	0,881	0,915	0,730
UB	0,861	0,862	0,915	0,783

Source: data processing results, 2024

3.3. Kolinearitas Test

The Variance Inflation Factor (VIF) value for all indicators is below 5.0, indicating no collinearity problem between independent variables. Thus, the relationship between variables in the research model does not influence each other excessively. Kolinearitas Test: The Variance Inflation Factor (VIF) value for all indicators is below 5.0 (Table 4), indicating no collinearity problem between independent variables.

Table 4 Collinearity Statistics (VIF)

	DS1	DS2	DS3	DS4	PA1	PA2	PA3	PA4	PA5	PG1	PG2
VIF	1,441	1,352	1,674	1,888	1,467	1,576	1,343	1,880	1,415	1,543	1,463
	PG3	PG4	QA1	QA2	QRM1	QRM2	QRM3	QRM4	UB1	UB2	UB3
VIF	1,717	1,392	1,429	1,429	2,216	2,481	1,831	2,876	2,112	2,619	2,087

Source: data processing results, 2024

3.4. Model Structure Test

The R-square test results show that exogenous variables moderately influence endogenous variables (Table 5).

Table 5 R Square

Variable	R Square	R Square Adjusted
Quishing Awareness	0,882	0,877
Quishing Risk Mitigation	0,507	0,502

Source: data processing results, 2024

The R-square for the User Awareness and Quishing Knowledge variables is 0.862, which means that 86.2 % of the variability is explained by independent variables such as Device Securement, Password Generation, Proactive Awareness, and Updating Behavior. Meanwhile, the Quishing Risk Mitigation variable has an R-square of 0.507, which means that the User Awareness and Quishing Knowledge variables explain 50.7 % of the variability.

3.5. Hypothesis Testing

Path analysis (Path Coefficient) shows the following relationship:

- Device Securement significantly negatively affects User Awareness and Quishing Knowledge (Path Coefficient=-0.189, P-Value<0.05). This indicates a negative and significant effect. Because even though the device is secure, it does not mean people have better quashing risk mitigation. User awareness of cyber threats, including phishing and squishing, significantly affects their mitigation actions. Users who have higher awareness tend to be better able to implement more effective preventive measures
 - Password Generation significantly positively affects User Awareness and Quishing Knowledge (Path Coefficient=0.273, P-Value<0.05). This indicates a significant positive effect. This means better password practices can improve the ability to mitigate quashing risk. Behavior-related security devices are influential and positive in mitigating risk but often do not directly influence it. Secure devices (as shown) can increase awareness of risk in a way as a whole, which in turn helps mitigate risks cyber such as phishing or quishing
 - Proactive Awareness does not significantly affect User Awareness and Quishing Knowledge (Path Coefficient=-0.015, P-Value>0.05). This shows that more proactive awareness helps in reducing the risk of quishing. Although creating a strong password contributes to subtraction of risk attack, influence the main thing lies in the increased awareness user about the importance security cyber, which then strengthens behavior mitigation risks others
 - Updating Behavior significantly positively affects User Awareness and Quishing Knowledge (Path Coefficient=0.844, P-Value<0.05). Importance regularly updates device software to prevent exploitation vulnerability cyber. Updates in device soft often overlooked but play a role important in reducing risk attack based on cyber
- Meanwhile, User Awareness and Quishing Knowledge significantly positively affect Quishing Risk Mitigation (Path Coefficient=0.712, P-Value<0.05). These results indicate that increasing user awareness and knowledge about QR phishing threats contributes significantly to risk mitigation.

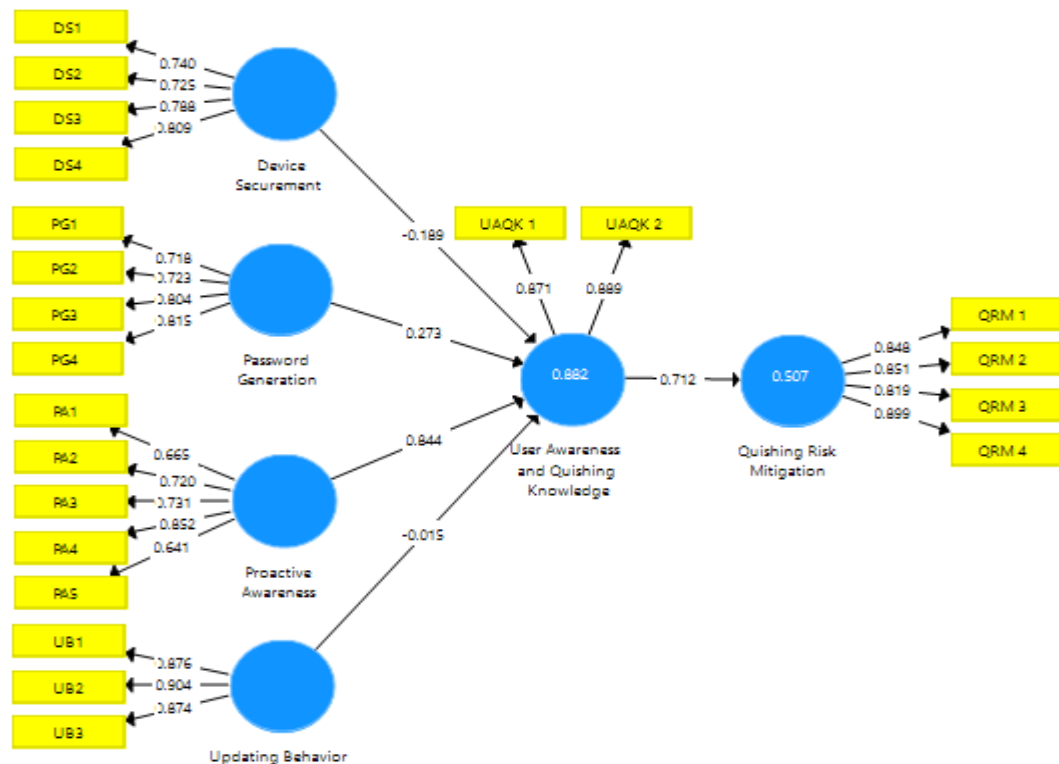


Fig. 4. Initial model diagram for quashing risk mitigation

Source: data processing results, 2024

The results of this study emphasize the importance of increasing user awareness of digital security threats such as QR phishing. From a practical perspective, organizations engaged in the digital economy can utilize these findings to design SeBIS-based training programs to improve user capabilities in Securing their devices, Creating strong passwords, Demonstrating proactive awareness of security threats, and Regularly updating their security software and systems.

The significant correlation between User Awareness, Quishing Knowledge, and Quishing Risk Mitigation shows that user education is a key element in building a safe digital economic ecosystem.

Discussion

Practical Implications

The findings of this study have several practical applications, particularly in enhancing digital security awareness and mitigating Quishing risks in the financial technology (Fintech) sector. Organizations, including banks, e-wallet providers, and regulatory bodies, can use these results to design targeted cybersecurity education programs. The high correlation between User Awareness and Quishing Knowledge and Quishing Risk Mitigation suggests that strengthening user knowledge can significantly reduce digital fraud cases. In practice, this means Improved Security Protocols for QR Code-Based Transactions. To minimize fraudulent transactions, fintech companies and digital payment service providers should implement multi-layered authentication for QR code payments. AI-powered QR scanners can be integrated into digital wallets to detect and block suspicious QR codes automatically. User Education and Digital Literacy Enhancement: Institutions should conduct digital literacy campaigns to educate users about safe QR code usage. Training modules can be developed using the Security Behavior Intentions Scale (SeBIS) to improve cybersecurity behaviors among financial technology users. Regulatory and Policy Improvements: Policymakers can establish stricter security guidelines for QR code transactions, requiring businesses to verify the authenticity of their payment QR codes.

Legal frameworks should be developed to penalize fraudulent activities related to Quishing, thus deterring cyber criminals. Business Risk Management: Companies that rely on QR codes for transactions, especially those in e-commerce and digital banking, should incorporate Quishing risk assessments into their security frameworks. Incident response mechanisms must be enhanced to ensure swift action against fraudulent QR codes.

Limitations of the Study

Despite its contributions, this study has several limitations that must be acknowledged. Geographical Scope: The study is limited to respondents in Makassar, Indonesia, which may not fully represent the security behaviors of users in other regions. Expanding the sample size to include diverse geographical locations would provide a more comprehensive understanding of Quishing risks. Limited Consideration of Technological Countermeasures: While the study focuses on user behavior, it does not extensively analyze the role of emerging technologies such as blockchain or AI-driven fraud detection systems in mitigating Quishing risks. A more technical evaluation could provide additional insights into preventive strategies. Lack of Longitudinal Analysis: This research provides a cross-sectional view of user behavior at a specific time. Future studies should employ longitudinal designs to track security awareness and behavior changes over time.

Prospects for Further Research

Future research can build upon this study by exploring the following areas: Development of a Resilient Financial Security Model. Future studies can create a "Digital Financial Security Model for Quishing Mitigation," integrating behavioral, technological, and regulatory factors to enhance financial cybersecurity. Expansion to Business and Government Sectors: While this study focuses on individual users, Quishing also affects businesses and government institutions. Research into how organizations implement security against fraudulent QR codes would provide valuable insights. Integration of AI and Machine Learning for Fraud Detection: Investigating how AI-driven QR scanners and fraud detection algorithms can enhance digital security would provide a technological perspective on risk mitigation. Cross-Country Comparative Studies: Conducting research across multiple countries would help determine whether cultural and regulatory differences impact users' ability to mitigate Quishing risks. Behavioral Economic Analysis of Financial Decision-Making in Digital Fraud: Studying how users make financial decisions when confronted with potential fraud scenarios could help improve fraud prevention strategies in Fintech applications. By addressing these areas, future research can further strengthen digital financial security and contribute to the ongoing efforts to protect users from emerging cybersecurity threats like Quishing.

Conclusions

This study provides theoretical and practical contributions to understanding how user security behavior can mitigate the threat of QR phishing. The research model based on SeBIS can be a reference for developing more effective digital security policies in the future. Based on the results of the data analysis, the following points can be concluded. The influence of security behavior on user awareness includes device securement behavior, which negatively influences user awareness and knowledge-squishing. This shows that device security alone cannot increase user awareness of QR phishing threats. Password Generation Behavior has a significant favorable influence, confirming the importance of strong password creation practices to increase awareness of QR phishing threats. Updating Behavior contributes positively and significantly to increasing user awareness and knowledge of Quishing threats. This shows the importance of software updates in reducing security risks. In contrast, Proactive Awareness does not show a significant influence, which may indicate most users' lack of proactive awareness.

Regarding quashing risk mitigation, user awareness and quashing knowledge have a significant positive effect. In other words, the higher the user awareness and knowledge of the QR phishing threat, the better their ability to mitigate the risk. Implications for Digital Economy Security show that good digital security behaviors, such as creating strong passwords and updating software regularly, are important in supporting digital economy security. By increasing user awareness, the risk of threats such as QR phishing can be minimized, thereby strengthening trust in the digital ecosystem.

There is a need for increased digital security education and training. Governments, educational institutions, and digital organizations need to organize training programs to increase public awareness of the threat of QR phishing. Education should include security practices such as creating strong passwords, updating software, and how to recognize the signs of phishing. In more detail, the Development of a More Proactive Mitigation Strategy can be done by Technology Companies by providing tools or applications that support user awareness of potential QR phishing threats, such as secure QR scanners. Also, Public awareness campaigns through social media, websites, or seminars can help raise public attention to the threat of QR phishing. Further research is expected to expand the geographical scope to understand digital security behavior in other areas and to generalize the research results more widely. Mixed methods can enrich the findings by exploring qualitative insights, such as the reasons behind user behavior related to digital security, and developing models that include external variables, such as the influence of organizational culture or government regulations, to understand more complex factors in mitigating digital security risks.

With these findings, the research makes a significant contribution to supporting more effective digital security strategies, especially in dealing with QR phishing threats, to strengthen user trust in the digital economy ecosystem.

Acknowledgment

We want to express our gratitude to Allah SWT for all His grace and gifts so that this research entitled "Mitigating the Risk of Quishing Threats (QR Phishing) Using the Security Behavior Intentions Scale (SeBIS) in Supporting Digital Economy Security" can be completed properly. This research aims to provide scientific contributions in supporting digital economic security through a QR phishing threat risk mitigation approach. We want to express our deepest gratitude to various parties who have contributed to this research process, including the Ministry of Education, Culture, Research, and Technology for the financial support that has been provided for the implementation of this research, the Nitro Makassar Business and Finance Institute for the support of facilities and opportunities provided to carry out this research, All respondents who have been willing to take the time to provide valuable data and information by filling out questionnaires, Lecturers, researchers, and students who provided input, criticism, and suggestions during the planning and implementation process of the research, Family and friends for their endless moral support and motivation so that this research can be completed properly. Finally, we hope that the results of this study can provide benefits for the development of science, especially in the field of digital security, and become a reference in efforts to mitigate digital threats in the future. We expect constructive criticism and suggestions for future improvement of this research.

References

Bonneau, Joseph & Herley, Cormac & Oorschot, Paul & Stajano, Frank. (2014). Passwords and the Evolution of Imperfect Authentication. *Communications of the ACM*. 58. 10.1145/2699390

- Cain Ashley A, Edwards Morgan E, Still Jeremiah D. (2018) An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*. doi:10.1016/j.jisa.2018.08.002.
- Egelman, S., and Peer, E. (2015). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). Paper presented at the Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea.
- Federal Bureau of Investigation. (2022). Cybercriminals Tampering with QR Codes to Steal Victim Funds. Available at: <https://www.ic3.gov/Media/Y2022/PSA220118>
- Filipo Sharevski, Amy Devine, Emma Pieroni, and Peter Jachim. (2022). Phishing with Malicious QR Codes. In 2022 European Symposium on Usable Security (EuroUSEC 2022), September 29–30, 2022, Karlsruhe, Germany. ACM, New York, NY, USA, 20 pages. <https://doi.org/10.1145/3549015.3554172>
- Godwin Awuah Amoah, Hayfron-Acquah J.B. (2022) QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing). *International Journal of Computer Applications*. 184, 33 (Oct 2022), 34- 39. DOI=10.5120/ijca2022922425
- Harrison, Brynne & Harrison, Brynne & Ng, Yu. (2018). Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility
- Jain, Anurag & Shanbhag, Devendra. (2012). Addressing Security and Privacy Risks in Mobile Applications. *IT Professional*. 14. 28-33. 10.1109/MITP.2012.72.
- M. S. Dr Duryadi, Metode penelitian : metode penelitian empiris, model path analysis dan analisis smart pls. Semarang: Yayasan Prima Agus teknik, STEKOM, 2021.
- Parsons, Kathryn & McCormac, Agata & Pattinson, Malcolm & Butavicius, Marcus & Jerram, Cate. (2013). Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails. *IFIP Advances in Information and Communication Technology*. 405. 366-378. 10.1007/978-3-642- 39218-4_27.
- Rachelle Chouinard. (2021). New Quishing Campaign Shows How Threat Actors Innovate to Bypass Security. Available at: <https://abnormalsecurity.com/blog/qrcode-campaign-bypass-security>
- Ransbotham, Sam & Mitra, Sabyasachi & Ramsey, Jon. (2012). Are Markets for Vulnerabilities Effective?. *MIS Quarterly*. 36. 43-64. 10.2307/41410405
- Sawaya, Yukiko, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. (2017). Self-confidence trumps knowledge: A cross-cultural study of security behavior. In Proceedings of the 2017 CHI conference on human factors in computing systems, pp. 2202–2214.
- Solic, Kresimir, Mateo Plesa, Tena Velki, and Kresimir Nenadic. (2019). Awareness about information security and privacy among healthcare employees. *Medicinski fakultet Osijek*.
- Tai-Wei Kan, Chin-Hung Teng, and Mike Y Chen. (2011). QR code based augmented reality applications. In *Handbook of augmented reality*. Springer, 339–354.
- Tersangka Penipuan QRIS di Kotak Amal Masjid Mantan Pegawai Bank (2023). CNN Indonesia. Available at: <https://www.cnnindonesia.com/nasional/20230411154515-12-936323/tersangka-penipuan-qr-is-dikotak-amal-masjid-mantan-pegawai-bank>
- Velki Tena, Romstein Ksenija. (2019) User risky behavior and security awareness through lifespan. *International Journal of Electrical and Computer Engineering Systems*. doi: 10.32985/ijeces.9.2.2
- Velki, Tena, Kresimir Solic, V. Gorjanac, and K. Nenadic. (2017). Empirical study on the risky behavior and security awareness among secondary school pupils-validation and preliminary results. In 2017 40th international convention on information and communication technology, electronics and microelectronics (MIPRO), 1280–1284. IEEE.
- Waspada! Penipuan Scan Barcode di Pintu Tol dengan Embel-Embel Gratis E-Toll Rp 500 Ribu (2023). Ardha Ihsan Asy'Ari. Available at:

<https://www.jawapos.com/nasional/012968990/waspada-penipuan-scan-barcode-di-pintu-tol-dengan-embel-embel-gratis-e-toll-rp-500-ribu>

<http://www.raosoft.com/samplesize.html>

<https://www.bps.go.id/id/publication/2023/02/28/18018f9896f09f03580a614b/statistik-indonesia-2023.html>