Advances in Community Services Research

Volume 4, Issue 2 (2026). 68-81

DOI: https://doi.org/10.60079/acsr.v4i2.878

OPEN ACCESS

e-ISSN: 2985-9778

ACSR | RESEARCH ARTICLE

Analysis of QRIS Misuse Mode as a Means of Personal Data Theft and Account Takeover in Bandung City, Indonesia

Nur Muhamad Hamka [1] Sylpi Nopiya [2] Tantri Pebyani [3] Suci Fitriani [4] Viny Limbong [5] Yulianah [6*]

[1, 2, 3, 4, 5, 6*] Universitas Kebangsaan Republik Indonesia, Bandung, Indonesia

Email: hamkamuhamad130@gmail.com, sylpinopiyaa11@gmail.com, tantripebyani@gmail.com, sucifitrianti2006@gmail.com, limbongvini@gmail.com, yulianah1288@gmail.com

ARTICLE HISTORY

Submitted	:	June 02, 2026
Reviewed	:	June 07, 2026 June 12, 2026
Revised	:	June 14, 2026
Accepted	:	June 15, 2026
Published	:	June 16, 2026

Conflict of Interest Statement:
The author(s) declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

ABSTRACT

Purpose: This study analyzes the mechanisms of quishing attacks within QRIS transactions, examines users' vulnerability to QR-code-based fraud, and evaluates mitigation efforts and legal protection in Indonesia's digital payment ecosystem.

Research Method: A sequential explanatory mixed-methods design was employed. Quantitative data were collected through online questionnaires distributed to QRIS users in Bandung using purposive sampling. Of the 100 questionnaires distributed, 89 valid responses met the inclusion criteria. Qualitative data from documented fraud cases and relevant literature were used to explain the quantitative findings.

Results and Discussion: Although 89.9% of respondents were aware of QR code fraud risks, 38.2% had experienced financial losses, and 31.5% had nearly become victims. Routine payment activities (44.6%) and promotional offers (24.1%) emerged as the dominant triggers for scanning fraudulent QR codes. Furthermore, 39.5% of respondents reported being redirected to phishing websites, indicating that quishing frequently facilitates credential theft and account takeover through social engineering techniques.

Implications: The findings highlight the need for stronger cybersecurity governance through dynamic QRIS implementation, enhanced security features, and continuous consumer education.

Originality: This study integrates behavioral evidence from QRIS users with legal and cybersecurity perspectives to provide a comprehensive understanding of quishing in Indonesia's digital payment ecosystem.

Keywords: QRIS; quishing; social engineering; account takeover; cybersecurity governance.

1. Introduction

The rapid development of digital payment systems has transformed Indonesia's financial landscape and accelerated the transition toward a cashless society. One of the major innovations introduced to support this transformation is the Quick Response Code Indonesian Standard (QRIS), which Bank Indonesia officially launched as a standardized QR code payment system. QRIS (Quick Response Code Indonesian Standard) is a standardized QR Code payment system developed by Bank Indonesia. QRIS ensures that the transaction process using QR Codes becomes faster, easier, more affordable, safer, and more reliable. According to Bank Indonesia, QR code payments are among Indonesia's strategic initiatives to

Advances in Community Services Research
Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
OPEN ACCESS
e-ISSN: 2985-9778

embrace the digital economy, as various digital financial services can be developed from transaction data generated by QR Code payments (Indonesia, 2019).

Fundamentally, the development of QR Code digital technology provides tremendous benefits in creating a more integrated and efficient national digital economy. In the economic sector, QR Codes not only serve as an alternative cashless payment method but also as a starting point for recording financial transaction histories, which are crucial to driving digitally based economic transformation. The widespread adoption of QRIS has contributed to expanding financial inclusion, improving transaction efficiency, and supporting the growth of micro, small, and medium enterprises (MSMEs). Nevertheless, the increasing reliance on QR-based transactions has expanded the attack surface for cybercriminals, creating new challenges for consumer protection and digital security.

Recent studies have highlighted that cybersecurity threats continue to evolve alongside the expansion of financial technology. One emerging threat is quishing, a phishing technique that exploits QR code technology to deceive users and steal sensitive information. Unlike conventional phishing attacks that rely on email links or text messages, quishing leverages users' trust in QR codes and their inability to visually verify the destination embedded within the code before scanning. Researchers argue that QR code-based attacks are particularly dangerous because they bypass traditional warning signs commonly associated with phishing attempts and capitalize on users' habitual trust in digital payment infrastructure (Tandel *et al.,* 2025). Quishing attacks typically redirect victims to fraudulent websites or applications designed to obtain personal information, login credentials, one-time passwords (OTPs), or financial assets. This attack vector is further strengthened by social engineering tactics that exploit emotions and trust, especially among users who prioritize convenience over verification in digital transactions (Wang *et al.,* 2021).

The threat of quishing has shifted from a potential risk to a real cybersecurity concern within Indonesia's QRIS ecosystem. Reports indicate that victims have suffered financial losses exceeding one million rupiah after being deceived through fraudulent fundraising schemes disseminated via WhatsApp. Similar incidents have also occurred in public spaces, as demonstrated by the discovery that dozens of QRIS stickers attached to donation boxes at Nurul Iman Mosque in Blok M had been replaced with QR codes belonging to fraudsters (Kumparan, 2023). These cases illustrate that quishing exploits not only technological vulnerabilities but also weaknesses in physical QRIS infrastructures, limited digital security literacy, and consumers' tendency to overlook merchant verification procedures. By imitating legitimate institutions and exploiting psychological biases, perpetrators increase the effectiveness of their attacks. Although existing cybersecurity literature has begun to address QR-code-based phishing, most studies focus primarily on technical aspects and general phishing awareness. Research specifically examining consumer vulnerability and the adequacy of legal safeguards within QRIS-based payment ecosystems, particularly in developing countries such as Indonesia, remains limited. This gap underscores the need for empirical studies that integrate behavioral, technological, and regulatory perspectives to comprehensively understand the quishing phenomenon in the context of Indonesia's rapidly growing cashless society.

Given the urgency of consumer data protection and the gap between the massive digitization of payments and the limited development of security literacy and mitigation strategies, the issue of quishing within QRIS facilities warrants deeper investigation. The destructive impact of quishing attacks cannot be underestimated, as consumer losses often manifest as credential theft, forced account takeovers (ATOs), unauthorized access to financial accounts, and substantial financial losses within a relatively short period. Despite the escalating threat landscape, the legal protection framework

Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
OPEN ACCESS
e-ISSN: 2985-9778

governing QR-code-based fraud in Indonesia remains fragmented and predominantly reactive rather than preventive.

Juridically, legal instruments such as the Electronic Information and Transactions Law (UU ITE) have not explicitly regulated criminal acts involving the quishing or the manipulation of QR codes as a specific cybercrime offense. As a consequence, law enforcement authorities often rely on broad interpretations of existing provisions addressing illegal access, fraud, or misuse of electronic systems when prosecuting offenders. This situation potentially contributes to evidentiary challenges, inconsistent legal interpretations, and reduced legal certainty for victims seeking justice. The existing approach also tends to emphasize post-incident prosecution rather than proactive prevention and early intervention. Similarly, although Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) normatively recognizes consumers' rights to protect their personal information, the practical implementation of this legislation in addressing QR code-related fraud remains underdeveloped. While the PDP Law provides avenues for compensation claims against Payment System Service Providers (PJSP) in the event of data breaches, it does not comprehensively establish mandatory emergency response mechanisms, inter-institutional coordination protocols, or real-time fraud mitigation frameworks specifically tailored to emerging cyber threats such as quishing (Benia, 2023). The absence of integrated response procedures involving Bank Indonesia (BI), the Financial Services Authority (OJK), law enforcement agencies, and payment service providers can prolong case resolution and reinforce consumer vulnerability in the digital payment ecosystem.

Based on the foregoing discussion, an important empirical and theoretical gap remains concerning the intersection between QRIS adoption, consumer cybersecurity awareness, quishing attack mechanisms, and the effectiveness of legal protections available to victims. Existing studies have rarely employed an integrative approach to simultaneously examine users' behavioral vulnerabilities and the adequacy of regulatory frameworks governing QR-code-based payment systems. Therefore, this study seeks to extend the current body of knowledge by integrating consumer perspectives with legal analysis to develop a more comprehensive understanding of the challenges posed by quishing in Indonesia's digital payment environment.

Accordingly, this study aims to analyze how quishing mechanisms operate in QRIS transactions in Indonesia, particularly in Bandung, and to evaluate the effectiveness of mitigation strategies and legal protection frameworks to minimize the risks associated with quishing attacks. Specifically, this study addresses the following research questions: (1) How do quishing attacks operate within QRIS-based transactions? (2) To what extent are QRIS users aware of the risks associated with quishing attacks? Moreover, (3) How effective are existing mitigation measures and legal protection mechanisms in safeguarding consumers against QRIS-related fraud? The novelty of this research lies in its integration of behavioral evidence from QRIS users with an examination of legal preparedness for responding to emerging QR-code-based cyber threats in the Indonesian context. By employing a sequential explanatory mixed-methods approach, this study contributes to the growing discourse on digital payment security by bridging technological, behavioral, and regulatory perspectives that are often investigated separately.

The remainder of this paper is organized as follows. Section 2 provides a literature review and hypothesis development. Section 3 presents the research method and design. Section 4 provides the results and discussion. Section 5 is Concluding Remarks and Recommendations.

Advances in Community Services Research
Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
OPEN ACCESS
e-ISSN: 2985-9778

2. Literature Review and Hypothesis Development

2.1 QRIS and the Digital Payment Ecosystem in Indonesia

The Quick Response Code Indonesian Standard (QRIS) represents one of the most significant innovations introduced by Bank Indonesia to support the development of an integrated, efficient, and inclusive digital payment ecosystem. QRIS serves as a national payment standard that enables consumers to conduct transactions using a single QR code format across various payment service providers. Through the implementation of the CEMUMUAH principle—Cepat, Mudah, Murah, Aman, dan Andal (Fast, Easy, Affordable, Safe, and Reliable)—QRIS has become a strategic instrument in accelerating the transition toward a cashless society while strengthening the national digital economy (Bank Indonesia, 2024). Beyond functioning as a payment mechanism, QRIS contributes to broader economic objectives by facilitating transaction recording, supporting financial transparency, and expanding access to formal financial services. Technological innovations in digital financial services have been recognized as important drivers of financial inclusion by expanding access, improving efficiency, and reducing barriers to participation in formal financial systems (Rahman, 2024). The widespread adoption of QRIS also reflects Indonesia's commitment to promoting digital transformation within the payment system, particularly among groups that previously experienced barriers to accessing conventional banking services. Recent evidence indicates that acceptance of QRIS is influenced by factors such as perceived usefulness, ease of use, social influence, facilitating conditions, and users' knowledge of digital technologies (Hamzah Muchtar *et al.,* 2024; Purwatiningsih *et al.,* 2025). In particular, younger generations demonstrate a high level of adaptability toward QRIS due to their familiarity with mobile technology and digital lifestyles, highlighting the role of technological readiness in shaping payment behavior (Andriyani *et al.,* 2025).

The expansion of QRIS adoption has also generated substantial implications for the development of micro, small, and medium enterprises (MSMEs), which constitute a vital pillar of Indonesia's economy. By providing an affordable and interoperable payment infrastructure, QRIS enables MSMEs to participate more actively in the digital economy, improve transaction efficiency, and reduce dependence on cash-based systems. Empirical studies have shown that QRIS adoption among MSMEs is driven by perceptions of convenience, operational efficiency, and business competitiveness, ultimately supporting the digitalization of commercial activities (Santika *et al.,* 2024). Furthermore, the use of QRIS has been associated with improvements in financial performance, including more systematic transaction recording, enhanced cash flow management, and expanded market reach among small-business actors (Utami, 2025). QRIS has therefore evolved beyond its role as a technological innovation and emerged as an instrument for fostering inclusive economic growth. Suseno (2025) further emphasizes that the successful implementation of QRIS can strengthen financial inclusion by integrating underserved communities and informal businesses into the formal financial ecosystem. Nevertheless, the increasing reliance on QR-based transactions also necessitates greater attention to digital literacy, consumer protection, and cybersecurity, given that the sustainability of the digital payment ecosystem ultimately depends not only on technological advancement but also on users' trust and security awareness.

Advances in Community Services Research
Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
OPEN ACCESS
e-ISSN: 2985-9778

2.2 Quishing as an Emerging Form of Social Engineering-Based Cybercrime

Quishing has emerged as a new form of cybercrime that combines the characteristics of phishing attacks with the widespread use of QR code technology. Unlike conventional phishing schemes that predominantly rely on suspicious emails or text messages, quishing exploits users' trust in QR codes by embedding malicious links within machine-readable codes that cannot be interpreted directly before scanning. As a result, users are often unable to assess the legitimacy of a destination website or application before interacting with it, increasing their susceptibility to deception. Sharevski *et al.,* (2022) demonstrated that malicious QR codes effectively manipulate users' decision-making processes by leveraging convenience and habitual trust in digital technologies. The study further revealed that individuals frequently prioritize speed and usability over security considerations when engaging with QR-based interactions. This vulnerability becomes more pronounced in environments where QR codes are routinely used for payments, authentication, and information access. Moreover, quishing should not be viewed solely as a technological issue because its effectiveness largely depends on social engineering strategies that exploit psychological factors such as urgency, authority, curiosity, and altruism. In this context, the success of quishing attacks is closely linked to human behavior rather than merely the sophistication of the underlying technology.

The evolution of quishing has extended beyond online settings and increasingly infiltrated physical public spaces where QR codes are commonly displayed. Sharevski *et al.,* (2024) found that contextual factors within public environments significantly influence individuals' willingness to advance in cyberattack techniques, which have enabled QR codes to function not only as phishing instruments but also as delivery mechanisms for malware and credential theft, emphasizing the need for proactive detection systems (Sarkhi & Mishra, 2024). From a behavioral perspective, recent evidence suggests that users with stronger security intentions and higher levels of cybersecurity awareness exhibit greater resistance to quishing attempts (Singkeruang *et al.,* 2025). Similarly, Baottong *et al.,* (2025) emphasized that educational interventions aimed at improving digital literacy can substantially reduce users' vulnerability to QR-phishing attacks, particularly in developing digital economies. However, emerging evidence suggests that quishing may be as effective as traditional phishing at deceiving victims yet more difficult for existing security mechanisms to detect (Weinz *et al.,* 2025). Consequently, scholars have increasingly advocated integrating technological safeguards and user-centered approaches to combat this threat. The development of machine-learning-based detection systems capable of identifying malicious QR codes prior to user interaction further represents a promising avenue for mitigating quishing risks (Trad & Chehab, 2025). Collectively, these findings underscore that quishing is an emerging social-engineering-based cybercrime requiring multidimensional mitigation strategies encompassing technological innovation, behavioral interventions, and institutional preparedness.

2.3 Legal Protection and Cybersecurity Governance in QRIS Transactions

The rapid expansion of QRIS-based transactions has created an urgent need for legal frameworks to ensure consumer protection and maintain trust in Indonesia's digital payment ecosystem. Although QRIS has successfully facilitated financial inclusion and transaction efficiency, its widespread use has also increased exposure to cybercrime, including unauthorized QR code manipulation, identity theft, and fraudulent transactions. Existing studies indicate that the current regulatory framework has not fully adapted to the evolving nature of digital threats targeting QRIS users. Emerging cyber threats within

Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
OPEN ACCESS
e-ISSN: 2985-9778

digital financial infrastructures necessitate adaptive regulatory frameworks and stronger cybersecurity protocols that emphasize prevention alongside post-incident response mechanisms (Alam *et al.,* 2025). Herryani (2023) argues that legal protection mechanisms for QRIS users require substantial strengthening because existing regulations often lag behind the development of increasingly sophisticated digital fraud schemes. Similarly, Anisa & Andraini (2023) emphasize that consumers remain vulnerable when losses arise from the misuse of digital payment systems, particularly due to the limited public understanding of legal remedies and the absence of explicit regulations governing emerging forms of QRIS-related cybercrime. From a banking law perspective, Sasra & Baidhowi (2025) further highlight that legal certainty is crucial to maintaining public confidence in non-cash transactions, necessitating a clearer delineation of responsibilities among payment service providers, regulators, and consumers. These findings collectively suggest that legal protection in QRIS transactions should extend beyond reactive dispute resolution mechanisms toward preventive approaches that anticipate future cybersecurity risks.

The governance of cybersecurity in QRIS transactions also requires a comprehensive institutional framework that involves regulators, payment service providers, and consumers. Windani *et al.,* (2025) note that despite the enactment of Indonesia's Personal Data Protection Law, its implementation in the context of QRIS transactions remains limited, particularly regarding supervisory mechanisms and incident response coordination. Moreover, Rahayu (2024) argues that consumer protection should be balanced with legal certainty for business actors by establishing clear standards concerning liability and risk allocation within digital payment systems. Regulatory developments have sought to address these challenges by issuing the Financial Services Authority Regulation Number 22 of 2023, which requires financial service providers to implement consumer protection principles, complaint-handling procedures, consumer education programs, and risk mitigation strategies for digital transactions (Otoritas Jasa Keuangan, 2023). In parallel, Bank Indonesia Regulation Number 3 of 2023 reinforces the obligation of payment service providers to ensure transparency, transaction security, effective complaint mechanisms, and consumer protection within the payment system ecosystem (Bank Indonesia, 2023). Nevertheless, the persistence of QRIS-related fraud cases indicates that regulatory effectiveness depends not only on the existence of legal provisions but also on the integration of technological safeguards, institutional preparedness, and public awareness initiatives.

3. Research Method

This study employed a sequential explanatory mixed-methods design, which integrates quantitative and qualitative approaches in two consecutive phases. In this design, quantitative data collection and analysis were conducted in the first phase to identify patterns related to QRIS usage, cybersecurity awareness, and exposure to quishing incidents. The qualitative phase was subsequently implemented to explain and deepen the interpretation of the quantitative findings by exploring attack mechanisms, victims' experiences, and the adequacy of legal protections within the Indonesian context. The integration of both approaches enabled the researchers to obtain a more comprehensive understanding of quishing as an emerging cybercrime phenomenon involving technological, behavioral, and regulatory dimensions.

The population in this study consisted of Bandung residents who actively use smartphones and utilize QR Code Indonesian Standard (QRIS)-based digital payment services. Population refers to the

Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
OPEN ACCESS
e-ISSN: 2985-9778

entire object or group targeted by a study (Notoatmodjo, 2020). Sampling was conducted using a purposive sampling technique distributed through online platforms. Respondents were required to meet the following inclusion criteria: (1) being at least 18 years old, (2) residing in Bandung, and (3) actively using at least one QRIS-compatible payment application, such as mobile banking or electronic wallet services. A total of 100 questionnaires were distributed during the data collection period. Following the screening process, 11 responses were excluded because they contained incomplete information or did not fulfill the predetermined inclusion criteria. Consequently, the final quantitative analysis was performed using 89 valid responses. This screening procedure was undertaken to enhance data quality and ensure that only eligible participants were included in the analysis.

Data collection was carried out using two primary sources. Primary data were obtained directly from respondents through structured online questionnaires administered via Google Forms. The questionnaire instrument consisted of four sections: (1) respondents' demographic characteristics, including age and occupational background; (2) the intensity of QRIS utilization and the level of cybersecurity literacy; (3) respondents' experiences related to exposure to QR-code-based fraud or quishing incidents; and (4) detailed information regarding the attack mechanism, motivations underlying QR code scanning behavior, and the consequences of financial loss or data theft among respondents who had encountered such incidents. Secondary data were collected through literature reviews and document analysis to provide contextual support for the study findings. These sources included peer-reviewed academic publications focusing on cybersecurity, phishing, social engineering, and personal data protection; reports and interview transcripts published by credible national news outlets concerning actual cases of QRIS misuse; and regulatory documents issued by Bank Indonesia, the Financial Services Authority (OJK), and legislation related to personal data protection, including Law Number 27 of 2022 concerning Personal Data Protection.

Quantitative data analysis was conducted using descriptive and exploratory statistical techniques. Descriptive statistics, including frequencies and percentages, were used to summarize respondents' demographic profiles, QRIS usage patterns, levels of cybersecurity awareness, and experiences with quishing incidents. To provide a deeper understanding of the relationships among key variables, cross-tabulation analyses were also performed to examine potential associations between age groups, QRIS usage intensity, cybersecurity awareness, and respondents' exposure to QRIS-related fraud. The findings were subsequently presented using tables and figures to facilitate interpretation and improve the clarity of data presentation. In each figure and table, the number of respondents serving as the sample base was explicitly stated, and explanations were provided whenever multiple responses were permitted.

The qualitative phase employed thematic analysis to interpret open-ended responses from the questionnaire and to analyze secondary case materials documenting QRIS-related fraud incidents in Indonesia. The researchers systematically reviewed the qualitative data to identify recurring themes and attack patterns associated with quishing practices. These themes included social engineering tactics, malicious applications, QR code replacement techniques, redirects to phishing sites, and account takeover attempts. The purpose of the qualitative analysis was not merely descriptive but explanatory, namely, to clarify and contextualize the quantitative findings obtained during the first phase of the study. Through this approach, qualitative evidence was used to explain why certain groups appeared more vulnerable to quishing attacks and how perpetrators exploited technological vulnerabilities alongside human behavioral tendencies.

Advances in Community Services Research
Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
OPEN ACCESS
e-ISSN: 2985-9778

To maintain the focus and depth of the investigation, several delimitations were established. First, the technical analysis was restricted to the abuse of QRIS interfaces from the perspective of end users or consumers. Accordingly, this study did not investigate vulnerabilities in the internal server infrastructure of Bank Indonesia or Payment System Service Providers (PJSPs). Second, the analysis concentrated exclusively on fraud incidents occurring within the Indonesian jurisdiction and involving local banking systems or QRIS-based payment services. Finally, because the quantitative sample was predominantly composed of younger respondents and students, the findings should be interpreted in light of the study population's characteristics. They should not be generalized to represent all segments of Indonesian society.

Participation in this study was voluntary. Prior to completing the questionnaire, respondents were informed of the research objectives and their right to withdraw from participation at any stage of the study. The anonymity and confidentiality of respondents were maintained throughout the data collection, analysis, and reporting processes to ensure compliance with ethical principles governing social and behavioral research.

4. Results and Discussion

4.1 Analysis Results

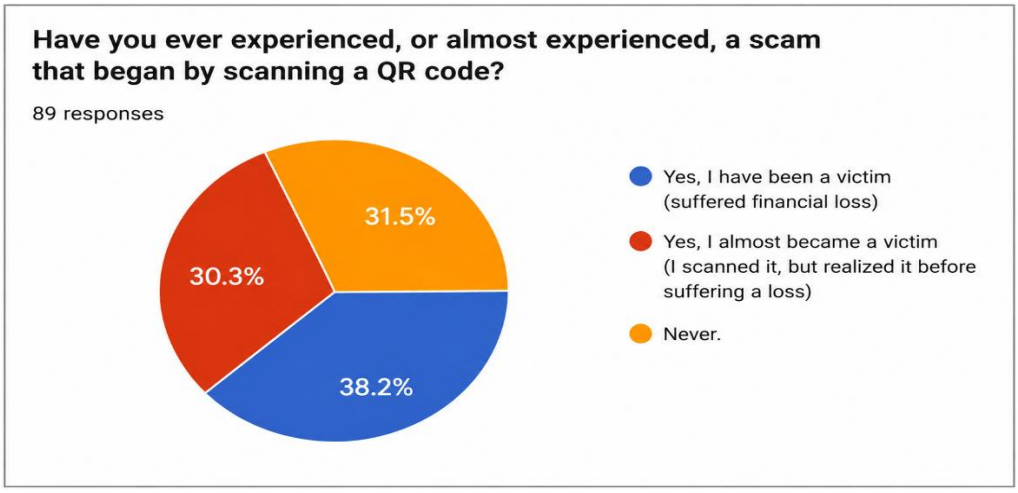
4.1.1 Demographic Profile and QRIS Usage Intensity

Based on data from 89 valid respondents, the demographic profile of participants was predominantly young adults aged 18–25 years (83.1%). Consistent with this age distribution, the majority of respondents were students (66.3%), followed by private-sector employees (21.3%). These demographic characteristics indicate that the respondents largely belong to the digitally connected generation, which actively engages in cashless transactions and mobile-based financial services. The intensity of QRIS use further supports this pattern: 58.0% of respondents reported frequently using QRIS, while 29.5% reported using it very frequently in their daily activities. These findings suggest that QRIS has become an integral component of routine financial behavior among younger users.

4.1.2 Security Literacy and Exposure to Quishing

Regarding cybersecurity literacy, the survey revealed encouraging initial findings. A total of 89.9% of respondents reported having heard of or understood the potential risks associated with QR code-based fraud, commonly referred to as quishing. However, this relatively high level of awareness was not accompanied by a correspondingly low level of victimization. As illustrated in Figure 1, 38.2% of respondents reported experiencing financial losses from QR code-related fraud, while another 31.5% reported nearly becoming victims but recognized the threat before incurring actual losses. Only 30.3% of respondents reported never having encountered such incidents. These findings suggest that awareness alone may be insufficient to prevent quishing incidents, particularly when perpetrators employ persuasive social engineering techniques that exploit trust and habitual transaction patterns.

Advances in Community Services Research
Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
OPEN ACCESS
e-ISSN: 2985-9778

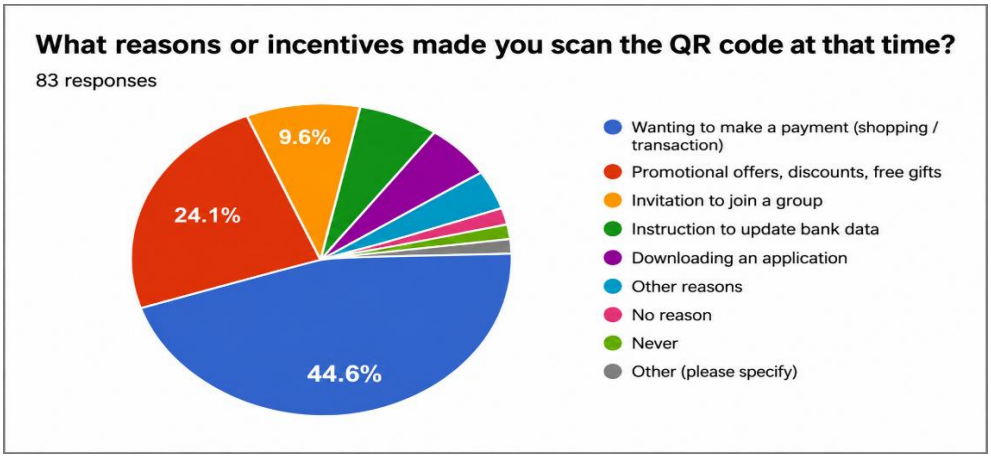


Source: *Primary data processed by the researchers (2026).*

Figure 1. Respondents' Exposure to Quishing Incidents (n = 89).

4.1.3 Motivational Factors Behind QR Code Scanning

The success of quishing attacks appears closely tied to exploiting users' everyday transactional behaviors. As presented in Figure 2, the most frequently reported reason for scanning QR codes was the intention to complete legitimate payment transactions (44.6%). This was followed by exposure to promotional offers, discounts, or giveaways (24.1%), and invitations to join specific groups or activities (9.6%). These findings suggest that perpetrators tend to target routine activities and exploit attractive incentives to increase the likelihood of victim compliance. Rather than relying solely on technical sophistication, quishing attacks often capitalize on convenience, urgency, and perceived legitimacy embedded within ordinary consumer interactions.



Source: *Primary data processed by the researchers (2026)*

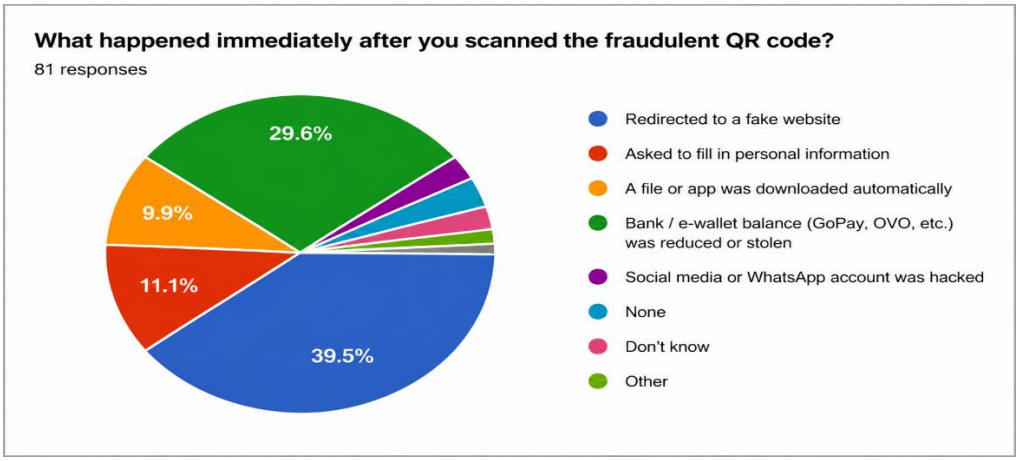
Figure 2. Factors Motivating Respondents to Scan QR Codes (n = 83).

4.1.3 Post-Scan Consequences and Attack Mechanisms

Following QR code scanning, respondents' experiences varied considerably and were not limited to direct financial losses. As depicted in Figure 3, the most commonly reported outcome was redirection to fraudulent websites that resembled legitimate platforms (39.5%). In addition, 11.1% of respondents

Advances in Community Services Research
Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
OPEN ACCESS
e-ISSN: 2985-9778

reported being prompted to provide personal information, such as identity card details or passwords, whereas 9.9% experienced automatic downloads of suspicious files or malicious applications (APKs). Notably, 29.6% of respondents reported unauthorized deductions from bank accounts or e-wallet balances after the incident. These findings demonstrate that quishing attacks often constitute the initial stage of broader credential theft schemes that may ultimately facilitate account takeover (ATO) and subsequent financial exploitation.



Source: *Primary data processed by the researchers (2026).*

Figure 3. Consequences Experienced After Scanning Fraudulent QR Codes (n = 81).

4.1.4 Integration of Quantitative and Qualitative Findings

The qualitative findings derived from open-ended responses and the review of documented fraud cases further enriched the interpretation of the quantitative results. Three recurring attack patterns were identified. First, perpetrators replaced legitimate static QRIS stickers displayed in public spaces with fraudulent QR codes. Second, QR codes were disseminated through social media platforms under the guise of promotional campaigns or prize distributions. Third, QR codes were distributed via private messaging applications by impersonating official institutions and requesting payments associated with donations, fines, or bills. The convergence of quantitative and qualitative evidence indicates that quishing attacks are sustained by the interplay among technological vulnerabilities, habitual consumer behaviors, and sophisticated social engineering practices. Consequently, effective mitigation requires not only improvements in technological safeguards but also continuous public education and stronger institutional preparedness to address emerging forms of QR-code-based cybercrime.

4.2 Discussion

The findings of this study indicate that awareness of quishing risks does not necessarily translate into effective protective behavior among QRIS users. Although most respondents reported having previously heard about the dangers of QR code-based fraud, a considerable proportion had either experienced actual losses (38.2%) or narrowly avoided becoming victims (31.5%). These findings suggest that cognitive awareness alone is insufficient to prevent victimization when users are exposed to sophisticated social engineering strategies. This observation supports the argument proposed by Krombholz *et al.,* (2015) that social engineering attacks primarily exploit human vulnerabilities rather

Advances in Community Services Research
Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
OPEN ACCESS
e-ISSN: 2985-9778

than technical weaknesses. In the context of quishing, perpetrators capitalize on individuals' inability to visually inspect URLs embedded in QR codes and manipulate users' trust in seemingly legitimate transaction environments. Consequently, the effectiveness of quishing attacks lies not only in technological deception but also in exploiting routine decision-making processes and limited security verification practices.

The motivational factors underlying QR code scanning behavior further illustrate how perpetrators exploit ordinary transactional habits. The present findings revealed that 44.6% of respondents scanned QR codes to make legitimate payments, whereas promotional offers, discounts, or giveaways influenced 24.1%. These findings suggest that quishing attacks are frequently embedded in contexts perceived by potential victims as normal, beneficial, or urgent. Rather than targeting technologically inexperienced individuals exclusively, perpetrators exploit situations that offer convenience and immediate rewards. This pattern aligns with the broader literature on social engineering, which emphasizes that trust, urgency, and perceived legitimacy constitute key determinants of compliance in cybercrime scenarios. Therefore, preventive strategies should extend beyond awareness campaigns and promote habitual verification practices, such as confirming merchant identities before authorizing transactions.

The discussion of post-scan consequences demonstrates that the impact of quishing extends beyond direct financial losses and frequently evolves into broader credential theft schemes. The findings showed that 39.5% of respondents were redirected to fraudulent websites resembling legitimate platforms, 11.1% were prompted to disclose sensitive personal information, and 9.9% experienced automatic downloads of suspicious APK files. These attack sequences represent the initial stages of account compromise. Malicious applications often operate as SMS stealers or forwarding tools that intercept one-time passwords (OTPs) sent by financial institutions. When combined with login credentials obtained via phishing websites, these intercepted authentication codes facilitate Account Takeover (ATO), enabling perpetrators to gain unauthorized access to digital accounts, transfer funds, and commit fraud. These findings suggest that current security features embedded within QR-based payment applications remain inadequate in identifying suspicious external links or warning users before harmful interactions occur.

The present findings are also consistent with previous studies emphasizing that the success of QR-phishing attacks depends on the interaction between technological vulnerabilities and human behavioral tendencies. While technological solutions such as secure QR infrastructures remain important, the findings highlight the equally significant role of digital security literacy and security-oriented behavioral intentions in mitigating cyber risks. This study extends prior discussions by demonstrating that even among relatively young and digitally active users, awareness of cybersecurity threats does not automatically lead to safer transactional practices. Therefore, interventions aimed at strengthening cybersecurity resilience should prioritize behavioral reinforcement mechanisms rather than relying solely on information dissemination.

From a legal perspective, the findings indicate that existing regulatory frameworks have not yet provided adequate preventive measures against emerging forms of QR code-based fraud. Although quishing-related activities clearly violate principles underlying personal data protection and electronic transaction regulations, the implementation of the Personal Data Protection Law (Law No. 27 of 2022) and the Electronic Information and Transactions Law remains predominantly reactive and focused on post-incident law enforcement. As a result, legal protection mechanisms frequently operate after consumers have already suffered financial or informational harm. This limitation becomes particularly

Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
OPEN ACCESS
e-ISSN: 2985-9778

problematic within static QRIS environments, where physical QR code manipulation can occur without immediate detection. Consequently, strengthening legal protection requires not only clearer institutional responsibilities and enforcement mechanisms but also the incorporation of preventive cybersecurity standards into payment system governance.

The practical implications of these findings underscore the necessity of collaborative efforts among multiple stakeholders. Bank Indonesia, the Indonesian Payment System Association (ASPI), Payment System Service Providers (PJSPs), and digital platform providers should strengthen the technological safeguards embedded in QR-based payment applications. The implementation of URL preview systems, domain allowlisting mechanisms, and anomaly detection technologies could provide users with early warnings before accessing potentially malicious destinations. Furthermore, accelerating the transition from static QRIS to dynamic QRIS systems, particularly among medium- and large-scale merchants, may substantially reduce opportunities for physical QR code manipulation. Simultaneously, ongoing public education initiatives should be developed to cultivate verification habits and encourage users to evaluate QR code-based interactions critically. Collectively, these measures have the potential to enhance the resilience of Indonesia's digital payment ecosystem against the growing threat of quishing attacks.

5. Concluding Remarks and Recommendation

This study aimed to analyze the mechanisms underlying QRIS quishing attacks, examine users' exposure to and vulnerability to QR-code-based fraud, and evaluate the adequacy of existing mitigation efforts and legal protections in the Indonesian context. Using a sequential explanatory mixed-methods approach, quantitative data obtained from 89 valid QRIS users in Bandung were complemented by qualitative evidence derived from open-ended responses and documented fraud cases. The findings indicate that phishing attacks predominantly exploit social engineering tactics embedded within routine transactional contexts, such as legitimate payment activities and promotional offers. Although 89.9% of respondents reported prior awareness of QR-code-related fraud risks, 38.2% had experienced actual victimization and 31.5% had narrowly avoided financial losses, suggesting that awareness alone does not necessarily translate into effective protective behavior. The findings further demonstrate that quishing incidents frequently evolve from deceptive QR code interactions into broader credential theft schemes involving phishing websites, malicious APK downloads, OTP interception, and ultimately Account Takeover (ATO). In addition, the persistence of static QRIS infrastructures and the limited implementation of preventive security features contribute to the continued vulnerability of QRIS users.

The present study offers several contributions from theoretical, practical, and policy perspectives. From a theoretical standpoint, the findings reinforce the notion that cybercrime targeting digital payment systems cannot be understood solely through a technological lens but must also incorporate behavioral and social-engineering dimensions. In practice, the study highlights the importance of strengthening security mechanisms embedded in QR-based payment applications, including URL preview systems, domain allowlisting, and anomaly detection. From a policy perspective, the findings emphasize the necessity of integrating consumer protection principles with proactive cybersecurity governance. The originality of this study lies in its attempt to combine behavioral evidence from QRIS users with an evaluation of legal preparedness to address emerging forms of QR-code-based

Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
OPEN ACCESS
e-ISSN: 2985-9778

cybercrime, thereby providing a more comprehensive understanding of quishing within Indonesia's evolving digital payment ecosystem.

Despite these contributions, several limitations should be acknowledged. First, the study was conducted exclusively among QRIS users residing in Bandung, thereby limiting the generalizability of the findings to other geographical contexts. Second, the respondent profile was predominantly composed of young adults and students, which may not adequately represent the experiences and security behaviors of other demographic groups. Third, the quantitative analysis relied primarily on descriptive methods given the characteristics of the available data. Therefore, future studies are encouraged to involve larger and more diverse samples across multiple regions in Indonesia and to employ inferential statistical techniques to examine relationships among cybersecurity awareness, QRIS usage intensity, and fraud exposure. Further investigations may also explore experimental approaches to assess the effectiveness of educational interventions and technological safeguards in reducing users' susceptibility to quishing attacks. Such efforts are expected to contribute to the development of a more secure, resilient, and trustworthy digital payment environment in Indonesia.

Statement of Use of Generative AI

During the preparation of this work, the author used generative artificial intelligence tools to support the scientific writing process. Grammarly was used to check grammar, refine writing style, and improve clarity in scientific writing. All interpretations, analyses, and conclusions presented in this study are the sole responsibility of the author.

References

Alam, M. A., Sarna, S. A., Rakibuzzaman, M., & Reza, J. (2025). Strengthening Cybersecurity Protocols to Safeguard U.S. Financial Infrastructure Against Emerging Threats. *Advances in Economics & Financial Studies*, *3*(2), 71–82. https://doi.org/10.60079/aefs.v3i2.506

Andriyani, F., Siagian, B., Suciati, P., & Citra, A. (2025). QRIS Adoption and Utilization: Examining Gen Z's Digital Payment Behavior Among Indonesian Vocational Students. *Jurnal Vokasi Indonesia*, *13*(1), 7. https://doi.org/10.7454/jvi.v13i1.1233

Anisa, F. N., & Andraini, F. (2023). Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Menggunakan Sistem Pembayaran Berbasis QRIS (Quick Response Code Indonesian Standard). *Jurnal Cahaya Mandalika*, *4*(2), 909–918.

Bank Indonesia. (2023). Peraturan Bank Indonesia Nomor 3 Tahun 2023 tentang Perlindungan Konsumen Bank Indonesia. https://www.bi.go.id/id/publikasi/peraturan/Pages/pbi_250323.aspx

Bank Indonesia. (2024). Quick Response Code Indonesian Standard (QRIS). Bank Indonesia.

Baottong, M. H., Kausar, A., Taufiq, M. I., & Krisnanto, B. (2025). Mitigating QR-Phishing Risks in Indonesian Digital Payments Through Security Behavior Intentions Scale. *Jurnal Manajemen Perbankan Keuangan Nitro*, *1*(3), 78–92. https://doi.org/10.56858/jmpkn.v1i3.757

Coils. (2023). The Puzzle of the Spread of Fake QRIS in Jakarta Mosques. Jakarta: KumparanNEWS.

Hamzah Muchtar, E., Trianto, B., Maulana, I., Alim, M. N., Marasabessy, R. H., Hidayat, W., Junaedi, E., & Masrizal. (2024). Quick response code Indonesia standard (QRIS) E-payment adoption: customers perspective. *Cogent Business & Management*, *11*(1), 2316044. https://doi.org/10.1080/23311975.2024.2316044

Herryani, M. R. T. R. (2023). Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia: Meningkatkan Perlindungan Hukum dalam Transaksi Digital: Mengatasi Sistem QRIS Palsu di Indonesia. *Rechtsidee*, *11*(1), 10.21070/jihr.v12i1.990. https://doi.org/10.21070/jihr.v12i1.990

Indonesia, B. (2019). Implementation of the National Standard Quick Response Code for Payments. Rules of the Board of Governors (p . No.21/18/PADG/2019). Jakarta: Bank Indonesia.

Volume 4, Issue 2 (2026). 68-81
DOI: https://doi.org/10.60079/acsr.v4i2.878
e-ISSN: 2985-9778

Otoritas Jasa Keuangan. (2023). Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. https://ojk.go.id/id/regulasi/Pages/POJK-Nomor-22-Tahun-2023.aspx

Purwatiningsih, A. P., Fitria, S., Indriani, A., & Kuriawan, C. S. (2025). Adoption of QRIS digital payment in Indonesia and Malaysia: A technology acceptance and knowledge perspective. *International Journal of Innovative Research and Scientific Studies*, *8*(6), 704–713.

Rahayu, T. P. (2024). Analisis Perlindungan Hukum bagi Pelaku Usaha Penyedia Sistem Pembayaran Qris (Quick Response Indonesian Standard) berdasarkan Undang-Undang Nomor 8 Tahun 1999. *Proceedings Series on Social Sciences & Humanities*, *17*, 444–449.

Rahman, A. (2024). Financial Inclusion through Technological Advancements in Banking Institutions: An Analytical Review. *Advances: Jurnal Ekonomi & Bisnis*, *2*(3), 163–173. https://doi.org/10.60079/ajeb.v2i3.303

Santika, A. Z., Musyaffi, A. M., & Zairin, G. M. (2024). Factors influencing the adoption of QRIS digital payments in MSMEs. *Jurnal Akuntansi, Perpajakan Dan Auditing*, *5*(1), 172–187. https://doi.org/10.21009/japa.0501.13

Sarkhi, M., & Mishra, S. (2024). Detection of QR Code-based Cyberattacks using a Lightweight Deep Learning Model. *Engineering, Technology & Applied Science Research*, *14*(4), 15209–15216. https://doi.org/10.48084/etasr.7777

Sasra, A. D., & Baidhowi, B. (2025). Perlindungan Hukum Dalam Transaksi Nontunai Berbasis Quick Response Code Indonesian Standards (QRIS) Berdasarkan Perspektif Hukum Perbankan. *Jurnal Ilmiah Nusantara*, *2*(4), 266–274. https://doi.org/10.61722/jinu.v2i4.5030

Sharevski, F., Devine, A., Pieroni, E., & Jachim, P. (2022). Phishing with malicious QR codes. *Proceedings of the 2022 European Symposium on Usable Security*, 160–171.

Sharevski, F., Mossano, M., Veit, M. F., Schiefer, G., & Volkamer, M. (2024). Exploring phishing threats through QR codes in naturalistic settings. *Symposium on Usable Security and Privacy (USEC) 2024*, *208*, 1–25. https://doi.org/10.14722/usec.2024.23050

Singkeruang, A. W. T. F., Susanto, S. E., & Saeni, N. (2025). Mitigating the Risk of Qushing Threats (QR Phishing) using the Security Behavior Intentions Scale (SeBIS) in supporting digital economic security. *Paradoks: Jurnal Ilmu Ekonomi*, *8*(2), 685–696. https://doi.org/10.57178/paradoks.v8i2.1196

Suseno, F. (2025). Evaluating QRIS Adoption: a pathway to inclusive digital payment for indonesia MSMEs. *GIC Proceeding*, *3*, 93–103. https://doi.org/10.30983/gic.v3i1.850

Tandel, S., Chordiya, J., & Patil, P. S. H. (2025). Tricked by the Square: Investigating the Rise and Reach of Quishing Attacks. *No. April*.

Trad, F., & Chehab, A. (2025). Detecting quishing attacks with machine learning techniques through qr code analysis. *ArXiv Preprint ArXiv:2505.03451*. https://doi.org/10.48550/arXiv.2505.03451

Utami, N. (2025). Adopsi pembayaran digital melalui QRIS dan dampaknya terhadap kinerja finansial UMKM di Daerah Istimewa Yogyakarta. *TRANSAKSI*, *17*(1), 1–13. https://doi.org/10.25170/transaksi.v17i1.7116

Wang, Z., Zhu, H., & Sun, L. (2021). Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities, and Attack Methods. *IEEE Access*, *9*, 11895–11910. https://doi.org/10.1109/ACCESS.2021.3051633

Weinz, M., Zannone, N., Allodi, L., & Apruzzese, G. (2025). The impact of emerging phishing threats: Assessing quishing and llm-generated phishing emails against organizations. *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*, 1550–1566. https://doi.org/10.1145/3708821.3736195

Windani, S., Fakhirah, P., Saleh, F., & Alamsyah, M. (2025). Legal Protection of Personal Data in Electronic Transactions through the QRIS Payment System in Indonesia. *Proceedings of International Conference on Islamic Community Studies*, 818–824. https://proceeding.pancabudi.ac.id/index.php/ICIE/article/view/581

Corresponding author
Yulianah can be contacted at: yulianah1288@gmail.com