Jurnal Akuntansi, Keuangan dan Auditing
Vol.6 (No.2), 2025, Hal: 32 – 46
DOI : 10.56696/jaka.v6i2.15318
http://publikasi.dinus.ac.id/index.php/jaka

GEN Z'S UNDERSTANDING OF INTERNAL CONTROLS DOMINATES QRIS PHISHING PREVENTION

Lukiyana Nurul Izza Kartika[1*] dan Zaky Machmuddah[2]
[1,2]Progdi Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Dian Nuswantoro
Jl. Nakula I No. 5-11 Semarang, Indonesia
[*]Corresponding Author: 212202204647@mhs.dinus.ac.id

Diterima: November 2025; Direvisi: Desember 2025; Dipublikasikan: Januari 2026

ABSTRACT

This study highlights the increasing cases of QRIS phishing targeting Generation Z through social media using various social engineering techniques. The research analyzes the influence of understanding internal controls, risk awareness, and self-efficacy on the effectiveness of QRIS phishing prevention. A quantitative approach was employed with a population of 10,951 active students at Dian Nuswantoro University and a sample of 408 respondents selected through purposive sampling based on their experience conducting QRIS transactions. Data were analyzed using multiple linear regression with SPSS. The results show that understanding internal controls, risk awareness, and self-efficacy have positive and significant effects on QRIS phishing prevention, both simultaneously and partially. Among the three variables, understanding internal controls is the most dominant factor. These findings underscore the importance of strengthening cybersecurity literacy to promote safer digital payment behavior among Generation Z.

Keywords: Quishing; Generation Z; Internal Controls; Risk Awareness; Self-Efficacy

ABSTRAK

Penelitian ini menyoroti meningkatnya kasus phishing QRIS yang menyasar Generasi Z melalui media sosial dengan berbagai teknik social engineering. Studi ini menganalisis pengaruh pemahaman pengendalian internal, kesadaran risiko, dan efikasi diri terhadap efektivitas pencegahan phishing QRIS. Pendekatan kuantitatif digunakan dengan populasi 10.951 mahasiswa aktif Universitas Dian Nuswantoro dan sampel 408 responden yang dipilih melalui purposive sampling berdasarkan pengalaman melakukan transaksi QRIS. Data dianalisis menggunakan regresi linear berganda dengan SPSS. Hasil penelitian menunjukkan bahwa pemahaman pengendalian internal, kesadaran risiko, dan efikasi diri berpengaruh positif dan signifikan terhadap pencegahan phishing QRIS, baik secara simultan maupun parsial. Di antara ketiga variabel, pemahaman pengendalian internal merupakan faktor paling dominan. Temuan ini menegaskan pentingnya penguatan literasi keamanan siber untuk mendorong perilaku pembayaran digital yang lebih aman pada Generasi Z.

Kata Kunci: Quishing; Generasi Z; Pengendalian Internal; Kesadaran Risiko; Efikasi Diri

INTRODUCTION

The Indonesian digital payment ecosystem has experienced remarkable evolution since Bank Indonesia introduced the Quick Response Code Indonesian Standard (QRIS) in 2019, fundamentally altering transaction patterns nationwide. According to an official Bank Indonesia (2025), as of the first half of 2025, QRIS had reached 57 million users and 39.3 million merchants, with 93.16% of them being Micro, Small, and Medium Enterprises (MSMEs). The total transaction volume reached 6.05 billion, with a value of IDR 579 trillion, underscoring the swift adoption of the QR code-based digital payment system in Indonesia.

This rapid growth trajectory, though instrumental in advancing financial inclusion, has simultaneously intensified security gaps, especially concerning QR code phishing (quishing) exploits that target unsuspecting users. According by Sharevski et al. (2025), a significant majority of users (67%) neglect to check URLs before scanning QR codes, a behavior that greatly increases their susceptibility to phishing schemes. Another study explains that malicious QR codes are often exploited by criminals to deceive users through public digital services, such as online parking systems or COVID-19 passport verification (Sharevski et al., 2022). From a regulatory perspective, Pattynama et al. (2024) argue that the legal protection for QRIS users remains insufficient, particularly against the use of counterfeit QRIS, which has the potential to cause financial losses.

Meanwhile, Generation Z (Gen Z) occupies a pivotal role in the adoption of QRIS, a trend intrinsically linked to their characteristics as adaptive digital natives. Bank Indonesia data confirms this, indicating that Gen Z constituted 27.94% of total cross-generational QRIS users in early 2025 (Suara Merdeka, 2025). Their key role in driving the cashless society through QRIS is further underscored by research from Lau & Kulsum (2023), which identified ease of use, efficiency, and convenience as the primary drivers of their adoption. Unfortunately, underlying this high adoption rate are significant security vulnerabilities. Research by Sharevski et al. (2025) highlights that the younger generation's focus on transaction speed and convenience often leads them to neglect security aspects, consequently posing a higher risk of falling victim to QRIS phishing. The severity of this vulnerability is demonstrated by data from the Financial Services Authority (OJK). As reported by CNBC Indonesia (2024), from 2022 to the first quarter of 2024, total reported consumer losses from fraud and deception cases reached IDR 2.5 trillion, with approximately 155,000 complaints lodged. The OJK also acknowledged that the actual losses are likely higher than the recorded figures. This data further confirms that the threat of quishing has become a tangible challenge for Indonesia's digital payment ecosystem.

Most prior studies on QRIS have focused on external factors, such as ease of use, perceptions of system security, and legal protections against QR code misuse (Safitri & Fihartini, 2024; Pattynama et al., 2024; Lau & Kulsum, 2023). However, digital security threats such as QR code phishing (quishing) are also profoundly influenced by users' internal factors. The Protection Motivation Theory (PMT) provides a relevant theoretical framework, specifically through the component of coping appraisal, which encompasses self-efficacy and belief in the effectiveness of preventive actions (Maddux & Rogers, 1983). Azhari & Bayunitri (2025) found that an understanding of internal control mechanisms is significantly associated with the prevention of digital fraud. Concurrently, while Singkeruang et al. (2025) and Lee et al. (2023) affirm the crucial role of self-efficacy in reducing vulnerability to quishing. These findings are reinforced by other studies, Ding (2024) highlights the critical role of internal control in fraud prevention and Hassan et al. (2024) found that cybersecurity efficacy directly influences protective behavior. Furthermore, Amoah & Acquah (2022) warns that low QR code security literacy further increases the likelihood of quishing attacks. Therefore, a research gap remains in integrating the aspects of internal control, self-efficacy, and risk awareness into a single empirical model, particularly concerning Generation Z as the most dominant yet digitally vulnerable group of QRIS users.

Given the urgency of the quishing threat and the dominance of Generation Z as the primary QRIS users, this study empirically examines the contribution of internal control comprehension, risk awareness, and self-efficacy in preventing QR code phishing. The theoretical framework employed is the Protection Motivation Theory (PMT), where threat appraisal is represented by risk awareness, while coping appraisal encompasses self-efficacy and the belief in the effectiveness of internal controls (Maddux & Rogers, 1983). Research by Handoyo & Bayunitri (2021) supports this proposition, demonstrating that strengthening

internal control systems is significant in suppressing the potential for fraud in digital environments. Conversely, the technological complexity of manipulation in QR code phishing attacks Amoah & Acquah (2022) renders individuals with low-risk awareness and self-efficacy the most vulnerable targets. Therefore, this study seeks to address a literature gap while providing both theoretical and practical contributions to strengthening digital payment security. It aims to overcome the scarcity of research by simultaneously testing these three internal factors in the context of quishing among Generation Z. The findings are expected not only to provide a theoretical contribution by extending the PMT model in the digital payment security domain but also to offer a practical contribution in the form of recommendations for enhancing consumer protection for QRIS users against increasingly sophisticated phishing attacks.

LITERATURE REVIEW

Protection Motivation Theory (PMT)

This research employs the Protection Motivation Theory (PMT) as its principal theoretical basis, originally introduced by Rogers (1975) and later enhanced by Maddux & Rogers (1983). Protection Motivation Theory posits a two-stage cognitive process in response to threats. Individuals first evaluate the severity of the risk itself, and then they assess their own ability to execute a protective response effectively. Threat appraisal pertains to the perceptions of vulnerability to a threat and its perceived severity. In contrast, coping appraisal encompasses an individual's belief in the effectiveness of a recommended protective response (response efficacy), their confidence in their ability to perform it (self-efficacy), and the consideration of associated costs or barriers (Maddux & Rogers, 1983). Within the context of digital security, PMT has become one of the most widely used theoretical frameworks for analyzing preventive behaviors against cyber threats, including phishing and QR code-based attacks (Crossler, 2009). Recent studies confirm the continued relevance of PMT in explaining the digital security behaviors of younger generations, such as Generation Z (Ma & Chen, 2023). Furthermore, Lee et al. (2023) demonstrated that PMT effectively explains the relationship between self-efficacy, protective attitudes, and vulnerability to phishing, thereby affirming its role as a robust conceptual foundation for research on quishing prevention.

Understanding of Internal Control

Internal control represents a structured framework consisting of protocols, processes, and safeguards designed to prevent fraudulent activities while ensuring operational effectiveness and efficiency within an organization. In an individual context, the understanding of internal control reflects the extent to which a person recognizes the importance of transaction verification, monitoring activities, and the use of digital security procedures. Within the Protection Motivation Theory (PMT) framework, this understanding is classified as response efficacy, namely the belief that a preventive action will be effective in reducing a threat (Crossler, 2009; Maddux & Rogers, 1983).

The study conducted by Azhari and Bayunitri (2025) reinforces this concept by demonstrating that internal control has a positive and significant effect on fraud prevention. Their findings highlight that clear authorization procedures, adequate documentation, and strong supervisory mechanisms effectively reduce opportunities for fraudulent behavior. This evidence supports the notion that the higher an individual's understanding of internal control mechanisms, the greater their ability to identify and prevent potential fraudulent actions. Furthermore, Faisol et al. (2023) emphasize that strengthening ethical frameworks and organizational culture enhances the effectiveness of internal controls, thereby reducing the likelihood of fraud. Research by Lau and Kulsum (2023) on Generation Z students also shows that a sound understanding of internal control encourages more cautious behavior when conducting transactions using QRIS, as individuals are more aware of the verification steps

that must be followed. Therefore, the higher an individual's understanding of internal control, the more likely they are to engage in preventive actions against quishing threats.

Risk Awareness

Risk awareness in the context of quishing prevention refers to users' subjective evaluation of their potential vulnerability to an attack and their perception of the seriousness of its possible consequences. Within the framework of Protection Motivation Theory (PMT), risk awareness is positioned within threat appraisal, which serves as a trigger for the development of protective motivation (Maddux & Rogers, 1983). The study by Singkeruang et al. (2025) highlights that users' level of risk awareness plays a critical role in mitigating quishing risks. Individuals with higher digital risk awareness particularly regarding suspicious QR codes and unsafe scanning behaviors are better equipped to identify and avoid potential quishing attempts. In contrast, low risk awareness not only heightens user vulnerability but also decreases the likelihood of adopting basic security practices.

Findings from Danquah et al. (2024) in the mobile banking context further reveal that perceived severity and perceived response efficacy significantly influence an individual's intention to secure transactions, whereas perceived vulnerability alone may not be sufficient to motivate protective behavior. Supporting this view, Amoah & Acquah (2022) emphasize that weak public literacy regarding QR code security creates substantial opportunities for quishing perpetrators, as many users remain unaware of the potential for QR code manipulation. Therefore, enhancing risk awareness—encompassing both perceived vulnerability and the severity of potential consequences—is essential for encouraging protective behaviors aimed at preventing quishing.

Self-Efficacy

Self-efficacy refers to an individual's belief in their own ability to carry out protective actions when confronted with cybersecurity threats in digital environments. Within the framework of Protection Motivation Theory (PMT), self-efficacy constitutes a key component of coping appraisal, namely an individual's evaluation of their capacity to cope with threats, which ultimately shapes their level of protective motivation (Maddux & Rogers, 1983). Individuals with high self-efficacy feel confident in their ability to implement preventive measures, such as identifying suspicious QRIS transactions, using QRIS safely, and refusing to scan untrusted QR codes.

According to Ma & Chen (2023), although digital natives generally possess high levels of technological literacy, self-efficacy remains a differentiating factor that determines whether such awareness can be translated into actual protective behavior. Empirical findings further reinforce the central role of self-efficacy in preventing both phishing and quishing. Lee et al., (2023) demonstrate that self-efficacy significantly reduces vulnerability to phishing attacks via instant messaging, with cautious behavior serving as an important mediating factor. In addition, a study by Hassan et al. (2024), which examined PMT in the context of digital security in Southeast Asia, identified self-efficacy as a primary predictor of online fraud prevention behavior. Consistent with these findings, Singkeruang et al. (2025) report that Generation Z university students in Indonesia with high self-efficacy are better able to avoid quishing attacks by utilizing available digital security indicators. Therefore, self-efficacy can be regarded as a pivotal psychological determinant influencing the effectiveness of quishing prevention behaviors among QRIS users.

Quishing Prevention

Quishing prevention can be defined as the protective behaviors performed by QRIS users to avoid QR code-based phishing attacks. These behaviors include verifying transaction details,

confirming merchant identity, utilizing multi-factor authentication, and reporting suspicious QR codes. Within the Protection Motivation Theory (PMT) framework, this protective behavior is a direct outcome of the interaction between threat appraisal—comprising risk awareness, perceived severity, and perceived vulnerability—and coping appraisal—encompassing self-efficacy and response efficacy (Maddux & Rogers, 1983). A study by Lau & Kulsum (2023) indicates that Generation Z students who understand the importance of security are more likely to exhibit preventive behaviors when using QRIS, although their actions are still influenced by transaction convenience. Aligning with this, Danquah et al. (2024), in a digital banking context, found that risk perception and trust in the effectiveness of controls play significant roles in encouraging consumer protective behavior.

Nonetheless, contemporary literature indicates that quishing prevention behavior remains suboptimal. Sharevski et al. (2025) highlight that most QR code users prioritize speed and convenience over performing security verifications, thereby increasing their vulnerability to attacks. Findings from Amoah & Acquah (2022) research also reveal that weak QR code security literacy means many users are unaccustomed to thoroughly checking transaction details. In Indonesia, Pattynama et al. (2024) identifies persistent legal and regulatory challenges that have not yet fully succeeded in protecting QRIS users from the threat of QR code manipulation, making individual protective behavior the first line of defense.Therefore, quishing prevention must be understood as a combination of individual factors, effective internal control systems, and public regulation and education to create a secure digital payment ecosystem.

Hypothesis Development

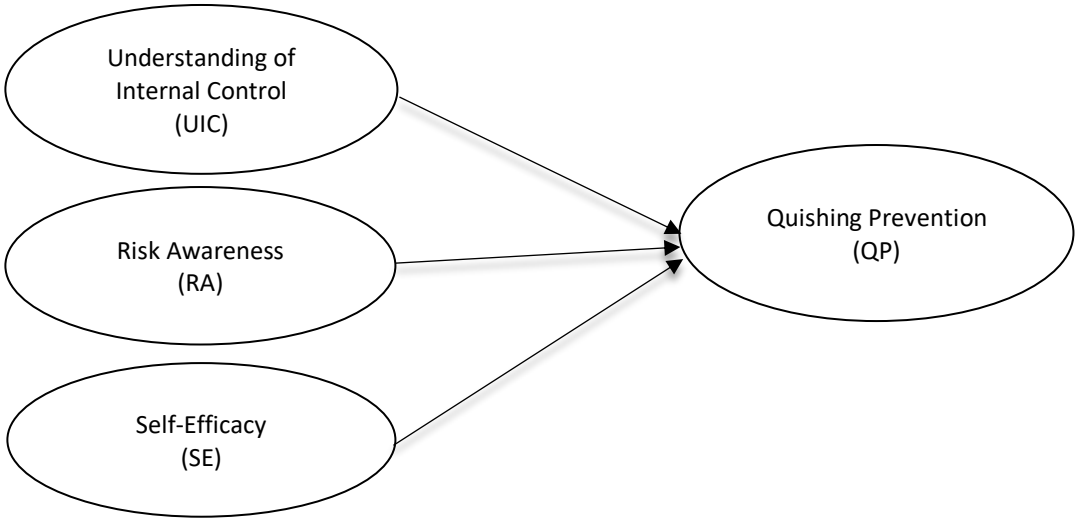

Figure 1. Conceptual Framework from the Research
Source: Data Research, 2025

The Influence of Interal Control Understanding on Quishing Prevention

A user's higher understanding of internal control corresponds to a greater capability to perform quishing prevention when using QRIS among Generation Z. Within the Protection Motivation Theory (PMT) framework, the understanding of internal control relates to response efficacy—the belief that a preventive action is effective in countering a threat (Maddux & Rogers, 1983). Research by Agyemang (2021) demonstrated that the effectiveness of internal controls has a significant positive influence on fraud prevention in the banking sector. Ding

(2024) also affirmed that an adaptive internal control system significantly reduces fraudulent activities. Furthermore, Shehu (2025) showed that control and monitoring activities have a significant positive effect on fraud mitigation in SMEs. In Indonesia, a study on the implementation of Cash Management Systems Anggia & Mutmainah (2025) also found that control behaviors significantly influence quishing prevention in QRIS transactions. Based on PMT and these empirical findings, the research hypothesis is:

H1: Understanding of internal control has a positive and significant effect on quishing prevention among Generation Z QRIS users.

The Influence of Risk Awareness on Quishing Prevention

A higher user awareness of quishing risks corresponds to a greater tendency to undertake preventive actions, such as verifying merchant authenticity or avoiding scanning suspicious QR codes. Within the Protection Motivation Theory (PMT) framework, risk awareness constitutes part of threat appraisal, which posits that higher threat perception leads to stronger protective motivation to act (Maddux & Rogers, 1983). Previous research supports this relationship. Sharevski et al. (2022) found that user awareness is significantly associated with quishing prevention behavior. Geisler & Pöhn (2024) demonstrated that high awareness significantly increases secure behaviors. Furthermore, studies in Indonesia by Baottong et al. (2025) and Singkeruang et al. (2025) proved that risk awareness has a significant positive effect on quishing mitigation among digital payment users. Based on PMT and these empirical findings, the research hypothesis is:

H2: Risk awareness has a positive and significant effect on quishing prevention among Generation Z QRIS users.

The Influence of Self-Efficacy on Quishing Prevention

The higher a user's level of self-efficacy, the stronger their conviction in their capability to protect themselves from quishing attacks through actions such as merchant verification, utilization of security features, or refusal to scan suspicious QR codes. Within the Protection Motivation Theory (PMT) framework, self-efficacy constitutes a crucial element of coping appraisal, which pertains to an individual's belief in their personal capacity to execute recommended protective behaviors against threats (Maddux & Rogers, 1983). Empirical evidence substantiates this relationship Lee et al. (2023) demonstrated that self-efficacy significantly reduces vulnerability to phishing attacks. Ma & Chen (2023) established that enhanced self-efficacy significantly promotes phishing reporting behavior. Furthermore, Puri et al. (2025) confirmed that self-efficacy exerts a significant influence on fraud-safe behaviors in digital payments. Supporting these findings, studies by Sharevski et al. (2022) and Geisler & Pöhn (2024) reinforce that elevated self-efficacy drives proactive prevention behaviors against quishing. Based on the theoretical foundation of PMT and these empirical findings, the research hypothesis is formulated as follows:

H3: Self-efficacy has a positive and significant effect on quishing prevention among Generation Z QRIS users.

RESEARCH METHOD

Utilizing an explanatory quantitative framework with survey-based data collection, this examination probes how comprehension of internal controls, risk perception, and self-efficacy shape quishing prevention behaviors within Generation Z QRIS user demographics. The research population consists of 10,951 active students at Universitas Dian Nuswantoro. The sample was selected using purposive sampling technique based on criteria of active students aged 18-25 years who had conducted at least one transaction using QRIS, resulting in 408

eligible respondents. The research instrument was an online questionnaire based on Google Forms, utilizing a 5-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree).

This study measured four main constructs: Understanding Internal Control (UIC) adapted from the COSO framework through Azhari & Bayunitri (2025), focusing on transaction verification, device security, and transaction monitoring; Risk Awareness (RA) measured using the SeBIS scale from Singkeruang et al. (2025), emphasizing suspicion toward suspicious QR codes and excessive offers; Self-Efficacy (SE) assessing confidence in recognizing threats and securing applications; and Quishing Prevention (QP) measuring concrete preventive behaviors such as source verification and data protection. Data analysis was conducted using SPSS version 25 with the following stages Ghozali (2018). The analytical stages included instrument validity and reliability tests, as well as classical assumption tests encompassing normality, multicollinearity, and heteroscedasticity tests. After all assumptions were met, hypothesis testing was performed using multiple linear regression analysis to examine the direct influence of internal control understanding, risk awareness, and self-efficacy on quishing prevention.

RESULTS AND DISCUSSION

Validity Test

Table 1. Validity Test

Variabel	Item	Pearson Correlation	R Table	Remarks
Quishing Prevention	Y1	0.753	0.0971	Valid
	Y2	0.773	0.0971	Valid
	Y3	0.776	0.0971	Valid
	Y4	0.659	0.0971	Valid
	Y5	0.693	0.0971	Valid
	Y6	0.762	0.0971	Valid
Understanding of Internal Controls	X1.1	0.677	0.0971	Valid
	X1.2	0.653	0.0971	Valid
	X1.3	0.691	0.0971	Valid
	X1.4	0.666	0.0971	Valid
	X1.5	0.602	0.0971	Valid
	X1.6	0.673	0.0971	Valid
Risk Awareness	X2.1	0.659	0.0971	Valid
	X2.2	0.739	0.0971	Valid
	X2.3	0.793	0.0971	Valid
	X2.4	0.744	0.0971	Valid
	X2.5	0.679	0.0971	Valid
Self-Efficacy	X3.1	0.805	0.0971	Valid
	X3.2	0.758	0.0971	Valid
	X3.3	0.608	0.0971	Valid
	X3.4	0.757	0.0971	Valid
	X3.5	0.700	0.0971	Valid
	X3.6	0.787	0.0971	Valid

Source: Output SPSS vers. 25 (2025)

Referring to the results of the validity assessment displayed in Table 1, it can be inferred that all questionnaire items across each variable are deemed valid. This inference arises from the fact that the Pearson correlation coefficient for every item surpasses the critical r-table threshold of 0.0971, which serves as the benchmark for construct validity in this research. Therefore, the instrument employed in this study is statistically validated, demonstrating accuracy in measuring the designated constructs and reliability in generating meaningful data for subsequent analysis.

Reliability Test

Table 2. Reliability Test

Variabel	Cronbach's Alpha	Keterangan
QP	0.822	Reliabel
UIC	0.738	Reliabel
RA	0.823	Reliabel
SE	0.761	Reliabel

Source: Output SPSS vers. 25 (2025)

Reliability testing demonstrated strong internal consistency for all constructs, with each variable's Cronbach's Alpha value exceeding the 0.70 acceptability threshold, as presented in the table above. Specifically, the reliability values for each variable are as follows: Quishing Prevention (QP) at 0.822, Understanding of Internal Controls (UIC) at 0.738, Risk Awareness (RA) at 0.823, and Self-Efficacy (SE) at 0.761, Therefore, all questionnaire instruments used in this study have met the criteria for good reliability, indicating that these measurement tools are consistent and trustworthy in measuring their intended constructs. Consequently, the data generated is suitable for further analysis.

Classical Assumption Test Results
Normality Test

Table 3. Normality Test

			Unstandardize Residual
N			408
Normal Parameters[a,b]	Mean		.0000000
	Std. Deviation		1.99911129
Most Extreme Differences	Absolute		. 056
	Positive		. 042
	Negative		-.056
Test Statistic			. 056
Asymp. Sig (2-tailed)			.004[c]
Monte Carlo Sig. (2-tailed)	Sig.		.149[d]
	99% Confidence Interval	Lower Bound	.140
		Upper Bound	.158

Source: Output SPSS vers. 25 (2025)

Based on the results of the normality test using Kolmogorov-Smirnov, the Asymp. Sig. (2-tailed) value of 0.004 indicates that asymptotically the data are not normally distributed as the value is less than 0.05. Nevertheless, the supplementary analysis employing the Monte Carlo Sig. (2-tailed) approach produced a significance value of 0.149. As this value exceeds the 0.05 threshold, it indicates that the residuals conform to the assumption of normal distribution.This approach is supported by Lomas & Grauer (2013) who assert that the Monte Carlo procedure produces a valid empirical p-value, particularly when conventional tests like Kolmogorov-Smirnov yield questionable results due to their sensitivity to large sample sizes. The consistency of this approach is also evident in applied research in Indonesia, as implemented by Azizah et al. (2023), who concluded normality based on a Monte Carlo Sig. (2-tailed) value above 0.05. Therefore, the use of the Monte Carlo significance value in this study is methodologically justified and has precedent in the literature, thereby strengthening the validity of the regression model's normality assumption.

Multicollinearity Test

Table 4. Multicollinearity Test

Coefficients[a]

Model		Collinearity Statistics	
		Tolerance	VIF
1	(Constant)		
	Understanding of Internal Controls	.624	1.603
	Risk Awareness	.580	1.723
	Self-Efficacy	.657	1.522

a. Dependent Variable: Quishing Prevention

Source: Output SPSS vers. 25 (2025)

Based on the multicollinearity test results presented in Table 4, it can be concluded that there is no indication of multicollinearity in the regression model. This is evidenced by the Tolerance values for all independent variables—Understanding of Internal Controls (0.624), Risk Awareness (0.580), and Self-Efficacy (0.657)—all exceeding the threshold value of 0.10. Correspondingly, the Variance Inflation Factor (VIF) values for each variable, namely 1.603, 1.723, and 1.522, are all well below the critical value of 10. Therefore, this regression model satisfies the assumption of no multicollinearity and is appropriate for further hypothesis testing.

Heterokedasticity Test (Glejser Test)

Table 5. Heterokedasticity Test

Coefficients[a]

	Unstandardized Coefficients		Standardized Coefficients			Correlations			Collinearity Statistics	
Model	**B**	**Std. Error**	**Beta**	**t**	**Sig.**	**Zero order**	**Partial**	**Part**	**Tolerance**	**VIF**
1(Constant)	3.643	.630		5.780	.000					
Understanding of Internal Controls	-.019	.027	-.043	-.695	.487	-.101	-.035	-.034	.624	1.603
Risk Awareness	-.002	.026	-.005	-.071	.944	-.090	-.004	-.003	.580	1.723
Self-Efficacy	-.052	.028	-.112	-1.849	.065	-.092	-.092	-.091	.657	1.522

Source: Output SPSS vers. 25 (2025)

The results of the heteroskedasticity test using the Glejser method, as presented in Table 5, the significance values (Sig.) for the independent variables are as follows: Understanding of Internal Controls is 0.487, Risk Awareness is 0.944, and Self-Efficacy is 0.065. As all these significance values exceed the 0.05 threshold, the test fails to provide sufficient statistical evidence to reject the null hypothesis of homoskedasticity. Therefore, it can be concluded that the regression model does not exhibit significant symptoms of heteroskedasticity. This result indicates that the residual variance is constant, thereby fulfilling the classical assumption of

homoskedasticity. This condition is crucial to ensure that the estimated regression parameters are BLUE (Best Linear Unbiased Estimators), in accordance with the assumptions of the classical linear regression model (Ghozali, 2018). Consequently, the regression analysis conducted is reliable, and the outcomes of the hypothesis tests can be interpreted with a greater degree of accuracy.

Auto Correlation

Table 6. Auto Correlation

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the estimate	R Square Change	F Change	df 1	df2	Sig. F Change	Durbin Watson
1	.803[a]	.644	.642	2.007	.644	234.965	3	404	.000	1.954

Source: Output SPSS vers. 25 (2025)

Based on the results of the autocorrelation test presented in Table 6, the Durbin-Watson (DW) value obtained is 1.954. This value lies within the acceptable range of –2 to +2, indicating that the regression model is free from both positive and negative autocorrelation. Therefore, it can be concluded that the classical assumption regarding the absence of autocorrelation is fulfilled. This result implies that the residuals in the regression model are independent and not correlated across observations, ensuring that the regression model used in this study is valid and reliable for further analysis without bias caused by autocorrelation.

Multiple Linear Regression Analysis
Coefficient of Determination (R^2) Test

Table 7. R-squared Test

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the estimate
1	.803[a]	.644	.642	2.007

Source: Output SPSS vers. 25 (2025)

Based on the analysis results shown in Table 7, the multiple linear regression model obtained a correlation coefficient (R) of 0.803, which reflects a strong relationship between the independent variables—Understanding of Internal Controls, Risk Awareness, and Self-Efficacy—and the dependent variable, Quishing Prevention. The determination coefficient (R^2) value of 0.644 indicates that about 64.4% of the variation in quishing prevention can be accounted for by these three predictors, whereas the remaining 35.6% is attributed to other variables beyond the scope of this study. Moreover, the Adjusted R^2 value of 0.642 supports that the model maintains a high explanatory ability even after adjusting for the number of independent variables. Therefore, the regression model can be regarded as statistically robust and theoretically relevant in describing the preventive behavior against quishing among Generation Z QRIS users in Indonesia.

Partial Test

Table 8. T Test

Coefficients[a]					
	Unstandardized Coefficients		Standardize Coefficients		
Model	**B**	**Std. Error**	**Beta**	**t**	**Sig.**
1 (Constant)	3.723	.859		4.336	.000
Understanding of Internal Controls	.357	.037	.365	9.720	.000
Risk Awareness	.289	.036	.312	8.020	.000
Self-Efficacy	.303	.039	.287	7.833	.000

Source: Output SPSS vers. 25 (2025)

The findings of the partial analysis (t-test) presented in Table 8 demonstrate that the Understanding of Internal Controls variable recorded a coefficient of 0.357, a t-value of 9.720, and a significance level of 0.000 (< 0.05), signifying a statistically positive and significant impact on quishing prevention. In addition, the Risk Awareness variable produced a coefficient of 0.289, a t-value of 8.020, and a significance value of 0.000 (< 0.05), confirming that risk awareness exerts a positive and significant influence on quishing prevention efforts. Likewise, the Self-Efficacy variable yielded a coefficient of 0.303 with a t-value of 7.833 and a significance of 0.000 (< 0.05), validating its positive and significant contribution to the prevention of quishing.

Accordingly, the results partially demonstrate that all three independent variables contribute to strengthening quishing prevention efforts. In general, the t-test outcomes indicate that Understanding of Internal Controls, Risk Awareness, and Self-Efficacy each exert a positive and statistically significant influence on quishing prevention behavior. These results highlight that preventive initiatives against quishing become more effective when individuals exhibit a solid comprehension of internal control mechanisms, elevated risk awareness, and greater self-assurance in performing security-oriented actions.

Simultaneous Test

Table 9. F Test

ANOVA[a]						
Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	2946.701	3	982.234	243.965	.000[b]
	Residual	1626.553	404	4.026		
	Total	4573.255	407			

Source: Output SPSS vers. 25 (2025)

The outcomes of the simultaneous analysis (F-test) shown in Table 9 reveal an F-value of 243.965 with a significance level of 0.000 (< 0.05). These results suggest that the independent variables—Understanding of Internal Controls, Risk Awareness, and Self-Efficacy—jointly exert a statistically significant influence on the dependent variable, Quishing Prevention. Hence, it can be inferred that the regression model applied in this research is well-suited for hypothesis testing, as the combined effect of the three predictors meaningfully explains the variance in quishing prevention behavior.

Understanding of Internal Controls Positively and Significantly Affects Quishing Prevention (H1 Supported)

The results indicate that Understanding of Internal Controls has a positive and significant effect on quishing prevention, with a t-value of 9.720 and a significance level of 0.000 (< 0.05).

This result supports H1 and indicates that individuals with stronger knowledge of internal control mechanisms—such as verifying merchant identity, safeguarding OTP codes, and reviewing transaction notifications—are better equipped to prevent quishing attempts. This aligns with the study by Lau & Kulsum (2023) on Generation Z students, which indicated that a sound understanding of internal control contributes to more cautious behavior in digital transactions. It also corroborates prior research (Azhari & Bayunitri, 2025; Ding, 2024) showing that internal control understanding significantly decreases digital fraud risk, which in this context manifests as quishing.

Beyond confirming existing evidence, the present study extends the discussion by situating internal control knowledge within the daily practices of QRIS users. This suggests that preventive capacity is not only theoretical but also highly practical in guiding secure decision-making in real digital payment scenarios. More importantly, the ability to implement internal control principles in everyday transactions highlights the role of financial literacy and institutional support in reducing vulnerabilities to phishing-based attacks. Thus, strengthening internal control awareness among Generation Z users is essential to ensure the sustainability and security of QRIS adoption in Indonesia's digital economy.

Risk Awareness Positively and Significantly Affects Quishing Prevention (H2 Supported)

The results indicate that Risk Awareness has a positive and significant effect on quishing prevention, with a t-value of 8.020 and a significance level of 0.000 (<0.05). This outcome validates H2 by revealing that users with elevated consciousness regarding QR transaction vulnerabilities exhibit heightened vigilance in detecting and circumventing fraudulent code deployments. Such awareness drives protective behaviors, including verifying QR authenticity, double-checking transaction details, and refraining from scanning codes from untrusted sources. This aligns with the threat appraisal dimension of Protection Motivation Theory Maddux & Rogers (1983), where a higher perception of threat encourages defensive actions. Empirical studies have similarly emphasized this relationship—Sharevski et al. (2022) found that users with low risk perception were more likely to scan malicious QR codes without verifying the embedded links, while Geisler & Pöhn (2024) confirmed that visually appealing but deceptive QR codes exploit users' curiosity and lack of risk vigilance, especially among younger digital users.

Furthermore, this study's results are consistent with Baottong et al. (2025), who observed that security awareness significantly mitigates the likelihood of falling victim to QR-phishing in Indonesian digital payments, as well as Singkeruang et al. (2025), who emphasized the pivotal role of user risk awareness in shaping protective digital behavior. The present findings extend this body of research by situating risk awareness within the context of Generation Z QRIS users, revealing that cognitive recognition of phishing risks translates into proactive behavioral responses. Practically, enhancing digital security literacy—through targeted awareness campaigns, education initiatives, and collaborative outreach by regulators and payment service providers—can significantly reduce quishing vulnerability. Therefore, fostering risk awareness is not merely a cognitive concern but a strategic foundation for cultivating secure and responsible behavior in Indonesia's growing digital payment ecosystem.

Self-Efficacy Positively and Significantly Affects Quishing Prevention (H3 Supported)

The results indicate that Self-Efficacy has a positive and significant effect on quishing prevention, with a t-value of 7.833 and a significance level of 0.000 (<0.05). This finding supports H3 and implies that individuals with higher confidence in their ability to recognize and respond to quishing threats are more likely to engage in preventive behaviors. Individuals with strong self-efficacy tend to feel capable of implementing various security measures—such as verifying merchant identities, activating two-factor authentication, and reporting phishing

incidents through official channels. This result is consistent with Protection Motivation Theory Maddux & Rogers (1983), which identifies self-efficacy as a core component of coping appraisal, where individuals evaluate their capacity to perform protective actions. Moreover, this aligns with the studies by Lee et al. (2023) and Ma & Chen (2023), who found that self-efficacy plays a dominant role in shaping cybersecurity behavior, particularly in preventing phishing and social engineering attacks.

Recent empirical evidence further reinforces these findings. Puri et al. (2025) demonstrated that high levels of self-efficacy significantly enhance individuals' adaptive responses to cyber threats by fostering confidence and proactive security behavior. When users believe in their capacity to detect and manage online risks, they are more resilient to deceptive tactics such as phishing or quishing. This study extends prior research by situating self-efficacy within the daily behavior of Generation Z QRIS users, revealing that the belief in one's ability to take protective actions strengthens the effectiveness of digital security practices. Practically, interventions aimed at enhancing self-efficacy—such as interactive education, simulated phishing training, and user-centered security workshops—can increase digital preparedness and reduce susceptibility to QRIS-based phishing. Therefore, self-efficacy functions not merely as an indicator of personal confidence but as a foundational determinant of sustainable preventive behavior, supporting individual resilience and promoting collective security within Indonesia's expanding digital payment ecosystem.

CONCLUSION AND LIMITATIONS

This study empirically examines the influence of internal control understanding, risk awareness, and self-efficacy on quishing prevention among Generation Z QRIS users in Indonesia. The results indicate that all three variables have a positive and significant effect on quishing prevention, both individually and simultaneously, with Understanding of Internal Controls identified as the most dominant factor. This suggests that individuals with a stronger understanding of verification processes, control procedures, and transaction monitoring are more effective in preventing quishing attacks.

The findings support the relevance of Protection Motivation Theory (PMT) in explaining protective behavior in digital payment contexts, where risk awareness (threat appraisal) and self-efficacy together with internal control understanding (coping appraisal) jointly shape users' security behavior. Practically, the study highlights the importance of strengthening cybersecurity literacy among Generation Z through education, awareness campaigns, and institutional programs. Overall, quishing prevention is primarily driven by users' internal psychological and cognitive factors rather than solely by technological safeguards, emphasizing the need to enhance risk awareness, internal control understanding, and self-efficacy through continuous digital literacy and user empowerment initiatives.

The main limitation of this study lies in its sampling scope, as Generation Z respondents were drawn from only one university, which limits the generalizability of the findings to the broader Generation Z population in Indonesia. In addition, the relatively small sample size, representing only 3.7% of the total population, may reduce the representativeness of the data. These limitations were influenced by constrained data collection time, limited respondent accessibility, and varying levels of participation. Therefore, future research is recommended to expand the population and sampling coverage by involving multiple universities or different regions to obtain more representative and generalizable results. The implications of this study suggest that Generation Z should strengthen their understanding of internal controls, enhance risk awareness, and improve self-efficacy as key measures to prevent quishing threats and support the secure and sustainable use of QRIS.

REFERENCES

Agyemang, J. K. (2021). Internal Control And Fraud Prevention. *Journal Of Business And Entrepreneurial Studie*, *March*. Https://Www.Journalbusinesses.Consultorioampuero.Com/Index.Php/Revista/Article/View/234

Anggia, S., & Mutmainah, S. (2025). Can Cash Management System Reduce Fraud Indications In Government Transactions? *International Journal Of Science And Society*, *7*(1), 177–189. Https://Doi.Org/10.54783/Ijsoc.V7i1.1370

Anisa Safitri, & Yuniarti Fihartini. (2024). The Influence Of Perceived Ease Of Use And Security On Qris Usage Decisions Among The Community In Lampung Province. *Epaper Bisnis : International Journal Of Entrepreneurship And Management*, *1*(4), 189–198. Https://Doi.Org/10.61132/Epaperbisnis.V1i4.145

Awuah Amoah, G., & Hayfron-Acquah, J. B. (2022). Qr Code Security: Mitigating The Issue Of Quishing (Qr Code Phishing). *International Journal Of Computer Applications*, *184*(33), 975–8887.

Azhari, F., & Bayunitri, B. I. (2025). The Influence Of Internal Control And Individual Morality On Fraud Prevention In Industrial Garment Company. *Assets : Jurnal Ilmiah Ilmu Akuntansi, Keuangan Dan Pajak*, *9*(1), 94–106. Https://Doi.Org/10.30741/Assets.V9i1.1446

Azizah, N., Dahliani, Y., & Qomaruzzaman Ratu Edi, B. (2023). Pengaruh Citra Merek, Kualitas Produk, Desain Dan Iklan. *Jurnal Manajemen Bisnis Dan Manajemen Keuangan*, *4*(1), 93–107. Www.Jurnal.Itsm.Ac.Id

Crossler, R. E. (2009). *Protection Motivation Theory: Understanding The Determinants Of Individual Security Behavior*. 169.

Danquah, P., Matey, H. A., & Asiamah, K. (2024). Influence Of Protection Motivation Theory On Information Security Practices: The Case Of Ghanaian Mobile Banking Merchants. *Journal Of Applied Science And Information Technology*, *1*(1), 1–27.

Geisler, M., & Pöhn, D. (2024). *Hooked: A Real-World Study On Qr Code Phishing*. Http://Arxiv.Org/Abs/2407.16230

Ghozali, I. (2018). *Aplikasi Analisis Multivariate Dengan Program Ibm Spss 25* (Edisi 9). Badan Penerbit Universitas Diponegoro.

Hassan, S., Ahmad, R., Katuk, N., Ghazali, N. N., Aripin, J. A., & Ali, F. (2024). Staying One Step Ahead: Exploring Protection Motivation Theory To Combat Cyber-Fraud Among E-Services Users. *Procedia Computer Science*, *234*(2023), 1364–1371. Https://Doi.Org/10.1016/J.Procs.2024.04.011

Indonesia, B. (2025). *Capaian Implementasi Qris Semester I 2025*. Bank Indonesia. Https://Www.Bi.Go.Id/Id/Publikasi/Ruang-Media/News-Release/Pages/Sp_2717025.Aspx

Indonesia, C. (2024). *Bos Ojk Ungkap Uang Hilang Akibat Scam Dan Fraud Capai Rp 25 Triliun*. Https://Www.Cnbcindonesia.Com/Market/20241211121934-17-595022/Bos-Ojk-Ungkap-Uang-Hilang-Akibat-Scam-Dan-Fraud-Capai-Rp-25-Triliun

Lau, E. A., & Kulsum, U. (2023). Becoming A Cashless Society: The Role Of Qris From The Z-Generation Student's Perspective. *Journal Of Accounting And Strategic Finance*, *6*(1), 172–191. Https://Doi.Org/10.33005/Jasf.V6i1.404

Lee, Y. Y., Gan, C. L., & Liew, T. W. (2023). Thwarting Instant Messaging Phishing Attacks: The Role Of Self-Efficacy And The Mediating Effect Of Attitude Towards Online Sharing Of Personal Information. *International Journal Of Environmental Research And Public Health*, *20*(4). Https://Doi.Org/10.3390/Ijerph20043514

Lomas, A. L., & Grauer, G. F. (2013). Re: Tepoxalin No Longer Available Commercially. *American Journal Of Veterinary Research*, *74*(7), 948. Https://Doi.Org/10.2460/Ajvr.74.7.948

Ma, S., & Chen, C. (2023). Are Digital Natives Overconfident In Their Privacy Literacy? Discrepancy Between Self-Assessed And Actual Privacy Literacy, And Their Impacts On Privacy Protection Behavior. *Frontiers In Psychology*, *14*(June 2022), 1–11. Https://Doi.Org/10.3389/Fpsyg.2023.1224168

Maddux, J. E., & Rogers, R. W. (1983). Protection Motivation And Self-Efficacy: A Revised Theory Of Fear Appeals And Attitude Change. *Journal Of Experimental Social Psychology*, *19*(5), 469–479. Https://Doi.Org/10.1016/0022-1031(83)90023-9

Merdeka, S. (2025). *Bank Indonesia Catat Pengguna Qris Capai 56,28 Juta Hingga Awal 2025*. Https://Surabaya.Suaramerdeka.Com/Ekonomi/106115564093/Bank-Indonesia-Catat-Pengguna-Qris-Capai-5628-Juta-Hingga-Awal-2025#Google_Vignette

Mozes Haryanto Baottong, Al Kausar, Muhammad Imam Taufiq, B. K. (2025). Mitigating Qr-Phishing Risks In Indonesian Digital Payments Through Security Behavior Intentions Scale (Sebis). *Jurnal Manajemen Perbankan Keuangan Nitro*, *1*(3), 78–92. Https://Doi.Org/10.56858/Jmpkn.V1i3.757

Pattynama, F. M., Santoso, H. A., Miarsa, F. R. D., & Pribadi, T. (2024). Legal Problems For Quick Response Code Indonesian Standard (Qris) Users In Online Payment Transactions. *Anayasa : Journal Of Legal Studies*, *2*(1), 44–55. Https://Doi.Org/10.61397/Ays.V2i1.183

Puri, L., Kumar, A., & Singh, R. (2025). What Drives Or Discourages Fraud-Safe Behavior In Digital Transactions? A Brt Perspective. *Acta Psychologica*, *260*(September). Https://Doi.Org/10.1016/J.Actpsy.2025.105675

Roemkenya Madolidi Handoyo, B., & Indah Bayunitri, B. (2021). The Influence Of Internal Audit And Internal Control Toward Fraud Prevention. *International Journal Of Financial, Accounting, And Management*, *3*(1), 45–64. Https://Doi.Org/10.35912/Ijfam.V3i1.181

Sharevski, F., Devine, A., Pieroni, E., & Jachim, P. (2022). Phishing With Malicious Qr Codes. *Acm International Conference Proceeding Series*, *1*(1), 160–171. Https://Doi.Org/10.1145/3549015.3554172

Sharevski, F., Mossano, M., Veit, M. F., Schiefer, G., & Volkamer, M. (2025). *Exploring Phishing Threats Through Qr Codes In Naturalistic Settings*. *February*. Https://Doi.Org/10.14722/Usec.2024.23050

Shehu, T. S. (2025). Internal Control System And Fraud Mitigation: A Case Of Selected Smes In Nigeria. *Asian Journal Of Advanced Research And Reports*, *19*(4), 301–315. Https://Doi.Org/10.9734/Ajarr/2025/V19i4985

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

Xinyan Ding. (2024). The Effectiveness Of Internal Control Systems In Preventing Financial Fraud: A Case Study Of Multinational Corporations. *Economics & Management Information*, *September 2024*, 1–5. Https://Doi.Org/10.62836/Emi.V3i4.231