Cybersecurity Awareness and Digital Minimalism towards Cyber Fraud Prevention in Generation Z

Indah Dwi Novianti[1]
Anis Chariri[2]
[1,2]Faculty of Economics and Business, Universitas Diponegoro, Indonesia
Correspondences* **: indhhdw@students.undip.ac.id

ABSTRACT

The increasing adoption of digital banking among Generation Z has also heightened the risk of cybercrime, particularly cyber fraud. This study aims to analyze the influence of Cybersecurity Awareness and Digital Minimalism on Cyber Fraud Prevention using a quantitative approach within the Protection Motivation Theory (PMT) framework. Data were collected through an online questionnaire distributed via Google Form during January–May 2025 to 77 Generation Z respondents in Indonesia who use digital banking services. Respondents were selected using purposive sampling, and the data were analyzed with multiple linear regression (SPSS 27). The findings reveal that both independent variables positively and significantly affect cyber fraud prevention. These results suggest that enhancing digital security awareness and adopting a minimalist digital lifestyle can strengthen efforts to prevent cybercrime. This study contributes to the development of behavior-based prevention strategies and advances the field of digital forensic accounting.

Keywords: Cybersecurity Awareness; Digital Minimalism; Cyber Fraud Prevention

e-ISSN 2302-8556

Vol. 35 No. 9
Denpasar, 30 September 2025
Hal. 2428-2442

DOI:
10.24843/EJA.2025.v35.i09.p14

PENGUTIPAN:
Novianti, I. D., & Chariri, A. (2025). Cybersecurity Awareness and Digital Minimalism towards Cyber Fraud Prevention in Generation Z. *E-Jurnal Akuntansi*, 35(9), 2428-2442

RIWAYAT ARTIKEL:
Artikel Masuk:
20 Mei 2025
Artikel Diterima:
18 Juli 2025

Cybersecurity Awareness dan Digital Minimalism terhadap Cyber Fraud Preention pada Generasi Z

ABSTRAK

Meningkatnya adopsi perbankan digital di kalangan Generasi Z juga telah meningkatkan risiko kejahatan siber, khususnya penipuan siber. Studi ini bertujuan untuk menganalisis pengaruh Kesadaran Keamanan Siber dan Minimalisme Digital terhadap Pencegahan Penipuan Siber menggunakan pendekatan kuantitatif dalam kerangka Teori Motivasi Perlindungan (PMT). Data dikumpulkan melalui kuesioner daring yang didistribusikan melalui Google Form selama Januari–Mei 2025 kepada 77 responden Generasi Z di Indonesia yang menggunakan layanan perbankan digital. Responden dipilih menggunakan purposive sampling, dan data dianalisis dengan regresi linier berganda (SPSS 27). Temuan ini mengungkapkan bahwa kedua variabel independen secara positif dan signifikan memengaruhi pencegahan penipuan siber. Hasil ini menunjukkan bahwa peningkatan kesadaran keamanan digital dan penerapan gaya hidup digital minimalis dapat memperkuat upaya pencegahan kejahatan siber. Studi ini berkontribusi pada pengembangan strategi pencegahan berbasis perilaku dan memajukan bidang akuntansi forensik digital.

Kata Kunci: *Cybersecurity Awareness; Digital Minimalism; Cyber Fraud Prevention*

Artikel dapat diakses : https://ejournal1.unud.ac.id/index.php/akuntansi/index

INTRODUCTION

The rapid advancement of digital technologies has significantly transformed the way individuals manage their daily lives, particularly in financial activities. In Indonesia, digital banking has experienced exponential growth, with transaction volumes increasing by 40.1% as of November 2024 (Puspadini, 2025; F. Sulaiman, 2024). Generation Z (Gen Z), often described as digital natives, has emerged as the most active user group for both digital banking and e-wallet services, particularly in Indonesia and other rapidly digitizing economies. Their adoption of digital financial services is primarily driven by perceived usefulness, ease of use, trust, security, and social influence, with digital platforms becoming integral to their daily routines (Abu Daqar et al., 2020; Rosli et al., 2023). Studies highlight that Gen Z values convenience, speed, and seamless integration with their mobile-centric lifestyles, frequently using digital banking and e-wallets for online shopping, peer-to-peer transfers, and routine transactions (Sanny et al., 2023). In Indonesia, Gen Z represents the largest proportion of digital financial users (Nurdien & Galuh, 2023). However, concerns regarding security, financial literacy gaps, and impulsive spending remain important issues (Jeevitha, 2025; Lu'ay Natswa & ., 2024). Their tendency to prioritize speed and ease of use over caution increases their exposure to cyber fraud risks, making Gen Z a critical yet vulnerable demographic for this study.

Cyber fraud has become one of the most prevalent forms of cybercrime amid increasing digitalization. According to the Financial Services Authority (OJK), over 572,000 cyber fraud cases were reported in Indonesia in 2023, with total financial losses reaching IDR 2.5 trillion (Simanjuntak, 2024). Common methods such as phishing, skimming, and data breaches often target users who exhibit low levels of cybersecurity awareness (Bognár & Bottyán, 2024; Sikdar & Maiti, 2023). Furthermore, data from the National Cyber and Crypto Agency (BSSN, 2022) identified the financial sector as one of the most vulnerable to cyberattacks (Flores et al., 2014). Given Generation Z's high exposure to digital platforms, understanding the behavioral factors that influence their cyber fraud prevention efforts is both timely and essential (Chouhan & Mehta, 2022).

This study adopts the Protection Motivation Theory (PMT), developed by Rogers (1975), as a theoretical foundation to explain individual motivation to engage in protective behaviors. PMT posits that protective behavior is determined by two cognitive processes: threat appraisal, which involves evaluating the severity and personal vulnerability to a threat, and coping appraisal, which involves assessing the efficacy of the protective response and one's confidence in executing it (Rogers, 1975). Prior studies have validated the applicability of PMT in cybersecurity contexts. For example, Sulaiman et al. (2022) found that PMT components significantly predicted cybersecurity behavior among Malaysian civil servants. Similarly, Kiran et al. (2025) demonstrated PMT's robustness in explaining digital protection behavior across devices and platforms (Ifinedo, 2012; Ameen et al., 2023).

A central factor within the PMT framework is cybersecurity awareness, which refers to an individual's knowledge of cyber threats and their ability to recognize, avoid, and respond to risks such as phishing, malware, and data misuse (Zwilling et al., 2022). Cybersecurity-aware individuals are more likely to

implement safe digital practices, including secure password management, vigilance against suspicious links, and adherence to institutional security guidelines (Vafaei-Zadeh et al., 2024; Bognár & Bottyán, 2024; Renaud et al., 2014). At the same time, an emerging but underexplored behavioral factor is digital minimalism—a lifestyle approach advocating for intentional and restrained use of digital technology to reduce distractions, dependence, and digital risk exposure (Nurhakim & Asbari, 2023). Individuals who practice digital minimalism are typically more selective in their digital engagement, thereby reducing their attack surface in online environments (Li & Siponen, 2024). Studies have shown that digital self-control is positively associated with cybersecurity behavior (Booc et al., 2024).

Despite growing interest in both cybersecurity awareness and digital minimalism, empirical research integrating these two constructs within a unified behavioral model remains limited—especially in the context of Generation Z. Much of the existing research on cybersecurity has focused on organizational contexts. For instance, Tariq et al. (2024) examined digital fraud prevention from the perspective of IT professionals, while Ali and Mohd Zaharon (2024) investigated user vulnerabilities to phishing without considering lifestyle-based behavioral strategies (Lowry et al., 2015). Meanwhile, research on digital minimalism has largely been sector-specific (e.g., healthcare, education) and has not addressed its implications for cyber fraud prevention (Akyon et al., 2024). Although PMT has been widely applied in cybersecurity literature, few studies have leveraged it to jointly examine how cybersecurity awareness and digital minimalism influence fraud prevention behavior in young, high-exposure populations (Vance et al., 2014).

Addressing this research gap, the present study proposes an integrated PMT-based model to empirically assess the role of cybersecurity awareness and digital minimalism in shaping fraud prevention behavior among Generation Z digital banking users. By focusing on this digitally immersed and increasingly targeted demographic, this study contributes to a more comprehensive understanding of behavioral cybersecurity and offers practical insights into personal-level fraud mitigation strategies in digital financial ecosystems

According to Protection Motivation Theory (PMT), the greater an individual's awareness of cyber threats (threat appraisal), the more likely they are to engage in protective behavior. Cybersecurity awareness shapes risk perception and promotes preventive responses to digital threats. Such actions include implementing two-factor authentication (2FA), avoiding phishing links, and verifying the authenticity of information sources before financial transactions. (Bognár & Bottyán, 2024; Kuzior et al., 2024). Tariq et al. (2024) Cybersecurity awareness significantly contributes to fraud prevention within Jordan's digital banking sector. N. S. Sulaiman et al. (2022) Further confirmed that threat and coping appraisals, supported by strong cybersecurity awareness, enhance individuals' preventive actions in addressing digital threats. Based on the theoretical framework and prior empirical evidence, this study proposes the following hypothesis:

H_1: Cybersecurity Awareness has a positive effect on Cyber Fraud Prevention.

Digital minimalism is a lifestyle approach that emphasizes the conscious, limited, and purposeful use of digital technology to improve the quality of life and reduce risks (Crasta, 2024; Drew & Farrell, 2018). Within the framework of Protection Motivation Theory (PMT), digital minimalism can be interpreted as a coping appraisal mechanism because intentional limitation of online exposure reduces opportunities for fraudulent encounters (response efficacy) and increases users' confidence in managing risks (self-efficacy). Empirical studies Khansa et al. (2017) found that selective digital engagement lowers vulnerability to data misuse; Akyon et al. (2024) showed that minimalism strengthens information security; Kumar & Nath (2024) confirmed that individuals with higher self-control are less susceptible to online scams; and Booc et al. (2024) demonstrated that digital self-regulation correlates with safer cybersecurity practices. Although no direct evidence has connected digital minimalism with cyber fraud prevention, these findings imply that a minimalist digital lifestyle indirectly enhances protection by reducing exposure to risky environments and fostering more mindful technology use. Therefore, the second hypothesis is proposed:

H_2: Digital Minimalism has a positive effect on Cyber Fraud Prevention.

The proposed research model integrates both cybersecurity awareness and digital minimalism as predictors of cyber fraud prevention behavior within the framework of Protection Motivation Theory, as shown in the following figure:

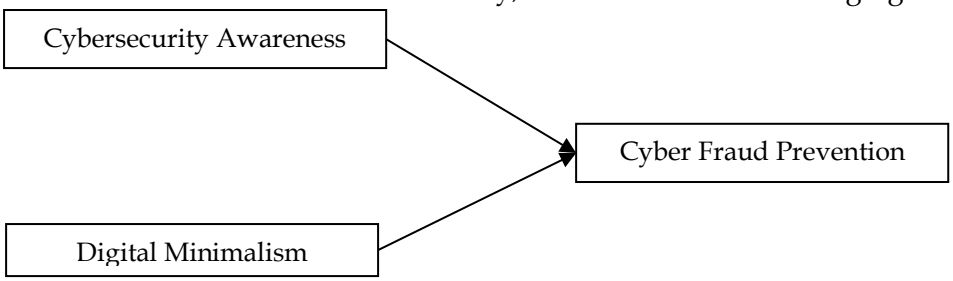

Figure 1. Research Model

Source: Research Data, 2025

Cyber fraud remains one of the most pressing challenges in the digital era (Pramesti & Kresnandra, 2024). Cyber fraud remains one of the most pressing challenges in the digital era (Pramesti & Kresnandra, 2024). This study contributes to forensic accounting by offering a holistic perspective on cyber fraud prevention, emphasising individual behavioural factors in managing digital risk. The novelty of this research lies in three aspects. First, it integrates cybersecurity awareness and digital minimalism into a single Protection Motivation Theory (PMT) framework, whereas prior studies typically emphasised either awareness or technical safeguards in isolation. Second, it introduces digital minimalism as a new construct in the cyber fraud prevention literature, filling a gap where no direct empirical evidence has previously linked this lifestyle approach to fraud prevention. Third, it focuses on Generation Z in Indonesia, the largest group of digital financial users and the most vulnerable to cyber fraud, thereby providing a contextual contribution to the development of cybersecurity literacy strategies in emerging economies.

In addition to its novelty, this study offers several advantages over previous research. Unlike earlier studies that focused on organisational or system-level defences, this study highlights individual-level behavioural strategies, demonstrating that fraud prevention is not only a matter of technology but also of user psychology and lifestyle. It also provides empirical evidence from a developing country context, which has often been underrepresented in cybersecurity research dominated by studies in advanced economies. Finally, this research advances the application of PMT beyond traditional domains by showing how its constructs can explain digital-native behaviour in the financial sector. By addressing these gaps and leveraging these advantages, this study extends the theoretical application of PMT. It provides practical insights for designing digital security education and policies tailored to the unique characteristics of digital-native populations.

RESEARCH METHOD

This study employs a quantitative approach within a positivist paradigm, with hypothesis testing grounded in the Protection Motivation Theory (PMT). The primary objective is to examine the effect of cybersecurity awareness and digital minimalism on cyber fraud prevention among Generation Z. This approach was chosen as it enables objective measurement of variables and statistical analysis of their relationships.

The population of this research is Generation Z in Indonesia, defined as individuals born between 1997 and 2012 who actively use digital banking services. Given the large size of this population, probability sampling was not feasible. Therefore, a purposive sampling technique was employed with the following inclusion criteria aged between 18 and 27 years, actively using the internet and digital devices, and having made online transactions.

A total of 77 respondents were obtained, which satisfies the minimum sample size requirement based on Cohen's (1988) guidelines for multiple linear regression with two predictors: a minimum of 68 participants at a 5% significance level, 0.80 statistical power, and a moderate effect size ($f^2 = 0.15$).

The research instrument was an online questionnaire developed by adapting and modifying items from prior studies. Indicators for cybersecurity awareness were adapted from Zwilling et al. (2022) and Vafaei-Zadeh et al. (2024); indicators for digital minimalism were based on Drew & Farrell (2018) and Kumar & Nath (2024); and indicators for cyber fraud prevention were adapted from Paul et al. (2023) and Crasta (2024). All items were measured using a 5-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree).

Data were collected through a Google Form questionnaire distributed via social media platforms (WhatsApp, Instagram) using a snowball sampling strategy. This method was considered most effective to reach Generation Z respondents. The data collection was conducted during January–May 2025.

Instrument validity was tested using item-total correlation (r-count), and all items showed r-values above the critical value of 0.2213 ($N = 77$, $\alpha = 0.05$), indicating that all items were valid. Reliability was tested using Cronbach's Alpha, resulting in coefficients of 0.915 for cyber fraud prevention, 0.837 for cybersecurity awareness, and 0.786 for digital minimalism, indicating that all instruments were

highly reliable. These reliability coefficients exceed the minimum threshold of 0.70, as recommended for social science research.

Each construct in this study was operationalized as follows Cybersecurity Awareness (X1): Knowledge and understanding of cyber threats and protective practices (7 indicators). Digital Minimalism (X2): Conscious, limited, and purposeful use of digital technology to reduce risks (7 indicators). Cyber Fraud Prevention (Y): Individual behaviors and actions to avoid fraudulent activities in digital financial transactions (7 indicators).

Data were analyzed using SPSS version 27. Multiple linear regression analysis was applied to assess the influence of cybersecurity awareness and digital minimalism on cyber fraud prevention. The coefficient of determination (adjusted R^2) was used to determine the explanatory power of the independent variables, while t-tests and F-tests were employed to examine the significance of individual and joint effects. All analytical steps were conducted systematically to ensure accurate, valid, and scientifically reliable findings.

RESULT AND DISCUSSION

This study investigates the influence of Cybersecurity Awareness and Digital Minimalism on Cyber Fraud Prevention among Generation Z digital banking users, utilizing the Protection Motivation Theory (PMT) as the underlying framework. Statistical analysis was conducted in several stages using SPSS software version 27.

Table 1. Validity Test Results

Variabel	Item	r hitung	R Tabel (N=77)	Ket
Cyber Fraud Prevention	Y.1	0,575		
	Y.2	0,833		
	Y.3	0,783		
	Y.4	0,734		
	Y.5	0,77		
	Y.6	0,747		
	Y.7	0,582		
Cybersecurity Awareness	X1.1	0,593		
	X1.2	0,751		
	X1.3	0,713		
	X1.4	0,741	0,2213	Valid
	X1.5	0,601		
	X1.6	0,556		
	X1.7	0,747		
Digital Minimalism	X2.1	0,844		
	X2.2	0,865		
	X2.3	0,828		
	X2.4	0,934		
	X2.5	0,817		
	X2.6	0,716		
	X2.7	0,727		

Source: Research Data, 2025

The item codes Y1–Y7, X1.1–X1.7, and X2.1–X2.7 presented in Table 1 are not arbitrary numbers but represent proxy indicators of each research variable, measured through specific questionnaire statements rated by respondents.

Cyber Fraud Prevention (Y1–Y7): These items capture preventive actions undertaken by respondents to secure their digital banking activities. They include behaviors such as using strong and unique passwords (Y1), activating multi-factor authentication (Y2), verifying transaction details before confirming (Y3), avoiding suspicious links or emails (Y4), regularly monitoring account activity (Y5), securing devices with updated software (Y6), and reporting unusual or fraudulent transactions to banks (Y7). Each of these items functions as a proxy to operationalize the construct of cyber fraud prevention.

Cybersecurity Awareness (X1.1–X1.7): These indicators measure the extent of respondents' awareness and vigilance regarding online threats. They include knowledge of phishing techniques (X1.1), understanding the risks of malware (X1.2), recognizing suspicious online behaviors (X1.3), updating and applying recommended cybersecurity practices (X1.4), awareness of institutional policies and guidelines (X1.5), ability to distinguish secure from insecure websites (X1.6), and adopting safe browsing or emailing habits (X1.7). Each item serves as a proxy reflecting cybersecurity awareness in practical terms.

Digital Minimalism (X2.1–X2.7): These items represent respondents' lifestyle-related digital behaviors, aligned with the concept of digital minimalism. Indicators include limiting installation of non-essential apps (X2.1), reducing the use of social media platforms (X2.2), allocating time selectively for digital engagement (X2.3), prioritizing purposeful technology use over impulsive consumption (X2.4), consciously avoiding unnecessary digital distractions (X2.5), curating digital footprints to minimize risks (X2.6), and maintaining self-discipline in online activity (X2.7). Each item is a proxy indicator that operationalizes the abstract construct of digital minimalism into observable behaviors.

Table 1 presents the results of the item-total correlation analysis for the three main variables. Based on the validity test results involving 77 respondents (N = 77), the critical value of the r table is 0.2213. All items under the Cyber Fraud Prevention variable obtained r-values ranging from 0.575 to 0.833, exceeding the minimum threshold. This indicates that each item has a moderate to strong correlation with its respective total construct score, validating their use in this study. Likewise, all items in the Cybersecurity Awareness variable show r-values between 0.556 and 0.751, also above the r table, confirming their validity. The Digital Minimalism variable showed the highest item-total correlations, ranging from 0.716 to 0.934, reflecting firm internal consistency. Overall, it can be concluded that all items across the three variables meet the validity requirements, making them appropriate for further analysis.

Table 2 Descriptive Statistics

Variable	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity Awareness (X1)	77	12	35	29.79	4.584
Digital Minimalism (X2)	77	11	35	28.40	4.423
Cyber Fraud Prevention (Y)	77	12	35	31.87	4.351

Source: Research Data, 2025

Table X shows the descriptive statistics for the three research variables. Cybersecurity Awareness (X1) recorded a relatively high mean score (M = 29.79), indicating that most Generation Z respondents have a strong understanding of cyber threats and adopt basic security practices. This finding is consistent with Zwilling et al. (2022) and Vafaei-Zadeh et al. (2024), who emphasize that cybersecurity awareness is a critical factor influencing protective digital behavior. Cyber Fraud Prevention (Y) achieved the highest average score (M = 31.87), suggesting that many respondents actively implement preventive measures such as strong password usage, multi-factor authentication, and transaction verification. This supports the arguments of Pillay et al. (2023) and Sulaiman et al. (2022), who found that heightened awareness strongly predicts fraud-prevention practices. In contrast, Digital Minimalism (X2) obtained a lower mean score (M = 28.40), reflecting that while some respondents consciously manage and limit their digital engagement, this practice is less consistent compared to awareness-driven behaviors. This aligns with Drew & Farrell (2018) and Kumar & Nath (2024), who argue that digital minimalism, while effective in reducing exposure to online risks, is less commonly adopted because of lifestyle habits and high social media dependence among younger generations. These results imply that although awareness and preventive actions are already relatively strong among Generation Z, digital minimalism remains an underdeveloped but potentially valuable strategy to enhance cyber fraud prevention.

Table 3. Reliability Test Results

No	Variable	Cronbach Alpha Value	Description
1	Cyber Fraud Prevention	0,915	Reliable
2	Cybersecurity Awareness	0,837	
3	Digital Minimalism	0,786	

Source: Research Data, 2025

All variables demonstrated high reliability levels based on Cronbach's Alpha coefficients. The Cyber Fraud Prevention variable recorded an alpha of 0.915, exceeding the 0.90 threshold, and was thus classified as highly reliable. Cybersecurity Awareness scored 0.837, indicating good internal consistency and meeting the general reliability standard of 0.70. Digital Minimalism achieved a Cronbach's Alpha value of 0.786, which signifies adequate reliability. These results suggest that all three instruments consistently measure their respective constructs and are therefore suitable for further statistical analysis (Nunnally & Bernstein, 1994).

Table 4. Classical Assumption Test Results

Variabel	Normalitas (Sig. K-S)	Tolerance	VIF	Glejser (Sig.)
Cybersecurity Awareness	0,200	0,530	1,888	1,000
Digital Minimalism	0,200	0,530	1,888	1,000

Source: Research Data, 2025

The classical assumption tests confirmed that the regression model fulfills all necessary statistical assumptions. First, the Kolmogorov-Smirnov test shows significance values of 0.200 for both independent variables, above the 0.05

threshold, indicating that the data are normally distributed. Second, multicollinearity tests reveal Tolerance values of 0.530 and VIF values of 1.888 for both variables, suggesting no multicollinearity concerns (Tolerance > 0.10; VIF < 10). Third, the Glejser test for heteroscedasticity reports significance values of 1.000 for both variables, far above the 0.05 cut-off, confirming homoscedasticity. The regression model is considered statistically appropriate and valid for hypothesis testing, with all assumptions met.

Table 5. Regression Model Summary and Coefficients

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	6.413	1.895		3.384	0.01
Cybersecurity Awareness	0.653	0.080	0.688	8.171	0.00
Digital Minimalism	0.211	0.83	0.215	2.552	0.13
Adjusted R Square	0,715				
Sig. F	0.000				

Source: Research Data, 2025

Table 5 presents the multiple linear regression results, showing that Cybersecurity Awareness has a significant effect (B = 0.653; β = 0.688). This implies that the higher Generation Z's awareness of cybersecurity, the more effective they are in preventing cyber fraud when using digital banking services. This finding is consistent with Alqarni et al. (2023), who confirmed that a high level of cyber awareness reduces vulnerability to digital crime.

Digital Minimalism also shows a positive and significant effect on fraud prevention, although its influence is smaller than Cybersecurity Awareness (β = 0.215). This indicates that consciously limiting digital usage helps Generation Z reduce their exposure to cyberattacks. From the perspective of Protection Motivation Theory (PMT), digital minimalism can be interpreted as a coping appraisal strategy that lowers the frequency and intensity of risky digital interactions, thereby enhancing both response efficacy and self-efficacy (Newport, 2019). Supporting studies such as Maier et al. (2015) and Hadlington & Parsons (2017) also highlight that deliberate digital disengagement—such as limiting social media activity or avoiding unnecessary applications—reduces opportunities for fraudsters to exploit user vulnerabilities.

The findings demonstrate that both threat appraisal and coping appraisal, as proposed in PMT (Rogers, 1975), are strongly reflected in the behavior of Generation Z. Awareness of online risks such as phishing, scams, and identity theft elevates threat appraisal, motivating protective actions like complex password usage, multi-factor authentication, and cautious evaluation of digital communications (Liang & Xue, 2010; Ifinedo, 2012; Tsai et al., 2022). At the same time, coping appraisal is strengthened by digital minimalism, which reduces

exposure to high-risk environments and instills a greater sense of control, thereby reinforcing motivation to adopt protective actions (Warkentin et al., 2016).

The adjusted R^2 value of 71.5% further demonstrates the strong explanatory power of the model, confirming that behavioral constructs meaningfully account for variations in fraud prevention. These results emphasize that while financial institutions provide technical safeguards, individual behaviors and psychological readiness remain critical in mitigating cyber threats. This observation aligns with Bada et al. (2019) and Crossler & Bélanger (2014), who advocate for a behavioral approach to cybersecurity alongside technical solutions.

Beyond supporting existing evidence, this study contributes several new insights. First, it introduces digital minimalism as a novel construct in the cyber fraud prevention literature—an area where empirical evidence has been limited. Second, it offers an integrated PMT-based framework that combines threat appraisal (cybersecurity awareness) with coping appraisal (digital minimalism), thus providing a more holistic behavioral explanation than prior studies, which typically focused on awareness or technical safeguards alone (Ifinedo, 2012; Sulaiman et al., 2022; Tariq et al., 2024). Third, by examining Generation Z in Indonesia, this study contributes contextual knowledge from a developing economy with rapid digital banking adoption but varied levels of cyber literacy. This demographic focus enriches global discourse that has been dominated by Western or organizational contexts.

To sum up, this study confirms the relevance of PMT in explaining digital safety behavior among Generation Z. More importantly, it expands the literature by integrating digital minimalism into fraud prevention research, providing both theoretical enrichment and practical implications for designing user-centered fraud prevention strategies tailored to digital-native populations.

CONCLUSION

This study provides empirical evidence that Cybersecurity Awareness and Digital Minimalism significantly and positively influence Cyber Fraud Prevention behavior among Generation Z users of digital banking services. The findings suggest that individuals with heightened awareness of cyber risks and those who adopt more deliberate, minimalist digital behaviors are more capable of avoiding fraudulent activities online. These behavioral tendencies serve as critical defenses against cybercrime in an increasingly digital financial ecosystem. This study offers a novel contribution to the existing cybersecurity and fraud prevention literature by integrating Protection Motivation Theory (PMT) into the context of Generation Z's digital banking behavior—an area that remains underexplored. While prior research has largely focused on institutional or system-level cybersecurity mechanisms, this study shifts the lens to individual behavioral predictors, namely cybersecurity awareness and digital minimalism, as proactive strategies to mitigate fraud risk. Moreover, the inclusion of digital minimalism as a predictive construct is particularly innovative, as it introduces a psychological self-regulation framework that has not been extensively linked to cybersecurity behavior in prior PMT-based studies.

The results further reinforce the relevance of Protection Motivation Theory (PMT) by illustrating that both threat appraisal—in the form of recognizing the

severity and susceptibility of cyber threats—and coping appraisal—as demonstrated by perceived self-efficacy and response effectiveness—are instrumental in motivating protective actions. This supports the theoretical proposition that individuals' psychological evaluations play a vital role in shaping cybersecurity behavior, especially among digital-native populations such as Generation Z. From a practical perspective, the integration of behavioral and psychological constructs into digital fraud prevention strategies offers a valuable extension to conventional system- and infrastructure-focused approaches. Encouraging digital literacy, security awareness, and conscious digital habits may significantly enhance fraud mitigation efforts, particularly in environments where technical safeguards alone are insufficient.

Despite its contributions, this study has several limitations. First, the research relied on a relatively small sample of 77 respondents. Although this number satisfies the minimum sample size requirement for multiple regression analysis (Cohen, 1988) It may not adequately represent the broader Generation Z population of digital banking users in Indonesia, which, according to BSSN (2022), reaches millions. This gap limits the external validity and generalizability of the findings. Second, the use of a structured, closed-ended questionnaire may restrict respondents from expressing deeper motivations or contextual nuances underlying their cybersecurity behavior. Moreover, self-reported data are prone to social desirability bias, where respondents may provide favorable rather than fully accurate answers (Podsakoff et al., 2003). Third, the cross-sectional design prevents the observation of behavioral dynamics over time, thus limiting the ability to draw causal inferences.

Future research should consider expanding the sample size and scope to include more diverse demographics, such as different age groups, occupational categories, and geographic regions, to enhance representativeness. In addition, longitudinal or mixed-method designs could provide richer insights into the evolving nature of protective behaviors. Integrating complementary theoretical frameworks—such as the Theory of Planned Behavior (TPB) or Technology Threat Avoidance Theory (TTAT)—may also enrich the explanatory power of future models and offer a more holistic perspective on cyber fraud prevention.

REFERENCES

Abu Daqar, M. A. M., Arqawi, S., & Karsh, S. A. (2020). Fintech in the eyes of Millennials and Generation Z (the financial behavior and Fintech perception). *Banks and Bank Systems*, *15*(3), 20–28. https://doi.org/10.21511/bbs.15(3).2020.03

Akyon, S. H., Akyon, F. C., Onur, G., & Arman, I. H. (2024). Digital Minimalism: Using Technology for Efficient Healthcare. Eurasian Journal of Family Medicine, 13(4), 147–154. https://doi.org/10.33880/ejfm.2024130401

Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A Cyber Fraud: The Types, Implications and Governance. International Journal of Educational Reform, 33(1), 101–121. https://doi.org/10.1177/10567879221082966

Ameen, N., Cheah, J. H., Sharma, A., & Rana, N. P. (2023). Cybersecurity behaviour of consumers in the era of digital banking: A protection motivation theory approach. Internet Research, 33(6), 1630–1653.

https://doi.org/10.1108/INTR-03-2022-0147
Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672. https://arxiv.org/abs/1901.02672
Bognár, L., & Bottyán, L. (2024). Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students. Education Sciences, 14(6). https://doi.org/10.3390/educsci14060588
Booc, A. C., Moisescu, O. I., & Gică, O.-A. (2024). Digital minimalism and online privacy behaviour: Evidence from young digital users. Technological Forecasting and Social Change, 197, 122886. https://doi.org/10.1016/j.techfore.2023.122886
Booc, N. B. B., Budiongan, K., & Carballo, R. (2024). Cybersecurity Awareness and Cybersecurity Behavior of High School Students in Davao City: A Mediation Role of Perceived Behavioral Control. European Journal of Applied Science, Engineering and Technology, 2(3), 4–9. https://doi.org/10.59324/ejaset.2024.2(3).01
BSSN. (2022). BSSN: Industri Keuangan Rawan Serangan Siber, Lakukan Update Aplikasi Digital Secara Berkala. Badan Siber Dan Sandi Negara. https://www.bssn.go.id/bssn-industri-keuangan-rawan-serangan-siber-lakukan-update-aplikasi-digital-secara-berkala/
Chouhan, R., & Mehta, D. (2022). Cyber security awareness and practices among young internet users. Information and Computer Security, 30(1), 92–108. https://doi.org/10.1108/ICS-06-2021-0071
Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences (2nd Editio). https://doi.org/https://doi.org/10.4324/9780203771587
Crasta, S. (2024). Enhancing Consumer Vigilance and Mitigating Tactics Against Internet Shopping Fraud. Al-Shodhana, 12(2), 86–93. https://doi.org/10.70644/as.v12.i2.7
Crossler, R. E., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. Information Systems Journal, 24(1), 61–83. https://www.jstor.org/stable/43825789
Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs. Police Practice and Research, 19(6), 537–549. https://doi.org/10.1080/15614263.2018.1507890
Flores, W. R., Holm, H., & Nohlberg, M. (2014). Investigating personal determinants of phishing and the effect of national culture. Computers & Security, 46, 28–47. https://www.sciencedirect.com/science/article/pii/S0167404814000296
Hadlington, L., & Parsons, K. (2017). Qualitative perceptions of employee security behaviour and challenges in organizational settings: A thematic analysis. Journal of Cybersecurity and Digital Forensics, 2(1), 1–12. https://onlinelibrary.wiley.com/doi/full/10.1002/cbdv.201700032
Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection

motivation theory. Computers & Security, 31(1), 83–95. https://www.sciencedirect.com/science/article/pii/S0268401218302093

Jeevitha, P. (2025). Analysis of Digital Banking Adoption among Gen Z Students. Interantional Journal of Scientific Research in Engineering and Management, 09(03), 1–9. https://doi.org/10.55041/ijsrem42972

Khansa, L., Kuem, J., Siponen, M., & Kim, S. S. (2017). To Cyberloaf or Not to Cyberloaf: The Impact of the Announcement of Formal Organizational Controls. Journal of Management Information Systems, 34(1), 141–176. https://doi.org/10.1080/07421222.2017.1297173

Kiran, U., Khan, N. F., Murtaza, H., Farooq, A., & Pirkkalainen, H. (2025). Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. Computers and Security, 149(October 2024), 104204. https://doi.org/10.1016/j.cose.2024.104204

Kumar, S., & Nath, L. (2024). "Digital Minimalism" - a Study To Find Out Ways To Make the Best Use of Digital Technologies and Minimise Its Ill-Effects. ShodhKosh: Journal of Visual and Performing Arts, 5(1), 279–290. https://doi.org/10.29121/shodhkosh.v5.i1.2024.640

Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies, 17(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12

Li, Y., & Siponen, M. (2024). The role of digital well-being and minimalism in predicting cybersecurity behavior. Information & Management, 61(1), 103755. https://doi.org/10.1016/j.im.2023.103755

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394–413. https://www.sciencedirect.com/science/article/pii/S0167404816300190

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organizational information security policies: An empirical study of the influence of counterfactual thinking and organizational trust. Information Systems Journal, 25(3), 193–273. https://doi.org/10.1111/isj.12050

Lu'ay Natswa, S., & . S. (2024). Gen Z's Cashless Behavior: How QRIS Moderating Digital Financial Literacy and Spending Behavior Affects on E-Wallet Utilization? KnE Social Sciences, 2024(Idc), 306–324. https://doi.org/10.18502/kss.v9i4.15078

Maier, C., Laumer, S., Eckhardt, A., & Weitzel, T. (2015). Giving too much social support: Social overload on social networking sites. European Journal of Information Systems, 24(5), 447–464. https://www.sciencedirect.com/science/article/pii/S0040162521000329

Newport, C. (2019). Digital minimalism: Choosing a focused life in a noisy world. Penguin Publishing Group.

Nurdien, F. G., & Galuh, A. K. (2023). Pengaruh Literasi Keuangan dan Literasi Digital terhadap Preferensi Menggunakan Qris Bsi Mobile (Studi Kasus Gen Z Di Kota Malang). Islamic Economics and Finance in Focus, 2(4), 588–601. https://doi.org/10.21776/ieff.2023.02.04.02

Nurhakim, M. I., & Asbari, M. (2023). Digital Minimalism: Filosofi Efisiensi

Penggunaan Teknologi Digital. Literaksi: Jurnal Manajemen Pendidikan, 1(2), 49–54. https://doi.org/10.30596/jimb.v22i1.4888

Paul, E. O., Callistus, O., Somtobe, O., Esther, T., Somto, K.-A., Clement, O., & Ejimofor, I. (2023). Cybersecurity Strategies for Safeguarding Customer's Data and Preventing Financial Fraud in the United States Financial Sectors. International Journal on Soft Computing, 14(3), 01–16. https://doi.org/10.5121/ijsc.2023.14301

Pillay, P., Ntuli, P. N., & Ehiane, S. O. (2023). Exploring the Prevalence of Cybercrime in the Banking Industry in KwaZulu-Natal, South Africa. International Journal of Membrane Science and Technology, 10(1), 1763–1775. https://doi.org/10.15379/ijmst.v10i1.3283

Podsakoff, P. M., MacKenzie, S. B., Lee, J., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. The Journal of Applied Psychology, 88(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Pramesti, I. G. A. I. S., & Kresnandra, A. A. N. A. (2024). Pengaruh Persepsi Kemudahan Penggunaan, Kualitas Layanan, dan Risiko Keamanan Informasi terhadap Penggunaan Dompet Digital. E-Jurnal Ekonomi Dan Bisnis Universitas Udayana, 13(7), 1443–1453. https://journalpedia.com/1/index.php/dkms/article/view/1775%0Ahttps://journalpedia.com/1/index.php/dkms/article/download/1775/1809

Puspadini, M. (2025). Transaksi Bank Digital Tumbuh 40,1%, Didominasi Gen Z & Milenial. CNBC Indonesia. https://www.cnbcindonesia.com/market/20250314201903-17-618812/transaksi-bank-digital-tumbuh-401-didominasi-gen-z-milenial

Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014). Why doesn't Jane protect her privacy? The influence of usability, risk perception, and social norms on security and privacy behaviour. Information & Computer Security, 22(1), 30–49. https://doi.org/10.1108/ICS-03-2013-0010

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. The Journal of Psychology, 91(91–1144). https://doi.org/https://doi.org/10.1080/00223980.1975.9915803

Rosli, M. S., Saleh, N. S., Md. Ali, A., & Abu Bakar, S. (2023). Factors Determining the Acceptance of E-Wallet among Gen Z from the Lens of the Extended Technology Acceptance Model. Sustainability (Switzerland), 15(7), 1–23. https://doi.org/10.3390/su15075752

Sanny, L., Chandra, G. R., Chelles, K., & Santoso, L. A. (2023). the Impulse Buying of Gen Z When Using E-Wallet in Indonesia. Journal of Applied Engineering and Technological Science, 5(1), 88–100. https://doi.org/10.37385/jaets.v5i1.2600

Sikdar, S., & Maiti, M. (2023). Phishing vulnerability and user behavior: The role of cyber hygiene and social engineering awareness. Journal of Enterprise Information Management, 36(2), 303–323. https://doi.org/10.1108/JEIM-06-2022-0274

Simanjuntak, M. H. (2024). OJK: Kerugian Konsumen Akibat Scam dan Fraud Mencapai Rp2,5 Triliun. Antara. https://www.antaranews.com/berita/4523695/ojk-kerugian-konsumen-

akibat-scam-dan-fraud-mencapai-rp25-triliun

Sulaiman, F. (2024). Survei Populix Ungkap Gen Z Dominasi Pengguna Bank Digital di Indonesia. Warta Ekonomi. https://wartaekonomi.co.id/read538862/survei-populix-ungkap-gen-z-dominasi-pengguna-bank-digital-di-indonesia

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. Information (Switzerland), 13(9). https://doi.org/10.3390/info13090413

Tariq, E., Akour, I., Al-Shanableh, N., Alquqa, E. K., Alzboun, N., Al-Hawary, S. I. S., & Alshurideh, M. T. (2024). How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. International Journal of Data and Network Science, 8(1), 69–76. https://doi.org/10.5267/j.ijdns.2023.10.016

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2022). Understanding online safety behaviors: A protection motivation theory perspective. Computers & Security, 114, 102582. https://www.sciencedirect.com/science/article/pii/S0167404822004412

Vafaei-Zadeh, A., Nikbin, D., Teoh, K. Y., & Hanifah, H. (2024). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. International Journal of Bank Marketing, 43(3), 476–505. https://doi.org/10.1108/IJBM-03-2024-0138

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). Journal of the Association for Information Systems, 15(10), 679–722. https://www.jstor.org/stable/43825953

Warkentin, M., Johnston, A. C., & Shropshire, J. (2016). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. European Journal of Information Systems, 25(4), 344–361. https://onlinelibrary.wiley.com/doi/abs/10.1111/isj.12050

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269