Journal of
Risk and Financial Management

MDPI

Article

Predictors of Digital Fraud: Evidence from Thailand

Tanpat Kraiwanit [1], Pongsakorn Limna [1,*], Rattaphong Sonsuphap [2,*] and Veraphong Chutipat [3]

[1] International College, Pathumthani University, Mueang, Pathum Thani 12000, Thailand; tanpat@ptu.ac.th
[2] Faculty of Economics, Rangsit University, Mueang, Pathum Thani 12000, Thailand
[3] College of Leadership and Social Innovation, Rangsit University, Mueang, Pathum Thani 12000, Thailand; veraphong.c@rsu.ac.th
* Correspondence: pongsakorn.l@ptu.ac.th (P.L.); rattaphong.s@rsu.ac.th (R.S.)

Abstract

This study examined the complex interplay of demographic characteristics, behavioral patterns, and technological factors that contribute to digital fraud victimization within the context of a developing economy, focusing specifically on Thailand. Utilizing data collected from 1200 respondents and applying binary logistic regression analysis, the research identified key predictors of fraud exposure, including age, income, student status, use of portable devices, and social media engagement. A paradoxical finding emerged: stronger perceived digital security was associated with higher fraud risk, indicating that overconfidence in platform safeguards may unintentionally increase vulnerability. Interestingly, users' perceptions of digital security—such as confidence in identity verification and password protocols—were positively associated with fraud victimization, indicating potential cognitive biases and overconfidence in digital environments. The findings revealed a high prevalence of fraud experiences among participants, highlighting the gap between perceived and actual digital safety. These results emphasized the urgent need for user-centered fraud prevention measures, enhanced digital literacy, and targeted public awareness campaigns. The study contributes to the broader understanding of cybersecurity challenges in emerging markets and offers policy-relevant insights for strengthening digital financial resilience.

Keywords: digital fraud; victimization; cybersecurity; behavioral risk; demographic characteristics; behavioral patterns; technological factors

JEL Classification: D18; D91; O33; K42

check for updates

Academic Editor: Christopher Gan

Received: 25 October 2025
Revised: 21 November 2025
Accepted: 22 November 2025
Published: 26 November 2025

Citation: Kraiwanit, T., Limna, P., Sonsuphap, R., & Chutipat, V. (2025). Predictors of Digital Fraud: Evidence from Thailand. *Journal of Risk and Financial Management*, *18*(12), 671. https://doi.org/10.3390/jrfm18120671

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The rapid digitalization of financial services has fundamentally transformed the manner in which individuals and businesses engage with monetary transactions, delivering unprecedented convenience, efficiency, and accessibility. Globally, the widespread adoption of mobile banking, e-wallets, and online payment platforms has significantly advanced financial inclusion, particularly in developing economies where conventional banking infrastructure remains underdeveloped or geographically inaccessible. These digital financial innovations reduce barriers to entry, lower transaction costs, and enable broader participation in formal financial systems, thereby contributing to economic development and social inclusion (Kandpal et al., 2025; Ly & Ly, 2024; Nwoke, 2024). Thailand exemplifies this trend, having undergone a remarkable digital transformation within its financial sector. This progress has been catalyzed by strategic government policies such as the National

e-Payment Master Plan and the implementation of the PromptPay system, which enable real-time interbank transfers and facilitate seamless digital payments across diverse population segments. The rapid proliferation of smartphones and improved internet penetration has further accelerated the uptake of digital financial services. Concurrently, the emergence of fintech enterprises and collaborations between traditional financial institutions and technology firms have diversified the financial ecosystem, expanding access to innovative products ranging from microfinance to automated investment platforms (Teerapunyachai & Bawornkitchaikul, 2024; Ungratwar et al., 2025; Warokka et al., 2025).

Despite these advancements, the proliferation of digital financial services has been accompanied by an alarming increase in digital fraud (Yoganandham & Govindaraj, 2024). Digital fraud encompasses a wide range of illicit activities conducted via digital channels, including phishing, identity theft, fraudulent investment schemes, unauthorized transactions, and social engineering attacks. These frauds exploit inherent vulnerabilities in digital ecosystems, leveraging deceptive techniques that manipulate users' trust and behavioral patterns to gain unauthorized access to financial assets. The rapid pace of digital adoption has often outstripped the development of comprehensive cybersecurity infrastructure and user education, particularly in contexts where regulatory frameworks are still evolving and enforcement mechanisms are nascent. This gap creates an environment conducive to cybercriminal activities, which are further complicated by the increasing sophistication of fraud techniques, including the use of artificial intelligence (AI) for deepfake communications and automated scam campaigns. This dynamic has resulted in rising incidents of digital financial fraud, with significant implications for consumer confidence, financial stability, and the overall sustainability of digital financial inclusion efforts (Alex-Omiogbemi et al., 2024; Chayanon et al., 2025; Odufisan et al., 2025; Oroșanu & Alexandru, 2024; D. Sharma et al., 2025; Udeh et al., 2024).

In the context of Thailand, recent reports and case studies have highlighted an alarming rise in digital fraud cases, affecting not only individual consumers but also contributing to broader economic losses (Dangpisan, 2025; The Nation, 2025). However, empirical investigations into the root causes of digital fraud victimization in Thailand—and similar developing economies—remain scarce. While international research (e.g., Choi et al., 2016; Marttila et al., 2021; Padyab et al., 2024) has identified key demographic and psychological traits associated with cybercrime exposure, these insights may not fully translate to the Southeast Asian context, where cultural, technological, and socioeconomic conditions differ significantly. There is a pressing need for localized, data-driven research that captures the lived experiences, behaviors, and perceptions of users in digitally maturing environments like Thailand. Specifically, few studies have systematically analyzed how individuals' demographic profiles (e.g., age, income, education), digital habits (e.g., device usage, time online, preferred social media), and perceived digital security features (e.g., password protocols, identity verification, alerts) intersect to influence fraud risk in developing nations. This study seeks to fill this critical research gap by conducting a comprehensive, empirical investigation into the predictors of digital fraud victimization in Thailand. By leveraging a large-scale dataset of 1200 respondents and applying binary logistic regression analysis, the research identifies statistically significant factors contributing to fraud susceptibility. Furthermore, the study estimates the national economic impact of digital fraud, offering policy-relevant insights that extend beyond academic theory to inform public awareness campaigns, consumer protection strategies, and digital literacy initiatives. In doing so, this research contributes to a nuanced understanding of the interplay between individual behavior, perception, and technology in shaping fraud vulnerability. It also provides one of the few large-scale, quantitative assessments of digital fraud victimization within a

Southeast Asian developing economy, thereby addressing a notable void in the literature and reinforcing the importance of context-specific cybersecurity research in the digital age.

2. Literature Review

As digital technologies become increasingly embedded in the financial systems of developing economies, concerns surrounding cybersecurity and fraud have intensified. While digital platforms offer convenience, speed, and greater access to financial services, they also create new vulnerabilities for users who may lack adequate technical awareness or protective tools. Digital fraud—ranging from phishing and identity theft to deceptive financial schemes—has become a significant threat, especially in countries where digital infrastructure outpaces cybersecurity regulation and consumer education. This literature review synthesizes existing research across four core domains: (1) the nature and prevalence of digital fraud in developing economies, (2) the role of demographic factors in fraud victimization, (3) behavioral and technological drivers of fraud risk, and (4) user perceptions of digital security and their paradoxical association with vulnerability. These themes provide the foundation for understanding how multiple dimensions interact to shape individuals' susceptibility to digital fraud, while also highlighting the gaps in current empirical research, particularly in the context of Thailand and comparable emerging markets.

2.1. The Nature and Prevalence of Digital Fraud in Developing Economies

The proliferation of digital technologies has revolutionized financial systems in developing economies, enabling increased access to banking, payments, and investment services through mobile and internet platforms. However, alongside these advancements, digital fraud has emerged as a growing threat, characterized by unauthorized transactions, phishing attacks, identity theft, and social engineering tactics aimed at deceiving users into compromising sensitive information. Digital fraud differs from traditional forms of fraud in its scope, speed, and technical complexity, often exploiting system vulnerabilities and low cybersecurity awareness among users (Jimmy, 2024; Li & Liu, 2021; Yoganandham & Govindaraj, 2024). In developing countries, including Thailand, the risks associated with digital fraud are exacerbated by structural challenges such as limited cybersecurity infrastructure, uneven digital literacy, and weak enforcement of data protection laws. Chayanon et al. (2025), Chusong et al. (2024), Lerdloompheephan (2024), and The Nation (2025) emphasize that despite growing internet penetration and digital transaction volumes, many users in Thailand remain unaware of the sophistication of online scams, making them prime targets. In addition, according to national surveys and law enforcement reports, cases of digital fraud—particularly those involving fake investment schemes and unauthorized mobile banking access—have surged over recent years. The lack of consistent preventive measures and limited consumer redress mechanisms further deepen the problem. These conditions underscore the urgency of context-specific research to understand the mechanisms of fraud exposure in emerging digital economies. In this study, digital fraud is viewed as a structural challenge in developing economies where rapid digital adoption outpaces cybersecurity readiness, regulation, and user awareness. This context frames Thailand as a high-risk environment in which widespread digital engagement coexists with limited protective capacity.

2.2. Demographic Factors Influencing Fraud Victimization

Several demographic variables have been identified in the literature as potential predictors of fraud susceptibility. Age, in particular, has received considerable attention. Older adults are often considered more vulnerable due to cognitive decline, limited digital familiarity, and increased trust in online systems (Ebner et al., 2023; Lazarus et al., 2025).

Conversely, younger individuals, while more digitally native, may engage in riskier behaviors due to overconfidence or insufficient understanding of digital risks (Freed et al., 2025; Holmarsdottir, 2024). Pituk et al. (2025) and Wang et al. (2025) argue that older adults with higher socioeconomic status are frequently targeted by fraudsters, not only because of their financial resources but also due to their social isolation and reduced access to technical support. Income level is another salient factor. Individuals with higher income are perceived as more attractive targets and may suffer greater financial losses, as confirmed in previous studies (Buse et al., 2024; Costantini et al., 2017; Sugiharti et al., 2023). Furthermore, student status also emerges as a significant predictor in some contexts. Abah and Agada (2025) highlight that students, while digitally active, often lack awareness of cybersecurity protocols, which increases their vulnerability. Gender, meanwhile, has produced inconsistent results in existing studies. While some researchers report that women are more frequently victimized (Kavvadias & Kotsilieris, 2025; Whitty, 2018), others find no significant differences (Hinduja & Patchin, 2008; Mwiraria et al., 2024), suggesting that gender alone may not determine fraud risk but could interact with other variables such as behavior, education, and device use. Moreover, education level, commonly assumed to provide a protective effect (Burke et al., 2022), has also yielded mixed findings. While higher education may improve critical thinking and awareness, some studies suggest that even well-educated individuals can fall victim to sophisticated scams, particularly if they are overconfident in their digital competence (Goud, n.d.; Griffith et al., 2023). In this study, these demographic insights collectively underline the importance of viewing fraud victimization as a multidimensional issue, shaped by a complex interplay of socio-economic, behavioral, and perceptual factors, rather than attributing risk to any single characteristic in isolation.

2.3. Behavioral and Technological Drivers of Digital Fraud Risk

Beyond demographics, behavioral patterns and technological engagement play a critical role in shaping digital fraud exposure. Frequent internet use, high engagement with social media, and reliance on mobile devices have been consistently linked to higher rates of victimization (Parmar et al., 2024; Marttila et al., 2021). These behaviors expand a user's digital footprint, thereby increasing the number of potential entry points for fraudulent actors. In Thailand, mobile-first behaviors—such as conducting banking or shopping activities via smartphones—have become widespread. However, this convenience often comes at the expense of security awareness, particularly when users click on unverified links or download applications without proper scrutiny. Furthermore, device type has also emerged as a key technological factor. Studies comparing Android and iOS operating systems have shown that Android users are generally more susceptible to fraud due to the platform's open-source nature and less stringent app review protocols (Ahmad et al., 2013). In contrast, the iOS ecosystem is widely regarded as more secure, largely owing to Apple's strict control over app distribution and stronger default privacy settings (Kollnig et al., 2022). The present study corroborates these findings, revealing that iOS users were significantly less likely to experience fraud compared to their Android counterparts. Additionally, social media usage further intensifies fraud risk. Popular platforms such as Facebook and LINE, which are heavily used in Thailand for both communication and commerce, are often exploited for fraudulent schemes ranging from fake promotions to impersonation scams (Lertsatitpirote & Kanyajit, 2023; Sirawongphatsara et al., 2024). Marttila et al. (2021) found a strong association between problematic social media use and cybercrime victimization, suggesting that both the frequency and psychological dependency on these platforms can increase an individual's vulnerability. These behavioral and technological trends underscore the need for improved digital hygiene, user education, and platform

accountability to mitigate exposure to cyber threats. In this study, behavioral routines and technological choices are recognized as critical drivers of digital fraud risk, emphasizing that fraud vulnerability is strongly tied to the everyday ways individuals interact with digital platforms.

2.4. Perceptions of Digital Security and the Illusion of Protection

Users' perceptions of digital security—how safe they believe online transactions and platforms to be—can significantly influence their actual risk of falling victim to fraud. Many individuals regard features such as password protection, two-factor authentication, and real-time alerts as sufficient safeguards. While these mechanisms are indeed essential, over-reliance on them can foster a false sense of security, leading users to engage in risky behaviors such as clicking on unknown links or disclosing personal information. This phenomenon, known as "risk compensation" or the "illusion of control," suggests that users may lower their guard in environments they perceive as secure (Arenas et al., 2024; D'Amato & Mastrolia, 2023; Kellner et al., 2019; Youn & Lee, 2009). Interestingly, perceptions of high security—such as confidence in identity verification protocols and alert systems—were associated with increased odds of fraud victimization. This paradox may be explained by a post-experience effect, wherein individuals who have previously been scammed report heightened awareness of security features. Alternatively, it may reflect an overestimation of one's ability to detect threats based on superficial cues rather than actual technical understanding. Maskall (2017) highlights that individuals often rely on the availability heuristic—judging the likelihood of events based on how easily examples come to mind—which can lead users to overestimate their own security. This bias reinforces a false sense of safety, particularly when identity verification features or security alerts are present, thereby increasing vulnerability to fraud. In addition, as Malik et al. (2024) note, the mere presence of visible security features does not guarantee user comprehension or cautious behavior. Perceptions of digital convenience—such as the ability to transact anytime and anywhere—can also diminish user vigilance. While users value speed and accessibility, they may overlook subtle warning signs or fail to verify the authenticity of transactions. This trade-off between usability and safety presents an ongoing challenge for digital platform designers and policymakers. As Lunn (2024) emphasizes, effective fraud prevention requires not only robust technical infrastructure but also user-centric design that actively encourages informed, reflective, and cautious digital behavior. In this study, users' perceptions of digital security are shown to contribute to vulnerability through overconfidence and risk-compensation behaviors. Even when security features are present, misplaced trust and cognitive biases may lead individuals to underestimate actual threat levels.

2.5. Conceptual Framework and Hypothesis Development

Figure 1 presents the conceptual framework illustrating the multidimensional predictors of digital fraud victimization, integrating demographic, behavioral, and perceptual determinants within a coherent theoretical structure.

The model in Figure 1 posits that demographic attributes shape individuals' baseline exposure and cognitive capacity to evaluate digital risks (Koning et al., 2024; Shi et al., 2024; Grigorescu et al., 2025). These demographic factors influence behavioral patterns, including the frequency and nature of digital engagement, reflected in portable device usage, social media participation, and operating system type (Marttila et al., 2021; Koch et al., 2024; Parmar et al., 2024). In turn, these behaviors affect users' perceptions of online safety and convenience, encompassing beliefs about transaction speed, accessibility, and the strength of digital security features (Hossain et al., 2024; Malik et al., 2024). Drawing on Rou-

tine Activity Theory, the framework conceptualizes fraud victimization as a consequence of increased exposure to motivated offenders through risky online routines (Puente & Hernández, 2022). Additionally, Cognitive Bias and Risk Compensation theories explain how perceived security fosters overconfidence, prompting riskier online behavior that paradoxically heightens vulnerability (Henkenjohann & Trenz, 2022; Ma & Chen, 2023; Maskall, 2017). The Socioeconomic Vulnerability perspective further contextualizes how financial capacity and life stage intersect with technology used to amplify risk, particularly among high-income individuals and older adults (Lazarus et al., 2025; Pituk et al., 2025; Wang et al., 2025). Collectively, this model underscores the dynamic interaction between who users are, how they behave online, and how they perceive digital security—offering a holistic understanding of the mechanisms driving fraud victimization in digital financial environments. Grounded in these theoretical perspectives, the model advances eighteen hypotheses, each representing a potential predictor of digital fraud victimization:

H1. *Gender is significantly associated with digital fraud victimization.*

H2. *Age is significantly associated with digital fraud victimization.*

H3. *Education is significantly associated with digital fraud victimization.*

H4. *Being a student is significantly associated with digital fraud victimization.*

H5. *Income is significantly associated with digital fraud victimization.*

H6. *Using iOS is significantly associated with digital fraud victimization.*

H7. *Internet usage time is significantly associated with digital fraud victimization.*

H8. *Having home internet access is significantly associated with digital fraud victimization.*

H9. *Using portable devices (e.g., smartphones, tablets) is significantly associated with digital fraud victimization.*

H10. *Social media engagement is significantly associated with digital fraud victimization.*

H11. *Perceived faster financial transactions (FFT) are significantly associated with digital fraud victimization.*

H12. *Perceived anytime, anywhere access to financial services (AAA) is significantly associated with digital fraud victimization.*

H13. *Perceived no travel costs, no queues, and no transaction fees (NTF) is significantly associated with digital fraud victimization.*

H14. *Perceived convenience in money transfers, top-ups, and payments (CMP) is significantly associated with digital fraud victimization.*

H15. *Perceived strong security systems (SSS) are significantly associated with digital fraud victimization.*

H16. *Password required for every login (PRL) is significantly associated with digital fraud victimization.*

H17. *Identity verification for first-time transactions (IVT) is significantly associated with digital fraud victimization.*

H18. *Alerts for every online transaction (AOT) are significantly associated with digital fraud victimization.*

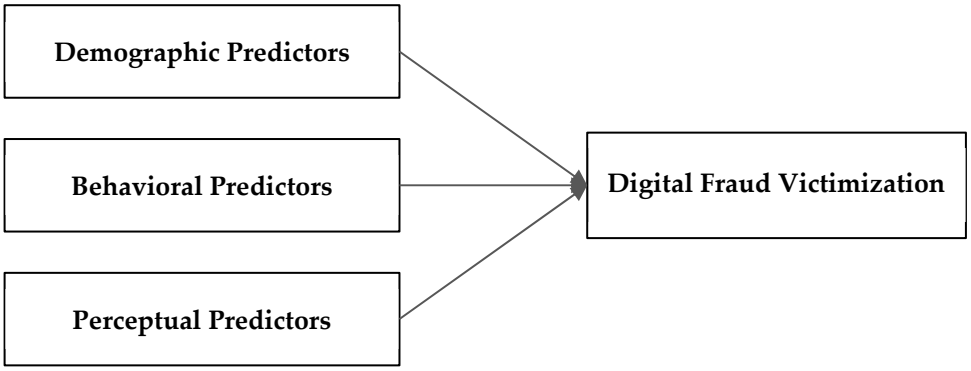


Figure 1. Conceptual Framework.

Collectively, these hypotheses reflect that digital fraud victimization arises from an interplay of individual characteristics, online behavioral exposure, and perceptual overconfidence in digital systems.

3. Materials and Methods

This study conducted a quantitative research approach, characterized by its systematic and empirical examination of phenomena through measurable data and statistical analysis. This methodology involves the rigorous collection and analysis of numerical data, enabling researchers to draw conclusions, make predictions, and identify patterns or relationships within the data.

3.1. Questionnaire Design and Instrument Validation

In this quantitative study, a structured questionnaire was carefully developed to ensure alignment with the research objectives and methodological rigor. The instrument consisted of five main sections: demographic information (e.g., age, gender, education level, occupation, and income), digital behavior (e.g., internet usage patterns, devices and operating systems used, and preferred social media platforms), perceived benefits of digital transactions (e.g., convenience, cost-efficiency, and accessibility), perceived digital security features (e.g., password protection, user authentication, and fraud alerts), and digital fraud experience, including victimization history and financial loss. The questionnaire items were developed from established literature on digital financial behavior, cybersecurity, and fraud victimization, with adaptations made to suit the Thai context. Variable selection was theory-driven, reflecting prior evidence on cybercrime, demographic vulnerability, behavioral exposure, and digital-security perceptions. All variables specified in the conceptual framework and hypotheses (H1–H18) were included in the full model to prevent omitted-variable bias and support both exploratory and confirmatory aims. No automated selection methods were applied; inclusion was based solely on theoretical and empirical relevance. A content validation process was conducted to ensure relevance, clarity, and cultural appropriateness of each item. A pilot test was conducted with a sample of 30 participants to assess clarity, identify ambiguities, and ensure respondent comprehension. Based on feedback from the pilot, several revisions were made: technical jargon was simplified, response categories were expanded to improve inclusiveness, and the item sequence was reorganized for better logical flow. Redundant or ambiguous items were

removed to enhance conciseness and internal consistency. Additionally, the reliability of the measurement scale was evaluated using Cronbach's alpha, which yielded a value of 0.896. This indicates a high level of internal consistency among the scale items, suggesting that the data collection instrument is reliable and robust. In general, a Cronbach's alpha coefficient ranging from 0.70 to 0.79 is considered acceptable, values between 0.80 and 0.89 denote good reliability, and coefficients approaching 0.90 reflect strong internal consistency (Arof et al., 2018; Phuangsuwan et al., 2025). Therefore, the obtained alpha confirmed that the scale effectively measures the intended constructs with minimal random error, ensuring the credibility of the study's findings.

3.2. Sample Selection

To examine the relationship between individual characteristics, digital behavior patterns, perceptions of digital transaction benefits and security, and the probability of experiencing digital fraud, this study employed a hybrid sampling strategy combining stratified and convenience sampling to ensure broader representativeness and methodological rigor. The target population comprised Thai residents aged 18 years and older who had prior experience with or exposure to online financial transactions. The minimum sample size was determined using Cochran's formula, based on a 95% confidence level and a 0.05 margin of error, yielding a baseline requirement of 384 participants as recommended by Uakarn et al. (2021). To enhance statistical robustness and account for non-responses or incomplete submissions, the final sample was expanded to 1200 valid and completed responses. In the stratified phase, the population was categorized according to key demographic criteria—age group, income level, and occupation—to ensure proportional inclusion of major segments within Thailand's digital user base. Within each stratum, convenience sampling was applied to recruit respondents efficiently via digital channels. This combined approach maintained the accessibility advantages of convenience sampling while improving the demographic balance and generalizability of the results.

3.3. Data Collection

The data collection phase was systematically carried out through online platforms, such as Facebook and LINE platforms, widely used communication applications in Thailand, chosen for their extensive reach and popularity across diverse segments of the population. The mobile-friendly survey was distributed during May and June 2025, leveraging Facebook and LINE's broad user base to optimize participant engagement and ensure high response rates. The timing and duration of data collection were strategically planned to capture a wide range of digital behaviors and fraud-related experiences across different demographic groups. Utilizing Facebook and LINE enabled efficient and real-time participation, facilitated technical support when needed, and contributed to maintaining a high level of response quality. Following data collection, all responses were rigorously screened for completeness, consistency, and adherence to the study's eligibility criteria—specifically, participants had to be Thai residents aged 18 years or older with prior experience or exposure to digital financial activities. Incomplete submissions and those failing to meet the inclusion criteria were excluded to preserve the integrity of the dataset. Only fully completed questionnaires were retained for analysis, ensuring that the data were both accurate and robust for statistical examination. This quality-control process strengthened the reliability of the findings and supported a comprehensive analysis of the factors influencing individuals' likelihood of experiencing digital fraud in the Thai context.

With regard to ethical considerations, this study employed a questionnaire-based design to collect data via an online survey distributed through online platforms. Prior to participation, all respondents were clearly informed of the study's objectives and assured

that their data would be used solely for academic purposes. The research was non-medical in nature, involved no vulnerable populations, and included only participants aged 18 years or older. Participation was entirely voluntary, and any incomplete or withdrawn responses were excluded from the analysis to maintain the integrity and voluntariness of the data. Anonymity and confidentiality were strictly preserved, with no personally identifiable information collected or reported. Informed consent was obtained from all participants, who received a transparent explanation of the study's purpose, procedures, and any potential risks or benefits. Data were analyzed in aggregate form and presented in a manner that precluded individual identification. In accordance with the announcement by Thailand Science Research and Innovation (TSRI), studies in the behavioral, social sciences, and humanities that do not affect the body, mind, cells, or genetic material, and that use anonymous instruments such as questionnaires, are exempt from formal ethics committee approval. As outlined in Guidance No. 3(3), this exemption applies to research conducted anonymously, where participants cannot be identified directly or indirectly (Phuangsuwan et al., 2024). Therefore, this study met the criteria for exemption but nonetheless adhered strictly to all ethical standards and regulatory frameworks, demonstrating a clear commitment to safeguarding the rights, dignity, and well-being of all individuals involved.

3.4. Data Analysis

Before data analysis, data cleansing was performed to check for missing values, coding errors, and logical inconsistencies. The analysis then applied descriptive and inferential statistical techniques using Jamovi (version 2.16.17.0), an open-source platform widely used in behavioral and social science research. Jamovi offers an intuitive interface, reproducible syntax, and high-quality implementations of generalized linear models, ensuring transparency and replicability. Descriptive statistics were first used to summarize participant demographics, digital behavior patterns, and perceptions related to digital transaction benefits and security. These summaries provided a foundational understanding of the sample's characteristics and behavioral trends. Multicollinearity among predictors was assessed using Tolerance and Variance Inflation Factor (VIF) values. All predictors met acceptable levels (Tolerance > 0.20; VIF < 5), indicating no multicollinearity concerns and supporting the inclusion of all variables in the final model. To assess the impact of various independent variables—including demographic attributes, internet usage habits, device types, and perceptions of transaction safety—on a binary dependent variable (fraud experience, coded as 1 = Yes and 0 = No), the study utilized binary logistic regression analysis, which is particularly suitable for this study. The dependent variable—digital fraud victimization—is dichotomous. As noted by Chatla and Shmueli (2017), logistic regression is a widely accepted method for examining dichotomous outcome variables, making it particularly suitable for this investigation. This technique estimated the probability of individuals falling victim to digital fraud based on the values of multiple predictor variables. The analysis yielded odds ratios, which allowed for the interpretation of how strongly each factor influenced the likelihood of fraud victimization. By modeling this binary outcome, the study generated statistically robust insights into the key drivers of digital fraud exposure in Thailand, offering evidence-based perspectives on the vulnerabilities present in a rapidly digitizing financial environment.

4. Results

The g 0.743(AAA) + gital behavior characteristics of the survey participants were carefully examined using data obtained from online questionnaires. This assessment served as a vital foundation for interpreting the study's overall results.

Table 1 presents the general demographic and digital behavior characteristics of the 1200 respondents who participated in the study. The sample was composed of 59.6% female and 40.4% male participants, reflecting a slightly higher representation of women in the dataset. In terms of age distribution, the largest group of respondents (27.0%) were between 21 and 30 years old, followed closely by those over 50 years (26.8%) and those under 21 years (21.8%). Educational attainment was relatively high, with 56.8% of participants holding a bachelor's degree, while 22.1% had education below the undergraduate level, and 21.1% had attained a postgraduate degree. Occupation-wise, students represented the largest group (34.8%), followed by government officers (28.7%), private company employees (15.7%), and business owners (18.5%). In terms of income, 39.3% of respondents reported earning more than 40,000 Baht per month, suggesting that the sample included a substantial proportion of individuals with higher income levels. Regarding mobile operating systems, users were nearly evenly split between iOS (49.4%) and Android (47.2%), with only a small proportion (3.4%) using other systems. Internet usage behavior revealed that a majority (66.3%) of participants reported spending more than two hours online per session, indicating high digital engagement. The most commonly used device for accessing digital platforms was the smartphone (83.2%), followed by computers (12.7%) and tablets (4.1%). In terms of social media usage, Facebook emerged as the dominant platform (61.1%), followed by Line (16.0%), X (formerly Twitter) (13.6%), TikTok (6.0%), and Instagram (3.3%). These findings provide a comprehensive overview of the respondents' demographic profiles and digital behaviors, offering a contextual foundation for analyzing their vulnerability to digital fraud in subsequent sections of the study.

Table 1. General demographic and digital behavior characteristics.

General Information		Frequency	Percentage
Gender	Male	485	40.4
	Female	715	59.6
Age	Less than 21 years old	261	21.8
	21–30 years old	325	27.0
	31–40 years old	168	14.0
	41–50 years old	125	10.4
	Over 50 years old	321	26.8
Education	Lower than bachelor's degree	265	22.1
	Bachelor's degree	681	56.8
	Higher than bachelor's degree	254	21.1
Occupation	Private company employee	188	15.7
	Government officer	344	28.7
	Business owner	222	18.5
	Student	417	34.8
	Freelancer	29	2.3
Income	Less than 10,001 THB	232	19.3
	10,001–20,000 THB	202	16.8
	20,001–30,000 THB	135	11.3
	30,001–40,000 THB	160	13.3
	More than 40,000 THB	471	39.3
Mobile operating systems	iOS	593	49.4
	Android	566	47.2
	Others	41	3.4

Table 1. *Cont.*

General Information		Frequency	Percentage
Internet usage time	Less than 30 min	96	8.0
	30 min–1 h	187	15.6
	1 h–2 h	122	10.1
	More than 2 h	795	66.3
Most-used portable devices	Computers and laptops	152	12.7
	Tablets	49	4.1
	Smartphones	999	83.2
Most-used social media	Facebook	733	61.1
	Line	192	16.0
	Instagram	40	3.3
	X (Twitter)	163	13.6
	TikTok	72	6.0
Total		1200	100.0

Table 2 summarizes participants' awareness and perceptions of digital transaction practices, as measured by mean scores and standard deviations. Overall, the findings indicate a high level of perceived benefit and security associated with digital financial activities among Thai users. The item with the highest mean score was "Convenient money transfers, top-ups, and payments" (CMP), with a mean of 4.54 and a standard deviation of 0.660, suggesting that most respondents strongly agree that digital platforms offer practical advantages for financial transactions. Similarly, high mean values were observed for "No travel costs, no queues, no transaction fees" (NTF) (M = 4.51), "Faster financial transactions" (FFT) (M = 4.43), and "Anytime, anywhere access to financial services" (AAA) (M = 4.43), all indicating broad recognition of digital convenience and efficiency. In terms of perceived security, the results were also positive. The items "Password required for every login" (PRL) and "Identity verification for first-time transactions" (IVT) both had mean scores of 4.26, while "Alerts for every online transaction" (AOT) followed closely with a mean of 4.25. Notably, the item "Strong security system" (SSS) received a slightly lower but still favorable mean of 3.92, implying that while users generally trust the security infrastructure, there may still be some residual concerns or variability in perceived robustness. The relatively low standard deviations across all items suggest consistency in user perceptions. Collectively, these results highlight that respondents are well aware of both the functional and protective features of digital transactions, which may influence their digital behavior and exposure to fraud-related risks in meaningful ways.

Table 2. Perceptual awareness of digital transaction practices.

Perceptual Awareness of Digital Transaction Practices	Mean	Std. Deviation
Faster financial transactions (FFT)	4.43	0.687
Anytime, anywhere access to financial services (AAA)	4.43	0.702
No travel costs, no queues, no transaction fees (NTF)	4.51	0.705
Convenient money transfers, top-ups, and payments (CMP)	4.54	0.660
Strong security system (SSS)	3.92	0.729
Password required for every login (PRL)	4.26	0.727
Identity verification for first-time transactions (IVT)	4.26	0.730
Alerts for every online transaction (AOT)	4.25	0.805

Table 3 presents the distribution of fraud experience among the 1200 respondents and reveals a strikingly high prevalence of digital fraud victimization. A substantial majority—843 respondents, or 70.3%—reported having experienced digital fraud, while only 29.8%

(357 respondents) indicated that they had never encountered such incidents. This finding underscores the widespread nature of digital fraud in the Thai context and highlights the growing urgency of addressing cybersecurity risks as digital financial transactions become more common. The high rate of fraud experience suggests that despite widespread awareness of digital transaction benefits and security features (as seen in Table 2), a significant portion of the population remains vulnerable to fraud attempts. This pattern may reflect gaps between perceived safety and actual protective behavior, or it may indicate that current digital security measures are insufficient to deter increasingly sophisticated fraud tactics. These results provide a critical foundation for deeper analysis of the variables that predict fraud victimization, particularly within the context of individual characteristics and digital engagement patterns explored in subsequent sections of the study.

Table 3. Fraud experience.

Fraud Experience	Frequency	Percentage
No	357	29.8
Yes	843	70.3
Total	1200	100.0

Subsequently, the dataset was refined through a data-cleaning process, focusing on 843 respondents who reported experiencing fraud. This targeted subset enabled a more precise analysis of influencing factors and an in-depth examination of individuals within the fraud experience context.

Table 4 presents the average monetary loss incurred by respondents who reported experiencing digital fraud. Among the 843 individuals who indicated they had been victims of digital fraud, the mean financial damage was 3236.69 Baht, with a standard deviation of 7294.31. This wide standard deviation suggests considerable variability in the extent of financial loss, indicating that while some victims may have suffered minor losses, others experienced significantly higher levels of financial damage. To estimate the broader economic impact of digital fraud at the national level, the study extrapolated these findings using demographic data from Thailand's 2025 national statistics. With 70.3% of respondents having experienced digital fraud, and the adult population aged 21 and over in Thailand estimated at 55,667,452 individuals, it was projected that approximately 39,127,707 people had encountered digital fraud. Multiplying this number by the average loss yielded an estimated total economic damage of approximately 126.63 billion Baht (39,127,707 $\times$ 3236.69) nationwide. These findings highlight not only the individual financial consequences of digital fraud but also its substantial macroeconomic implications, reinforcing the need for targeted digital security interventions and consumer protection policies within Thailand's rapidly evolving digital economy.

Table 4. Damage value.

N	Mean	Std. Deviation
843	3236.688	7294.313

Table 5 presents the results of the Omnibus Test of Model Coefficients, assessing the overall significance of the logistic regression model predicting digital fraud victimization. The chi-square value is 575.152 with 18 degrees of freedom and a p-value of 0.000, indicating statistical significance at the 0.05 level. This confirms that the independent variables collectively enhance the prediction of whether an individual has experienced digital fraud compared to a model without predictors.

Table 5. Omnibus test of the model's performance.

		Chi-Square	df	Sig.
Step 1	Step	575.152	18	0.000
	Block	575.152	18	0.000
	Model	575.152	18	0.000

Table 6 provides the model summary statistics for the logistic regression analysis, offering insights into the model's explanatory power in predicting digital fraud victimization. The reported −2 Log Likelihood value is 885.803, indicating the goodness-of-fit of the model; lower values generally suggest a better-fitting model. Two pseudo R-square statistics are also presented: Cox & Snell R^2 = 0.381 and Nagelkerke R^2 = 0.541. While Cox & Snell R^2 gives a conservative estimate of the explained variance, Nagelkerke R^2 adjusts the value to range from 0 to 1, allowing for clearer interpretation. In addition, the model yielded a Nagelkerke R^2 value of 0.541, indicating that approximately 54.1% of the variance in digital fraud victimization is explained by the combined demographic, behavioral, and perceptual predictors. Within social science research, where complex human behavior is influenced by multiple unobserved or latent factors, a value above 0.50 is considered notably strong. This suggests that the model not only fits the data well but also captures key mechanisms underlying fraud vulnerability in Thailand's digital environment.

Table 6. The model summary.

Step	−2 Log Likelihood	Cox & Snell R Square	Nagelkerke R Square
1	885.803 [a]	0.381	0.541

[a]. Estimation terminated at iteration number 6 because parameter estimates changed by less than 0.001.

Table 7 presents the classification results of the logistic regression model, which assesses its ability to accurately predict whether an individual has experienced digital fraud. The classification table compares observed outcomes with predicted classifications, using a cut-off value of 0.50 to distinguish between predicted cases of fraud victimization (Yes) and non-victimization (No). According to the results, the model correctly predicted 64.4% of non-victims and 87.7% of victims, resulting in an overall prediction accuracy of 80.8%. This high level of classification accuracy demonstrates the model's effectiveness in distinguishing between individuals who have and have not experienced digital fraud based on the selected independent variables. The relatively higher accuracy in predicting fraud victims suggests that the model is particularly sensitive to identifying risk factors associated with vulnerability to digital fraud. These results confirm the practical utility of the model for predictive purposes and support its robustness in capturing the dynamics of fraud victimization within the surveyed population.

Table 7. Classification table for back-testing.

Observed			Predicted		
			Fraud Experience		Percentage Correct
			No	Yes	
Step 1	Fraud experience	No	230	127	64.4
		Yes	104	739	87.7
Overall percentage					80.8%

Note: The cut-off value is 0.500.

The predictive regression equation of Model (1) using the coefficients from Table 8 can be described by the following equation:

$$P = \frac{1}{1 + e^{-z}} \quad (1)$$

where P is the digital fraud victimization in Thailand, and $Z = -21.876 + 0.671$(age) + 0.740(being a student) + 1.305(income) − 0.673(using iOS) + 0.788(portable devices) + 0.761(social media) + 1.054(FFT) + 0.743(AAA) + 0.468(SSS) + 0.687(PRL) + 1.070(IVT).

Table 8. Variables in the model.

	Variables	B	S.E.	Wald	df	Sig.	Exp(B)	Tolerance	VIF	Actions
Step 1 [a]	H1: Gender	−0.048	0.196	0.060	1	0.806	0.953	0.834	1.200	Rejected
	H2: Age	0.671	0.103	42.517	1	0.000	1.956	0.321	3.117	Accepted
	H3: Education	0.297	0.157	3.598	1	0.058	1.346	0.693	1.443	Rejected
	H4: Being a student	0.740	0.321	5.314	1	0.021	2.095	0.382	2.617	Accepted
	H5: Income	1.305	0.104	156.102	1	0.000	3.687	0.394	2.541	Accepted
	H6: Using iOS	−0.673	0.195	11.901	1	0.001	0.510	0.780	1.282	Accepted
	H7: Internet usage	0.164	0.096	2.948	1	0.086	1.179	0.711	1.407	Rejected
	H8: Home internet	0.135	0.200	0.460	1	0.498	1.145	0.876	1.142	Rejected
	H9: Portable devices	0.788	0.142	30.787	1	0.000	2.198	0.757	1.320	Accepted
	H10: Social media	0.761	0.100	57.450	1	0.000	2.141	0.822	1.217	Accepted
	H11: FFT	1.054	0.252	17.468	1	0.000	2.870	0.328	3.053	Accepted
	H12: AAA	0.743	0.316	5.541	1	0.019	2.103	0.265	3.768	Accepted
	H13: NTF	0.264	0.255	1.072	1	0.300	1.303	0.403	2.484	Rejected
	H14: CMP	0.284	0.290	0.959	1	0.327	1.329	0.304	3.293	Rejected
	H15: SSS	0.468	0.186	6.328	1	0.012	1.596	0.487	2.052	Accepted
	H16: PRL	0.687	0.218	9.930	1	0.002	1.989	0.347	2.884	Accepted
	H17: IVT	1.070	0.247	18.758	1	0.000	2.915	0.383	2.610	Accepted
	H18: AOT	0.221	0.181	1.494	1	0.222	1.248	0.397	2.518	Rejected
	Constant	−21.876	2.663	67.504	1	0.000	0.000	-	-	Accepted

[a]. Variable(s) entered in step 1: Gender, age, education, being student, income, using iOS, internet usage time, home internet, portable devices, social media, FFT, AAA, NTF, CMP, SSS, PRL, IVT, AOT. Note: Variables with p-values below 0.05 are accepted as significant predictors (Accept), while those with p-values above 0.05 are not statistically significant (Reject). Note: Since the Constant is not a predictor variable, it is not correlated with other predictors, and therefore Tolerance and VIF values are not computed for it.

Table 8 summarizes the logistic regression results, highlighting both significant and non-significant predictors of digital fraud victimization among the respondents. Several variables showed statistically significant effects at the 0.05 level, indicating a meaningful influence on the likelihood of experiencing fraud, while others did not demonstrate significant associations and therefore do not reliably predict fraud victimization.

Among demographic factors, gender (H1: B = −0.048, Sig. = 0.806, Exp(B) = 0.953) and education level (H3: B = 0.297, Sig. = 0.058, Exp(B) = 1.346) were not significant predictors of fraud victimization, indicating that being male or female, or holding higher educational qualifications, does not meaningfully influence the likelihood of experiencing digital fraud. In contrast, age (H2: B = 0.670, Sig. = 0.000, Exp(B) = 1.956), student status (H4: B = 0.739, Sig. = 0.021, Exp(B) = 2.095), and income (H5: B = 1.305, Sig. = 0.000, Exp(B) = 3.687) emerged as significant predictors. Older individuals were found to have nearly double the odds of victimization, while students were over twice as likely to be targeted compared to non-students. Higher-income individuals were almost 3.7 times more likely to experience fraud, suggesting both increased exposure to digital financial activities and greater financial attractiveness to scammers.

Within behavioral factors of technological usage, iOS usage (H6: B = −0.673, Sig. = 0.001, Exp(B) = 0.510), reliance on portable devices (H9: B = 0.787, Sig. = 0.000, Exp(B) = 2.198), and social media engagement (H10: B = 0.761, Sig. = 0.000, Exp(B) = 2.141) significantly influenced fraud risk. iOS users were less likely to be victimized, reflecting the platform's stronger security architecture, whereas individuals relying on portable devices

or engaging intensively with social media were more than twice as likely to experience fraud. Conversely, internet usage time (H7: B = 0.165, Sig. = 0.086, Exp(B) = 1.179) and home internet access (H8: B = 0.135, Sig. = 0.498, Exp(B) = 1.145) were not significant predictors, suggesting that general levels of online connectivity do not inherently elevate the risk of fraud.

In terms of user perceptions, faster financial transactions (H11: B = 1.054, Sig. = 0.000, Exp(B) = 2.870), anytime–anywhere access (H12: B = 0.744, Sig. = 0.019, Exp(B) = 2.103), confidence in strong security systems (H15: B = 0.468, Sig. = 0.012, Exp(B) = 1.596), reliance on password-based login (H16: B = 0.687, Sig. = 0.002, Exp(B) = 1.989), and trust in identity verification for first-time transactions (H17: B = 1.070, Sig. = 0.000, Exp(B) = 2.915) were all significant predictors. These findings suggest that individuals who strongly prioritize convenience or who exhibit high confidence in platform security features may unintentionally expose themselves to greater risk, reflecting tendencies toward overconfidence and risk-compensating behaviors. Meanwhile, perceptions of no travel cost, queues, or fees (H13: B = 0.264, Sig. = 0.300, Exp(B) = 1.303), convenience in payments (H14: B = 0.284, Sig. = 0.327, Exp(B) = 1.329), and transaction alerts (H18: B = 0.222, Sig. = 0.222, Exp(B) = 1.248) were not statistically significant, indicating that these convenience- and alert-related features alone do not meaningfully influence the probability of becoming a fraud victim.

Overall, the combined findings indicate that fraud victimization is shaped less by general demographics or routine digital access and more by specific behavioral, perceptual, and technological risk factors. Significant predictors such as age, student status, income, portable device use, social media activity, and convenience-driven attitudes all substantially heighten vulnerability, while strong confidence in security features further amplifies risk through overconfidence. In contrast, factors such as gender, education, internet usage time, and basic convenience perceptions show no meaningful impact. The protective effect of iOS highlights the role of secure ecosystems in reducing exposure. Taken together, the results suggest that fraud risk is primarily driven by targeted behaviors and perceptions rather than broad user characteristics, emphasizing the need for improved digital literacy, cautious transaction practices, and awareness of social-engineering threats.

5. Discussion

This study explored the demographic, behavioral, and perceptual factors associated with digital fraud victimization in the context of a developing economy, using Thailand as a case study. The results offer several important insights into the profiles and experiences of individuals who fall victim to digital fraud and highlight broader implications for public policy, consumer protection, and digital literacy initiatives.

First, the finding that 70.3% of respondents had experienced digital fraud underscores the alarming prevalence of this issue in Thailand's digital economy. This high rate is especially notable considering the strong awareness levels reported regarding digital transaction benefits and security features. While respondents widely acknowledged the convenience, speed, and accessibility of digital financial platforms, these advantages have not necessarily translated into safety. This disconnect between perceived protection and actual vulnerability suggests that user confidence in digital systems may lead to underestimating fraud risks—a phenomenon that aligns with previous literature on overconfidence bias in cybersecurity behaviors. Aligned with Lunn (2024), the implementation of advanced security measures—such as encryption, Multi-Factor Authentication (MFA), and secure payment gateways—plays a critical role in safeguarding sensitive information. However, despite their importance, these security protocols can introduce complexity that may negatively affect the user experience. Specifically, the additional steps required for authentication and

transaction verification can create friction, leading to user frustration or abandonment of the process. Balancing robust security with seamless usability thus remains a key challenge in digital transaction design. Furthermore, as indicated by Chayanon et al. (2025) and P. Sharma (2024), inadequate user training in identifying and reporting suspicious activity can allow fraudsters to exploit the convenience of a system. Striking an effective balance between security and user convenience is therefore essential. Insufficient user awareness creates critical vulnerabilities, highlighting the need for clear guidance and user-oriented security practices as integral components of effective fraud prevention strategies (Tripathi & Tripathi, 2024).

The logistic regression analysis identified several significant predictors of fraud victimization. Demographic factors, including age, income, and student status, were positively associated with an increased likelihood of experiencing fraud. Older adults and individuals with higher income levels may be targeted more frequently due to greater digital exposure or their perceived financial worth. Consistent with Lazarus et al. (2025), digital fraudsters often exploit age as a vulnerability, thereby reinforcing ageist practices. In this context, ageism in cybercrime can be understood as the deliberate targeting or prioritization of older adults as potential victims. This demographic is particularly susceptible due to a combination of physiological factors, such as cognitive decline; psychological factors, including heightened fear of cybercrime; familial risks, such as insider fraud; and sociocultural conditions, including social isolation. Cybercrimes against senior citizens are predominantly socioeconomic in nature and typically motivated by financial gain. Similarly, Wang et al. (2025) confirmed that older adults with higher socioeconomic status are more likely to be targeted by digital fraud, although this does not necessarily result in actual financial loss. Furthermore, students also emerged as a high-risk group, likely due to limited financial resources, lack of digital security experience, and inadequate understanding of the legal consequences of cybercrime. In line with Abah and Agada (2025), many students remain unaware of the potential repercussions of their actions, which can lead to risky behaviors and further increase their vulnerability to both perpetrating and falling victim to cyber-related offenses. These findings highlight the importance of implementing targeted digital safety campaigns and interventions that address the specific needs and vulnerabilities of different demographic groups.

Behavioral factors also played a significant role in cybercrime victimization. Frequent use of portable devices and social media platforms was associated with a higher likelihood of victimization, likely because these technologies create multiple points of entry for fraudulent actors. Notably, iOS users were significantly less likely to experience fraud compared to Android users, potentially due to stricter security protocols or differing usage patterns. These findings indicate that both device-level features and individual usage habits can tangibly affect exposure to cyber threats. Consistent with Parmar et al. (2024), increased daily mobile use, a preference for social media as the primary mobile activity, and social media addiction were linked to a heightened risk of cyberbullying. Similarly, Griffith et al. (2023) reported that greater engagement in online activities correlates with a higher likelihood of cybercrime victimization. Risky online behavior and inadequate security measures further compound this vulnerability. Marttila et al. (2021) also found a strong association between problematic social media use and increased risk of cybercrime, with within-subjects analysis revealing that higher levels of problematic use were significantly linked to a greater chance of being victimized. These findings underscore the cumulative impact of excessive and irresponsible online behavior on cybercrime vulnerability, emphasizing the importance of mindful digital engagement. Moreover, Ahmad et al. (2013) highlighted that Android devices are more susceptible to viruses and other security threats, primarily due to their open-source architecture and less rigorous app review process. In comparison, Kollnig et al.

(2022) noted that the iOS ecosystem is generally more privacy-protective, offering tighter restrictions on data sharing and third-party access. Apple's strict control over its App Store reduces the risk of malware, thereby enhancing the overall security of iOS devices relative to Android.

Moreover, perceptions related to security features—such as identity verification protocols, password requirements, and alert systems—were paradoxically associated with a higher likelihood of fraud victimization. Although this may initially appear counterintuitive, such heightened security awareness often arises from prior negative experiences, such as having been previously targeted by fraud. This post-experience learning effect suggests that security consciousness may function more as a reactive measure than a preventive one. Additionally, awareness of phishing and other digital scams typically increases following exposure or victimization. Another plausible explanation is that the presence of perceived security features may foster a false sense of safety, prompting users to engage in riskier online behaviors—a phenomenon known as "risk compensation." This is further supported by Arenas et al. (2024) and Kellner et al. (2019), who argue that security tools can create an "illusion of control," giving users a false sense of security and thereby encouraging riskier online activity that may ultimately lead to security incidents. This underscores the importance of designing security systems that not only incorporate robust technical safeguards but also provide behavioral guidance and user education. Consistent with the findings of Li and Liu (2021) and Malik et al. (2024), fear of data breaches, unauthorized access, and misuse of personal information can lead to heightened anxiety and mistrust. Individuals may become increasingly concerned about the safety of their digital identities, financial data, and personal communications. As a result, they may be reluctant to engage in online activities—such as e-commerce or social networking—that require the disclosure of personal information. These widespread concerns about data privacy in the digital era contribute to a sense of vulnerability and can adversely affect overall well-being.

A notable and counterintuitive finding of this study is the positive association between perceived digital security and fraud victimization. Individuals who expressed strong confidence in password requirements, identity verification mechanisms, and overall platform security were significantly more likely to have experienced digital fraud. This paradox may be driven by risk-compensation behavior, where users relax vigilance when they believe security systems are robust, or by cognitive biases such as the illusion of control. It may also reflect post-victimization learning, as individuals who have already been scammed become more aware of security features afterward. This dynamic underscores the importance of designing security systems that promote not only technical protection but also continuous user vigilance (Brandimarte et al., 2013; Datta et al., 2022; Maini & Sindhi, 2025; Whitty, 2025).

Interestingly, several demographic and behavioral variables—such as gender, education level, daily internet usage time, and perceived benefits like transaction alerts and cost savings—were not statistically significant predictors of fraud. These findings contradict earlier assumptions that linked demographic characteristics with differential vulnerability to cybercrime (e.g., Buse et al., 2024; Dadà et al., 2025; Kavvadias & Kotsilieris, 2025). Consistent with this, Mwiraria et al. (2024) found no statistically significant difference in the rates of cybercrime victimization between males and females, suggesting that both sexes are equally at risk. Nonetheless, their research also showed that age and education level were significantly associated with cybercrime victimization, indicating the importance of developmental and cognitive maturity in digital risk assessment. Taken together, these findings emphasize the complexity of cybercrime exposure and the necessity of moving beyond oversimplified demographic generalizations. Context-specific, data-driven insights are vital for shaping effective and equitable fraud prevention strategies.

The discussion highlights the multifaceted nature of digital fraud risk, driven by a complex interplay of demographics, technology use, and psychological perceptions. Addressing these risks requires a combination of technical safeguards, user education, and behaviorally informed policy interventions. As digital transactions continue to grow in popularity, especially in developing economies, building public resilience to fraud must become a national priority.

6. Conclusions

This study investigated the demographic, behavioral, and technological determinants of digital fraud victimization in a developing economy, using empirical data from Thailand. The results revealed that digital fraud is highly prevalent, with more than 70% of respondents reporting personal experience with online scams. Logistic regression analysis identified age, income, student status, device usage, social media engagement, and perceived digital security features as significant predictors of fraud vulnerability. Notably, individuals who believed in the strength of digital security measures—such as identity verification and login protocols—were paradoxically more likely to experience fraud, suggesting a possible overconfidence effect or reactive security awareness following prior victimization. This paradox underscores the need for policies and digital literacy initiatives that address user overconfidence and emphasize careful, informed online behavior, even when security mechanisms appear robust. Furthermore, iOS users were found to be significantly less likely to fall victim, pointing to potential differences in operating-system-level security. These findings underscore the need for a multidimensional approach to digital fraud prevention, one that incorporates technological safeguards, behavioral education, and user-centric design.

6.1. Research Contribution

This study contributes to the understanding of digital fraud victimization in developing economies by examining how demographic characteristics, behavioral patterns, and technological factors collectively shape exposure to fraud. Drawing on a large dataset from Thailand, the findings identify key predictors—including age, income, student status, mobile-device dependence, and social media engagement—that help explain why certain population groups are more vulnerable. A distinctive contribution is the identification of a paradoxical effect in which stronger perceived digital security corresponds with greater fraud victimization, underscoring the influence of cognitive biases and overconfidence in digital environments. This insight enriches current discussions on cybersecurity by highlighting the importance of user psychology and behavioral tendencies in shaping actual risk.

6.2. Policy Implication

The findings underscore the urgent need for coordinated national action to reduce digital fraud vulnerability. Public agencies should prioritize continuous digital literacy and fraud-awareness programs, with targeted interventions for high-risk groups such as students, young adults, and lower-income users. These initiatives should incorporate behavioral-science principles to address cognitive biases, including the illusion of control and risk-compensation tendencies, which can inflate confidence in platform security. Communication strategies must correct misconceptions about digital safeguards by emphasizing that technical features alone do not eliminate fraud risks. Stronger collaboration among regulators, digital platforms, telecom operators, and financial institutions is essential to enhance real-time detection, reporting, and coordinated responses. Financial institutions and fintech developers should adopt secure-by-design approaches that prioritize user

comprehension, integrate behavioral cues, and minimize opportunities for error. Additionally, policymakers should update legal frameworks to address evolving scam tactics and invest in specialized cyber-investigation capacity. Collectively, these actions can mitigate behavioral vulnerabilities, bridge the gap between perceived and actual digital security, and strengthen national digital resilience.

6.3. Limitations and Future Research

This study has limitations that suggest directions for future research. First, the use of convenience sampling may limit generalizability, particularly for underrepresented groups such as rural residents or those with limited internet access; future studies should employ more diverse and probabilistic sampling and consider cross-country comparisons in Southeast Asia to enhance external validity. Second, reliance on self-reported data may introduce recall and social desirability biases; integrating objective measures, such as transaction or platform-reported data, could improve reliability. Third, the cross-sectional design limits causal inference; longitudinal studies are needed to examine how security perceptions, behaviors, and fraud experiences evolve over time. Finally, the absence of interaction terms highlights the importance of exploring moderating effects between demographic, behavioral, and perceptual variables—for example, how age or income influences the link between perceived security and fraud risk. Addressing these limitations can provide more nuanced, robust, and generalizable insights into digital fraud vulnerability, informing both theory and practice in cybersecurity.

Author Contributions: Conceptualization, T.K., P.L. and R.S.; methodology, T.K. and P.L.; software, T.K., P.L., R.S. and V.C.; validation, T.K., P.L., R.S. and V.C.; formal analysis, T.K., P.L. and R.S.; investigation, T.K., P.L., R.S. and V.C.; resources, T.K., P.L., R.S. and V.C.; data curation, T.K., P.L., R.S. and V.C.; writing—original draft preparation, T.K., P.L., R.S. and V.C.; writing—review and editing, P.L.; visualization, P.L.; supervision, T.K., P.L. and R.S.; project administration, T.K. and P.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Ethical review and approval were waived for this study. The study employed an anonymous, non-interventional questionnaire survey involving adult participants. The research did not collect any sensitive personal information and strictly adhered to principles of data confidentiality and anonymity.

Informed Consent Statement: Informed consent was obtained from all participants. The online questionnaire included an introductory section outlining the purpose of the study, voluntary participation, anonymity, and data confidentiality. Participants indicated their consent by continuing with the survey.

Data Availability Statement: The data supporting the findings of this study are available from the first or corresponding author upon reasonable request.

Acknowledgments: The authors extend their sincere gratitude to Pathumthani University and Rangsit University for their invaluable support and encouragement throughout the research process. The institutions' academic resources, collaborative environment, and unwavering commitment to scholarly excellence significantly contributed to the successful completion of this study. During the preparation of this manuscript, the authors utilized the GPT-4o model to assist with language refinement and optimization of select sections. All content was subsequently reviewed and revised by the authors, who assume full responsibility for the final version of this publication.

Conflicts of Interest: The authors declare no conflicts of interest.

References

Abah, J. A., & Agada, P. I. (2025). Students' vulnerability to cybercrime: Implications for cybersecurity in the Global South. *International Journal of Didactic Mathematics in Distance Education*, *2*(2), 141–164. [CrossRef]

Ahmad, M. S., Musa, N. E., Nadarajah, R., Hassan, R., & Othman, N. E. (2013, July 1–4). *Comparison between Android and iOS operating system in terms of security*. 2013 8th International Conference on Information Technology in Asia (CITA) (pp. 1–4), Kota Samarahan, Malaysia. [CrossRef]

Alex-Omiogbemi, A. A., Sule, A. K., Omowole, B. M., & Owoade, S. J. (2024). Advances in cybersecurity strategies for financial institutions: A focus on combating e-channel fraud in the digital era. *Finance & Accounting Research Journal*, *6*(12), 2208–2219. [CrossRef]

Arenas, Á., Ray, G., Hidalgo, A., & Urueña, A. (2024). How to keep your information secure? Toward a better understanding of users security behavior. *Technological Forecasting and Social Change*, *198*, 123028. [CrossRef]

Arof, K. Z. M., Ismail, S., & Saleh, A. L. (2018). Contractor's performance appraisal system in the Malaysian construction industry: Current practice, perception and understanding. *International Journal of Engineering and Technology*, *7*(3.9), 46–51. [CrossRef]

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. [CrossRef]

Burke, J., Kieffer, C., Mottola, G., & Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud? *Journal of Economic Behavior & Organization*, *198*, 250–266. [CrossRef]

Buse, J. H., Fong, C., & Tripathi, S. (2024). The interplay of social behaviour and demographics in cyber scam susceptibility: A Singapore study. *Open Journal of Business and Management*, *12*(5), 2949–2964. [CrossRef]

Chatla, S. B., & Shmueli, G. (2017). An extensive examination of regression models with a binary outcome variable. *Journal of the Association for Information Systems*, *18*(4), 340–371. [CrossRef]

Chayanon, S., Phoraksa, T., & Thitalampoon, S. (2025). Digital deception: Exploring the societal vulnerabilities to online scams and fraud. *Dhammathas Academic Journal*, *25*(1), 357–370.

Choi, K. S., Choo, K., & Sung, Y. E. (2016). Demographic variables and risk factors in computer-crime: An empirical assessment. *Cluster Computing*, *19*, 369–377. [CrossRef]

Chusong, W., Kanyajit, S., & Poonyarith, S. (2024). Preventing victims of online shopping fraud in Thai teenagers: A case study of Bangkok. *Suan Dusit Graduate School Academic Journal*, *20*(3), 107–121.

Costantini, M., Meco, I., & Paradiso, A. (2017). Do inequality, unemployment and deterrence affect crime over the long run? *Regional Studies*, *52*(4), 558–571. [CrossRef]

Dadà, C. B., Colautti, L., Rosi, A., Cavallini, E., Antonietti, A., & Iannello, P. (2025). Uncovering vulnerability to fraud and scams among adult victims in online and offline contexts: A systematic review. *Computers in Human Behavior*, *172*, 108734. [CrossRef]

D'Amato, A., & Mastrolia, E. (2023). The control of risk in financial decisions: Illusion or reality? *International Journal of Behavioural Accounting and Finance*, *7*(1), 41–54. [CrossRef]

Dangpisan, T. (2025). The impact of call center gangs on Thailand's economy: Financial losses and psychological damage. *Thai Social Science Journal*, *2*(2), 15–27.

Datta, P. M., Acton, T., & Carroll, N. (2022, April 25). *Penny wise, pound foolish: An experimental design of technology trust amongst organizational users*. 2022 Cyber Research Conference-Ireland (Cyber-RCI) (pp. 1–4), Galway, Ireland. [CrossRef]

Ebner, N. C., Pehlivanoglu, D., & Shoenfelt, A. (2023). Financial fraud and deception in aging. *Advances in Geriatric Medicine and Research*, *5*(3), e230007. [CrossRef] [PubMed]

Freed, D., Bazarova, N., Consolvo, S., Cosley, D., & Gage Kelley, P. (2025). PROTECT: A framework to foster digital resilience for youth navigating technology-facilitated abuse. *Social Sciences*, *14*(6), 378. [CrossRef]

Goud, N. (n.d.). *Educated people becoming prime targets to cyber frauds*. Cybersecurity Insiders. Available online: https://www.cybersecurity-insiders.com/educated-people-becoming-prime-targets-to-cyber-frauds/ (accessed on 2 September 2025).

Griffith, C. E., Tetzlaff-Bemiller, M., & Hunter, L. Y. (2023). Understanding the cyber-victimization of young people: A test of routine activities theory. *Telematics and Informatics Reports*, *9*, 100042. [CrossRef]

Grigorescu, A., Alistar, T. V., & Lincaru, C. (2025). Digital skills, ethics, and integrity—The impact of risky internet use, a multivariate and spatial approach to understanding NEET vulnerability. *Systems*, *13*(8), 649. [CrossRef]

Henkenjohann, R., & Trenz, M. (2022). Risk compensation behaviors on cascaded security choices. In *WISP 2022 proceedings*. Available online: https://aisel.aisnet.org/wisp2022/5 (accessed on 2 September 2025).

Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior*, *29*(2), 129–156. [CrossRef]

Holmarsdottir, H. (2024). The digital divide: Understanding vulnerability and risk in children and young people's everyday digital lives. In H. Holmarsdottir, I. Seland, C. Hyggen, & M. Roth (Eds.), *Understanding the everyday digital lives of children and young people*. Palgrave Macmillan. [CrossRef]

Hossain, M. A., Islam, S., Rahman, M. M., & Arif, N. U. M. (2024). Impact of online payment systems on customer trust and loyalty in e-commerce analyzing security and convenience. *Academic Journal on Science, Technology, Engineering & Mathematics Education*, *4*(3), 1–15.

Jimmy, F. (2024). Cybersecurity threats and vulnerabilities in online banking systems. *International Journal of Scientific Research and Management*, *12*(10), 1631–1646. [CrossRef]

Kandpal, V., Ozili, P. K., Jeyanthi, P. M., Ranjan, D., & Chandra, D. (2025). Digital finance: An overview. *Digital Finance and Metaverse in Banking*, 1–32. [CrossRef]

Kavvadias, A., & Kotsilieris, T. (2025). Understanding the role of demographic and psychological factors in users' susceptibility to phishing emails: A review. *Applied Sciences*, *15*(4), 2236. [CrossRef]

Kellner, A., Horlboge, M., Rieck, K., & Wressnegger, C. (2019, June 17–19). *False sense of security: A study on the effectivity of jailbreak detection in banking apps*. 2019 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 1–14), Stockholm, Sweden. [CrossRef]

Koch, T., Laaber, F., & Florack, A. (2024). Socioeconomic status and young people's digital maturity: The role of parental mediation. *Computers in Human Behavior*, *154*, 108157. [CrossRef]

Kollnig, K., Shuba, A., Binns, R., Van Kleek, M., & Shadbolt, N. (2022). Are iPhones really better for privacy? A comparative study of iOS and Android apps. In *Proceedings on privacy enhancing technologies* (pp. 6–24). De Gruyter. [CrossRef]

Koning, L., Junger, M., & Veldkamp, B. (2024). Risk factors for fraud victimization: The role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge. *International Review of Victimology*, *30*(3), 443–479. [CrossRef]

Lazarus, S., Tickner, P., & McGuire, M. R. (2025). Cybercrime against senior citizens: Exploring ageism, ideal victimhood, and the pivotal role of socioeconomics. *Security Journal*, *38*, 42. [CrossRef]

Lerdloompheephan, P. (2024). Computer security and crime digital and transaction risks affecting digital technology acceptance of generation X consumer in Bangkok Metropolis. *Journal of Humanities and Social Sciences Thonburi University*, *18*(2), 106–120.

Lertsatitpirote, K., & Kanyajit, S. (2023). Causes and types of online fraud victimization in Thailand. *International Journal of Criminal Justice Sciences*, *18*(2), 387–400.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. [CrossRef]

Lunn, S. (2024). Data privacy in online transactions: Balancing security and convenience. *Journal of Internet Banking and Commerce*, *29*(3), 1–4.

Ly, R., & Ly, B. (2024). Digital payment systems in an emerging economy. *Computers in Human Behavior Reports*, *16*, 100517. [CrossRef]

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*, 1224168. [CrossRef]

Maini, R. N., & Sindhi, V. K. (2025). Digital banking fraud in India: Typologies, victim behaviour, and AI-enabled risk governance in a global context. *International Journal for Multidisciplinary Research*, *7*(5), 1–10. [CrossRef]

Malik, A. S., Acharya, S., & Humane, S. (2024). Exploring the impact of security technologies on mental health: A comprehensive review. *Cureus*, *16*(2), e53664. [CrossRef]

Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime victimization and problematic social media use: Findings from a nationally representative panel study. *American Journal of Criminal Justice*, *46*(6), 862–881. [CrossRef] [PubMed]

Maskall, P. (2017, January 23–25). *Risk and digital security: The perception versus reality and the cognitive biases of online protection*. International Conference on Economic Sciences and Business Administration (Vol. 4, pp. 280–287), Phuket, Thailand. Available online: https://icesba.eu/RePEc/icb/wpaper/ICESBA2017_Maskall_p280-287.pdf (accessed on 2 September 2025).

Mwiraria, D., Ngetich, K., & Mwaeke, P. (2024). Exploring individual factors associated with the prevalence of cybercrime victimization among students at Egerton University, Kenya. *European Journal of Humanities and Social Sciences*, *4*(5), 35–40. [CrossRef]

Nwoke, J. (2024). Digital transformation in financial services and fintech: Trends, innovations and emerging technologies. *International Journal of Finance*, *9*(6), 1–24. [CrossRef]

Odufisan, O. I., Abhulimen, O. V., & Ogunti, E. O. (2025). Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria. *Journal of Economic Criminology*, *7*, 100127. [CrossRef]

Oroșanu, M. A., & Alexandru, M. (2024, November 13–15). *Cybercrime: A new challenge of criminality in the digital age*. International Conference on Cybersecurity and Cybercrime (Vol. 11, pp. 115–121), New Delhi, India. [CrossRef]

Padyab, M., Padyab, A., Rostami, A., & Ghazinour, M. (2024). Cybercrime in Nordic countries: A scoping review on demographic, socioeconomic, and technological determinants. *SN Social Sciences*, *4*, 205. [CrossRef]

Parmar, P., Yogesh, M., Damor, N., Gandhi, R., & Parmar, B. (2024). Beyond the screen: Examining the associations between cyberbullying, social media addiction, and mental health outcomes among medical students: A cross-sectional study. *Indian Journal of Psychiatry*, *66*(7), 641–648. [CrossRef]

Phuangsuwan, P., Limna, P., & Siripipatthanakul, S. (2024). Ethics in the social sciences research. *Advance Knowledge for Executives*, *3*(4), 1–11. Available online: https://www.researchgate.net/publication/394223864 (accessed on 9 September 2025).

Phuangsuwan, P., Siripipatthanakul, S., Siripipattanakul, S., & Jaipong, P. (2025). The impact of community participation in sustainable learning resource development: A case of Bangkok, Thailand. *Sustainability*, *17*(10), 4620. [CrossRef]

Pituk, P., Chutipattana, N., Laor, P., Sukdee, T., Kittikun, J., Jitwiratnukool, W., Fajriyah, R., & Saisanan Na Ayudhaya, W. (2025). Digital media victimization among older adults in upper-southern Thailand. *Informatics*, *12*(1), 24. [CrossRef]

Puente, S. M., & Hernández, I. N. R. (2022). Cyber victimization within the routine activity theory framework in the digital age. *Revista de Psicología*, *40*(1), 265–291. [CrossRef]

Sharma, D., Tomar, G. S., & Jha, A. (Eds.). (2025). *Artificial intelligence for cyber security and industry 4.0* (1st ed.). CRC Press. [CrossRef]

Sharma, P. (2024). Algorithms and strategies for fraud prevention on online platforms. *World Journal of Advanced Research and Reviews*, *23*(02), 2220–2225. [CrossRef]

Shi, X., He, J., & Niu, G. (2024). The association between family socioeconomic status and children's digital literacy: The explanatory role of parental mediation. *Adolescents*, *4*(3), 386–395. [CrossRef]

Sirawongphatsara, P., Pornpongtechavanich, P., Sriamorntrakul, P., & Daengsi, T. (2024). Exploring bank account information of nominees and scammers in Thailand. *Bulletin of Electrical Engineering and Informatics*, *13*(6), 4439–4450. [CrossRef]

Sugiharti, L., Purwono, R., Esquivias, M. A., & Rohmawati, H. (2023). The nexus between crime rates, poverty, and income inequality: A case study of Indonesia. *Economies*, *11*(2), 62. [CrossRef]

Teerapunyachai, B., & Bawornkitchaikul, Y. (2024). Innovations and resilience in Thailand's payment ecosystem: A comprehensive analysis—Connectivity initiatives, challenges and solutions. *Journal of Digital Banking*, *9*(1), 67–85. [CrossRef]

The Nation. (2025, February 10). *Millions of Thais fall victim to online scams*. The Nation Thailand. Available online: https://www.nationthailand.com/news/general/40046127 (accessed on 2 September 2025).

Tripathi, R., & Tripathi, S. (2024). Frauds and cyber security issues in the finance sector. In G. Malik, G. Malik, & S. Aggarwal (Eds.), *Transforming the financial landscape with ICTs* (pp. 165–189). IGI Global Scientific Publishing. [CrossRef]

Uakarn, C., Chaokromthong, K., & Sintao, N. (2021). Sample size estimation using Yamane and Cochran and Krejcie and Morgan and green formulas and Cohen statistical power analysis by G* Power and comparisons. *APHEIT International Journal of Interdisciplinary Social Sciences and Technology*, *10*(2), 76–88.

Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The role of big data in detecting and preventing financial fraud in digital transactions. *World Journal of Advanced Research and Reviews*, *22*(2), 1746–1760. [CrossRef]

Ungratwar, S., Sharma, D., & Kumar, S. (2025). Mapping the digital banking landscape: A multi-dimensional exploration of fintech, digital payments, and e-wallets, with insights into current scenarios and future research. *Humanities and Social Sciences Communications*, *12*, 1064. [CrossRef]

Wang, D., Duan, Y., & Jin, Y. (2025). Navigating online perils: Socioeconomic status, online activity lifestyles, and online fraud targeting and victimization of old adults in China. *Computers in Human Behavior*, *162*, 108458. [CrossRef]

Warokka, A., Setiawan, A., & Aqmar, A. Z. (2025). Key factors influencing fintech development in ASEAN-4 countries: A mediation analysis. *FinTech*, *4*(2), 17. [CrossRef]

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 105–109. [CrossRef] [PubMed]

Whitty, M. T. (2025). A systematic literature review of profiling victims of cyber scams: Setting up a framework for future research. *Cogent Social Sciences*, *11*(1), 2563781. [CrossRef]

Yoganandham, G., & Govindaraj, A. (2024). Emerging trends in digital fraud with a focus on the rising threat of malicious applications, exploitative loan financing, and payment manipulation in privacy, security and consumer trust—A theoretical assessment. *Science, Technology and Development*, *13*(12), 43–60.

Youn, S., & Lee, M. (2009). The determinants of online security concerns and their influence on e-transactions. *International Journal of Internet Marketing and Advertising*, *5*(3), 194–222. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.