Advanced International Journal of Business, Entrepreneurship and SME's
EISSN: 2682-8545
AIJBES
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

ADVANCED INTERNATIONAL JOURNAL OF BUSINESS, ENTREPRENEURSHIP AND SMES (AIJBES)
www.aijbes.com

WHAT LEADS TO ONLINE FINANCIAL FRAUD VICTIMIZATION AMONG CONSUMERS: AN EMPIRICAL ANALYSIS

Mohammad Tahir Zainuddin[1*], Wan Nur Fazni Wan Mohamed Nazarie[2], Natasya Aina Abdul Khadir[3]

[1] Faculty of Economics and Muamalat, Universiti Sains Islam Malaysia, Malaysia
Email: tahir@usim.edu.my
[2] Faculty of Economics and Muamalat, Universiti Sains Islam Malaysia, Malaysia
Email: fazni@usim.edu.my
[3] Faculty of Economics and Muamalat, Universiti Sains Islam Malaysia, Malaysia
[*] Corresponding Author

Article Info:

Article history:
Received date: 27.10.2025
Revised date: 17.11.2025
Accepted date: 10.12.2025
Published date: 23.12.2025

To cite this document:

Zainuddin, M.T., Nazarie, W. N. F. W. M., & Abdul Kadir, N. A. (2025). What Leads to Online Financial Fraud Victimization Among Consumers: An Empirical Analysis. *International Journal of Business Entrepreneurship and SMEs, 7* (26), 372-390.

DOI: 10.35631/AIJBES.726026

Abstract:

The widespread adoption of digital technologies has enhanced modern life but simultaneously fuelled a surge in online financial fraud, generating severe socio-economic repercussions. Fraud, defined as intentional deception for personal gain, now represents a global phenomenon that undermines trust in financial systems. In Malaysia, the National Scam Response Centre (NSRC) documented 33,234 scam cases in 2023 with losses amounting to RM1.34 billion. By 2024, reported cases increased to 35,368, resulting in losses of RM1.58 billion, while in the first quarter of 2025 alone, consumers lost RM573.7 million to various online scams. This study investigates the underlying factors leading to fraud victimization among Malaysian consumers. Employing a quantitative survey with 267 respondents analysed through SPSS, the research identifies four primary predictors: poor knowledge, low self-control, financial pressure, and bad/ risky routine activities. Findings provide valuable insights for policymakers and financial institutions in designing targeted interventions to reduce victimization and strengthen consumer resilience.

Keywords:

Consumers, Online Financial Fraud, Victimization, Malaysia, SPSS Analysis

Introduction

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

Digital connectivity has reshaped communication, commerce, and financial services, but it has also expanded opportunities for financial crime. Recent evidence shows that fraud is now a major operational threat rather than a peripheral concern. The PwC Malaysia edition of the Global Economic Crime and Fraud Survey reports that asset misappropriation, corruption, customer fraud, and cyber-enabled attacks accounted for roughly 70% of recorded incidents, highlighting their severity (PwC Malaysia, 2025). Similar international findings indicate that fraud and cybercrime remain the most disruptive risks, particularly in highly digital environments. Fraud arises both internally, through staff misconduct and weak controls, and externally via organized syndicates exploiting institutional or consumer vulnerabilities (Mokhtar & Rohaizat, 2024). Industry research stresses the need for layered defenses, combining advanced analytics for anomaly detection, strong compliance structures, and consumer education to reduce exposure (Ilori et al., 2024). These measures help institutions identify suspicious behavior quickly without burdening legitimate users. Malaysia's rapid digital adoption makes it an illustrative case. By 2023, over 96.8% of the population had internet access (Bank Negara Malaysia, 2025; OECD, 2020), expanding opportunities for commerce as well as fraud. In the first half of 2024 alone, authorities recorded 14,490 online fraud cases with losses nearing RM581 million (Zhi et al., 2025). These crimes range from phishing and malware to deceptive investment and e-commerce schemes. Regulatory responses have grown more assertive. Bank Negara Malaysia has pushed for device-bound or app-based authentication and the phasing out of SMS OTPs due to risks such as SIM swapping and OTP harvesting (Bank Negara Malaysia, 2025). Yet technology alone cannot contain evolving threats, as scammers continually refine malware, phishing kits, and social engineering tactics (Shete et al., 2024). Public awareness initiatives by banks, regulators, and law enforcement therefore remain essential, though research shows that awareness must be reinforced by systemic protections such as device binding and transaction monitoring (Kumar et al., 2024).

Problem Statement

Since threat actors are using AI-driven technologies to automate and adapt attacks at scale, combating online financial fraud has become increasingly important in 2024 and 2025. Recent findings show that generative AI has been weaponized to craft highly convincing phishing messages and deepfake content, which significantly increases the success rate of social engineering attacks (Cybersecurity Malaysia, 2024). In Malaysia, fraud cases involving impersonation and scam calls using AI-generated voices surged by 38% in the first half of 2024, prompting renewed calls for real-time verification mechanisms and tighter regulation of digital identity technologies (Bernama, 2024). Moreover, cybercriminals are no longer operating in isolation but through well-organized transnational syndicates that exploit jurisdictional gaps, making enforcement and prosecution more complex (Interpol, 2025). As fraud vectors evolve, traditional perimeter-based security models are proving inadequate, highlighting the need for zero-trust architectures and proactive monitoring. Concurrently, regulatory bodies and financial institutions in 2025 have escalated efforts to create a fraud-resilient financial ecosystem. Bank Negara Malaysia introduced enhanced digital banking guidelines mandating fraud risk management frameworks that integrate behavioural biometrics, device fingerprinting, and AI-led risk scoring to detect suspicious activity in real-time (Bank Negara Malaysia, 2025). These measures reflect a growing recognition that reactive controls are insufficient in high-speed digital environments. However, even with these advancements, the gap between fraud detection and prevention persists, especially in smaller financial institutions and fintech startups that may lack the resources to implement advanced systems (PwC Malaysia, 2025). Additionally, new fraud typologies, such as synthetic identity

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026
fraud and mule account rings, are emerging faster than institutions can adapt, underscoring the importance of sector-wide intelligence sharing, agile regulatory responses, and continuous innovation in fraud deterrence strategies.

Literature Review

Fraud is broadly defined by the U.S. Department of Justice (2020) as intentional deception involving misrepresentation of products, services, or financial benefits. Its scope is wide-ranging, covering traditional offline scams as well as technologically mediated schemes that exploit both systemic weaknesses and human vulnerabilities. In recent years, fraud has become increasingly complex and adaptive, with perpetrators leveraging emerging technologies, social engineering techniques, and global interconnectedness to design schemes that are difficult to detect, trace, and prosecute (Button et al., 2024). Common manifestations include phishing, identity theft, romance scams, online marketplace frauds, cryptocurrency-related investment scams, loan frauds, and increasingly sophisticated business email compromise attacks (Europol, 2020). Each of these reflects not only the creativity of fraudsters but also their ability to exploit regulatory loopholes and psychological predispositions of victims.

The rise of fraud is a global concern. In Malaysia, in the first half of 2025 alone saw financial losses from online scams reaching RM1.12 billion signalling the convergence of two forces: the rapid adoption of digital banking and e-commerce platforms, and the parallel evolution of fraud techniques targeting less digitally literate populations (The Star, 2025; Bank Negara Malaysia, 2025). Looking into historical perspectives, according to reports, 13,000 complaints of cybercrime involving losses above RM539 million were filed in 2019. In 2020, 17,000 cases were documented. Nearly 20,000 incidents occurred in 2021, with a total loss of RM560 million. 3,273 events with RM114 million in damages were reported up till February 2022, (Muharram et al., 2022). This reflects global trends: according to Interpol (2025), cyber-enabled fraud ranks among the fastest-growing financial crimes worldwide, while the United Nations Cybercrime Convention (UNCC) highlights its role in transnational organized crime networks (Interpol, 2025). In Europe, it was documented a surge in online scams targeting both consumers and businesses, while the U.S. Federal Trade Commission (FTC) recorded over $10 billion in fraud losses in 2022 alone, the highest annual total on record (Europol, 2020; FBI, 2020).

The economic and social consequences of fraud are substantial (Levi & Smith, 2022; PwC Malaysia, 2025; U.S. Department of Justice, 2020). Beyond direct financial losses, fraud undermines public confidence in digital platforms, banking systems, and regulatory institutions, which in turn hinders digital transformation agendas in many economies (Button et al., 2022). Victims often experience emotional distress, shame, and in severe cases, deteriorating mental health. On a societal level, large-scale fraud places pressure on law enforcement agencies, drains financial institutions' resources through compliance and security costs, and compels governments to enact stronger consumer protection regulations (Button et al., 2022; Asher, 2025; PwC Malaysia, 2025). Fraud, therefore, is not merely a criminal issue but also a socio-economic and psychological one (Zainuddin, 2016).

Given these realities, understanding the psychological, social, and behavioral antecedents of fraud victimization has become an essential scholarly pursuit. Previous research identifies several recurring risk factors that explain why some populations are disproportionately vulnerable. Insufficient knowledge and financial literacy are commonly recognized as

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

significant factors in digital situations where consumers frequently fail to spot fraudulent indicators (Zheng et al., 2024). People who are unable to comprehend financial jargon or see offers that seem too good to be true, for example, may be the target of scams involving loan products or investments (Singh & Misra, 2023). The elderly, those with low incomes, and those with limited access to digital education are disproportionately affected by gaps in financial literacy (Czech et al., 2024). Another well-researched antecedent as a behavioral propensity is poor self-control. According to the general theory of crime, people who lack self-control are more likely to engage in risky or harmful activities, making them more susceptible to victimization (Kwak & Kim, 2022). Real research in the realm of fraud supports this association. Ngo et al., (2024) showed that a lack of self-control is associated with a higher likelihood of falling victim to consumer fraud, whereas Hernandez & Cruz (2025) discovered similar relationships in Macau. More recent studies expand this to online fraud contexts, showing that personality, individual characteristics, behaviour, cognition, self-esteem, and attitudes/ beliefs correlate with cyber scam victimizations (Whitty, 2025).

Financial pressure is another critical determinant. Economic strain resulting from unemployment, debt, or inflationary environments creates conditions where individuals are more motivated to take risks, making them susceptible to scams promising quick financial relief (Nasruddin et al., 2024). Fraudsters exploit this desperation by offering fraudulent investment schemes, fake job opportunities, or predatory loans. The COVID-19 pandemic intensified such pressures globally, with fraudsters capitalizing on financial aid programs and stimulus packages to target vulnerable households (Ahmad, 2025; Levi & Smith, 2022; Jamil et al., 2022).

In another perspective, equally important are bad/ risky routine activities, derived from routine activity theory, which explains victimization as a product of daily lifestyle patterns that bring individuals into contact with motivated offenders in the absence of capable guardians (Wambugu et al., 2024). Studies in cybercrime contexts illustrate that individuals who spend more time engaging in unregulated online activities, such as gambling, online dating, or unverified e-commerce, are disproportionately exposed to fraudulent schemes (Bar Lev et al., 2022; Kwak & Kim, 2022; Xu et al., 2024). For example, it demonstrated that excessive online presence, combined with weak cybersecurity practices, heightens susceptibility to phishing and identity theft. Strengthening financial literacy, promoting digital resilience, addressing socio-economic inequalities, and encouraging safer online practices could significantly reduce victimization risks (Abdul Jamal, 2022; Ahmad, 2025; Antipova & Riurean, 2025; Ogunola et al., 2024).

Based on literature discussions, thus, these four constructs underpin the present research framework.

Key Risk Factors

There are four major risk factors identified:

Poor Knowledge

Poor knowledge, especially limited financial literacy and gaps in digital skills, continues to make people more vulnerable to deception. Newer research shows that older adults are disproportionately affected: age-related cognitive decline, including reductions in working memory and brain structural integrity, correlates with increased vulnerability to phishing and

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

scam susceptibility even among those without clinically diagnosed cognitive impairment (Lamar et al., 2024). Scam susceptibility has also been shown to predict earlier onset of Alzheimer's dementia, one study found that older people with high scam susceptibility developed Alzheimer's disease approximately seven years earlier than those with low susceptibility (Boyle et al., 2025). However, younger adults are not immune. A report in 2025 found that about 82.9% of people aged 16–29 have been tricked at least once by suspicious links in messages, often due to impulsive clicking and weak scrutiny rather than lack of technical access or familiarity (Klutsch et al., 2025). Encouragingly, education interventions are showing promise. Among older adults (60+), video-based anti-fraud education significantly outperforms text-based material on measures of comprehension, emotional engagement, and intent to resist fraud (Zhou et al., 2025). Also, how prevention advice is delivered matters: older adults, especially those over 75, respond more positively when the medium matches their preferences and when messages are disseminated via trusted channels (Button et al., 2024). Victims frequently fail to report fraud incidents due to embarrassment, social stigma, or lack of awareness about appropriate reporting mechanisms. This underreporting not only hinders accurate statistics but also perpetuates the cycle of victimization, as fraudsters remain undetected. Recent studies in developing countries such as China, India and Nigeria suggest that the gap between fraud experience and reporting is particularly wide, with more than 60% of victims never seeking legal or institutional recourse (Bar Lev et al., 2022). Moreover, poor knowledge is not limited to individuals but also reflects systemic gaps in consumer protection policies, financial education programs, and digital governance frameworks. Research highlights that countries with comprehensive financial literacy campaigns record significantly lower levels of fraud victimization (Singh & Misra, 2023). Thus, improving knowledge at both the individual and institutional level is vital in mitigating fraud risk.

H1: Poor Knowledge Increases the Likelihood of Financial Fraud Victimization.

Low Self-Control

A thorough definition of self-control is the capacity to suppress cravings, delay pleasure, and pursue long-term goals in the face of present temptations (Hofmann, 2024). People who lack self-control are far more susceptible to dishonesty since they are more likely to make snap decisions (Ong, 2022). A lack of self-control is directly linked to risk-taking and giving in to peer pressure, both of which raise the chance of fraud, according to previous research (Kwak & Kim, 2022). The problem is particularly serious in developing countries. Impulsivity and an incorrect belief in unproven financial potential increase vulnerability, especially in environments with less stringent consumer protection laws, claim Bar Lev et al. (2022). This is consistent with research conducted in Malaysia, where scam investment schemes have disproportionately targeted people looking to make quick money (Bank Negara Malaysia, 2025). Additionally, cognitive biases including optimism bias, overconfidence, and trust heuristics frequently combine with a lack of self-control to increase the likelihood that someone would become a victim of fraud. Cross-cultural studies demonstrate that self-control is influenced by socioeconomic conditions in addition to being a psychological feature. Individuals who are socially or financially insecure frequently lack self-control, leading to more hasty financial decisions (Hernandez & Cruz, 2025).

Therefore, to help people with poor self-control, fraud prevention techniques should incorporate behavioral treatments like nudges and digital safeguards.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

H2: Low Self-Control Increases the Likelihood of Financial Fraud Victimization.

Financial Pressure

Financial stress, caused by debt, unemployment, or inflation, compels individuals toward irrational financial decisions and heightened risk-taking. Jouali et al., (2024) notes that financial distress weakens decision-making capacity, reducing the ability to scrutinize financial offers. Fraudsters are adept at exploiting such desperation, particularly during times of crisis. The COVID-19 pandemic, for instance, witnessed a global surge in fraudulent schemes promising quick returns or emergency relief, targeting those most economically strained (Bar Lev et al., 2022). Recent data from global sources indicate that financial insecurity is one of the strongest predictors of victimisation in digital financial fraud, especially in developing economies (Bar Lev et al., 2022). In Malaysia, scams related to emergency loans, job opportunities, and fake aid programs were reported to have spiked during and after the pandemic (Jamil et al., 2022). Beyond individual desperation, financial pressure can create systemic vulnerabilities. For instance, families experiencing sustained economic hardship may normalize risky behaviours such as borrowing from unverified sources or investing in unregulated platforms (McCoy, 2025). These coping strategies, while intended for survival, inadvertently increase exposure to fraudulent networks.

H3: Financial Pressure Increases the Likelihood of Financial Fraud Victimization.

Bad Routine Activity

Routine activity theory posits that crime occurs when motivated offenders converge with vulnerable targets in the absence of capable guardianship (Reynald, 2016). In the context of financial fraud, bad/ risky digital habits act as routine activities that increase exposure to motivated offenders. Such behaviours include oversharing personal information on social media, engaging with unsolicited online offers, downloading unverified applications, or clicking on unknown links (Kwak & Kim, 2022). The digitalization of daily life has intensified opportunities for fraud. A study by Europol (2020) highlighted that phishing, identity theft, and fraudulent online transactions surged significantly during the pandemic, as individuals spent more time online. Malaysia recorded 195,032 phishing cases in early 2022 alone, indicating the scale of the problem (Franceschini et al., 2025). Younger people are paradoxically more exposed since they use the internet more frequently and partake in riskier online behaviors, even while they are more tech-savvy (Carcelén et al., 2023). Additionally, the effectiveness of capable guardianship, which encompasses institutional safeguards, cybersecurity knowledge, and regulatory oversight, is essential. Lax enforcement, a lack of digital safety training, and ignorance of cyber hygiene practices create an environment that is conducive to fraud (Kumar et al., 2024). Therefore, just as much of the reason for cyber-enabled fraud as personal carelessness are institutional inability to provide appropriate digital guardianship.

H4: Bad Routine Activities Increase the Likelihood of Financial Fraud Victimization.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

The Research Framework

Four independent variables are included in this study as predictors of Financial Fraud Victimization: Poor Knowledge, Low Self-Control, Financial Pressure, and Bad Routine Activity (Refer Figure 1).

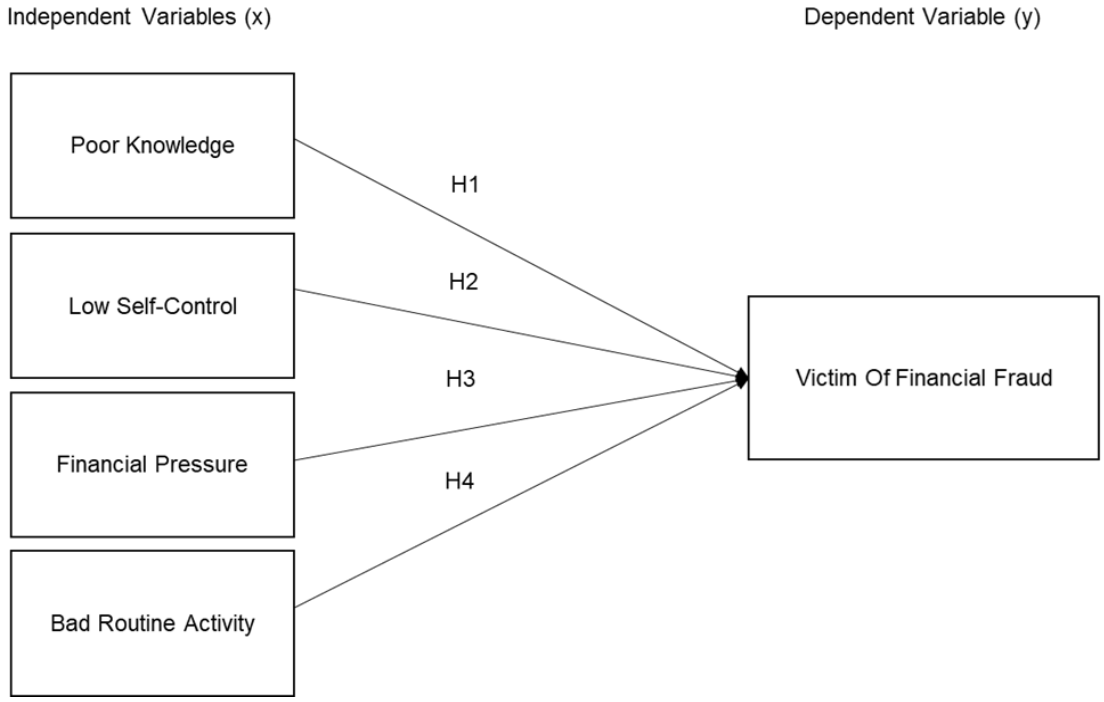

Figure 1: The Research Framework

Source: This Study.

Methodology

As part of a quantitative design, structured questionnaires were distributed via Instagram, Telegram, and WhatsApp (Creswell & Creswell, 2017). The instrument looked at demographics, independent variables (12 items), and dependent variables (4 items) using a seven-point Likert scale. Using SPSS, data from 267 respondents were subjected to descriptive analysis, regression, hypothesis testing, and reliability testing (Cronbach's alpha). Secondary sources, including reputable articles and journals, provided support for the findings.

Results

Reliability Analysis

A crucial first step in guaranteeing the precision and dependability of the measuring tools used in a study is reliability analysis. Cronbach's alpha remains the most widely used statistical technique for evaluating internal consistency, especially when a study instrument uses a lot of Likert-scale questions to measure latent variables (Cheung et al., 2024). Cronbach's alpha coefficients are used to quantify internal dependability, they have a range of 0 to 1. According to Nunnally and Bernstein (1994), an alpha value of 0.70 or above is typically considered sufficient for social science research, values above 0.80 are considered good, and those above 0.90 suggest remarkable dependability. All of the study's constructs met or beyond the reliability criterion, according to Cronbach's alpha calculations, suggesting that the survey

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

items were internally consistent and dependable in capturing the intended dimensions. The specific results are shown in Table 1.

Table 1: Reliability Analysis

Constructs	Cronbach's Alpha	Number of Items
Fraud Victimization	.850	4
Poor Knowledge	.900	3
Low Self-Control	.910	3
Financial Pressure	.871	3
Bad Routine Activity	.857	3

Source: This Study.

The dependent variable, the Fraud Victimization construct, was examined using four items, and the Cronbach's alpha was 0.850. This implies that participants' impressions of fraudulent interactions were consistently captured by the highly dependable items included. A high level of internal consistency is particularly important in this case because fraud victimization is often a complex term having behavioral, psychological, and financial components. The assessment items in these categories are guaranteed to fairly represent the variety and complexity of victimization experiences when they are trustworthy (Daigle et al., 2016).

The three-item Poor Knowledge construct had a Cronbach's alpha of 0.900. This is considered "excellent," meaning that the elements conveyed the notion of having little awareness or understanding of financial operations and fraud concerns in a way that was closely related. In line with the findings of Cheung et al. (2024), high alpha values show that items considerably converge on the underlying latent trait.

The Low Self-Control construct demonstrated the highest reliability among all constructs, with a Cronbach's alpha of 0.910 across three items. This suggests that the items used to measure impulsivity, inability to resist temptation, and lack of restraint in financial decision-making were extremely consistent. Revicki (2024) argued that such high reliability is valuable for behavioural constructs, as it reduces measurement error in psychological dimensions.

With Cronbach's alpha of 0.871, the three-item Financial Pressure measure showed good internal consistency. This implies that the instrument was helpful in identifying the requirements and constraints that participants face when handling debt, financial obligations, or a limited income. Since financial stressors significantly influence people's inclination to make dangerous financial decisions, it is imperative to appropriately assess them (Graham et al., 2024).

Lastly, the Cronbach's alpha for the three-item Bad Routine Activity construct was 0.857. Strong dependability is demonstrated by the questions' constant ability to capture habits and lifestyle patterns that may make a person more vulnerable to fraud victimization, such as risky or dangerous online activities or insufficient protection of personal information. Internal consistency dependability is essential in these psychological ideas to guarantee that the observed scores accurately reflect consistent activity patterns rather than random variation (Revicki, 2024).

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

According to the total Cronbach's alpha values, the instrument used in this study shows good reliability across all constructs. This increases the credibility of the subsequent research since reliable constructs ensure that the outcomes are correct representations of the underlying theoretical notions rather than the product of measurement error (Storey et al., 2025). Furthermore, the scale's design, item phrasing, and grouping were appropriate and successfully in line with the study's conceptual framework, as seen by the consistently high alphas across constructs (Lambert & Newman, 2023).

Multiple Regression Analysis

The results of the multiple regression analysis provide substantial support for the traits that predict fraud victimization in the study population. The four independent factors under investigation, poor understanding, financial pressure, bad regular behavior, and inadequate self-control, can explain nearly 76% of the variance in fraud victimization, according to the model's comparatively high explanatory power ($R^2 = 0.760$). The large quantity of explained variations suggests that the conceptual and quantitative theoretical underpinnings of the study are sound.

The significant ANOVA result ($F = 207.145$, $p < 0.001$) further underscores the reliability of the model in predicting fraud victimization, confirming that the set of predictors contributes meaningfully to explaining the outcome variable. Coefficients revealed poor knowledge ($\beta = .541$, $p < 0.001$) as the strongest predictor, followed by financial pressure ($\beta = .185$, $p < 0.001$), bad routine activity ($\beta = .182$, $p < 0.001$), and low self-control ($\beta = .090$, $p = 0.050$). Table 2 presents the Multiple Regression Analysis.

Table 2: Multiple Regression Analysis

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	.205	.207		.990	.323	-.203	.612
	Poor_Knowledge	.556	.050	.541	11.014	.000	.457	.656
	Low_Self_Control	.083	.044	.090	1.898	.050	-.003	.169
	Financial_Pressure	.179	.046	.185	3.928	.000	.089	.269
	Bad_Routine_ Activity	.159	.033	.182	4.788	.000	.093	.224

a. Dependent Variable: Financial_Fraud_Victimization

Source: This Study.

Poor Knowledge as the Strongest Predictor

Poor Knowledge was the most significant predictor among all of them ($\beta = .541$, $p < 0.001$), highlighting the significance of consumer awareness and financial literacy in predicting fraud risk. According to Zheng et al. (2024), financial literacy directly improves consumers' capacity to identify fraudulent schemes and take precautionary action. This outcome is in line with their previous studies. Victimization is frequently made easier by inadequate knowledge, especially when it comes to digital platforms, risk assessment, and financial commodities (Ogunola et al., 2024). Lack of understanding of digital banking operations, cybersecurity measures, and

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026
contractual obligations increases one's susceptibility to manipulative tactics such phishing, investment frauds, and identity theft (Kumar et al., 2024).This outcome is also consistent with current debates regarding consumer empowerment in the digital economy, where consumers are often disadvantaged by the asymmetry of knowledge between service providers and consumers (Ogunola et al., 2024; Zheng et al., 2024; Bank Negara Malaysia, 2025; Vetrivel et al., 2025). In cultures that were digitizing quickly, such as the COVID-19 epidemic, consumers with low levels of digital literacy were disproportionately vulnerable to fraud (Button et al., 2022). In order to reduce the risk of fraud, it should be beneficial to improve consumer education through targeted awareness campaigns and integrate financial literacy into the curriculum (Vetrivel et al., 2025).

Financial Pressure and Fraud Vulnerability

Financial Pressure was the second most important predictor (β =.185, $p < 0.001$). This is consistent with economic pressure theories, which contend that people are frequently compelled to take risks due to financial difficulties (Reale et al., 2023). People who are struggling financially might be more vulnerable to predatory schemes or "too good to be true" offers that guarantee immediate financial support (Bar Lev et al., 2022; De Bruijn & Antonides, 2022; Ahmad, 2025). Research has revealed an increase in fraudulent activities amid economic downturns and unpredictability, such as inflationary cycles and the worldwide pandemic, which represent increased despair and reduced mental acuity among vulnerable groups (Levi & Smith, 2022). This conclusion is supported by behavioral finance research, which shows that a shortage of resources might hinder the capacity for critical risk assessment and logical decision-making (De Bruijn & Antonides, 2022). Psychological biases such as the sunk-cost fallacy and the scarcity effect are used by scammers to influence victims who are struggling financially (Ahmad, 2025). By providing debt counseling services, creating widely accessible microcredit networks, and guaranteeing transparent lending practices, policymakers and financial institutions could reduce these risks.

Bad Routine Activity and Fraud Exposure

The study also confirmed that routinely bad behavior is a strong predictor of being a victim of fraud (β =.182, $p < 0.001$). Routine activity theory states that when there are no capable guardians present, crime occurs when motivated criminals and appropriate targets come together (Cohen & Felson, 2015). In the digital age, when frequent online activities like social media use, online shopping, or using digital financial platforms may raise the danger of fraud attempts, this convergence is occurring more and more in cyberspace (Kumar et al., 2024). During the COVID-19 pandemic, there was a marked increase in internet-based activities, which inadvertently elevated opportunities for cybercriminals to exploit unsuspecting victims (FBI, 2020). Victims with high levels of digital routine activity often leave behind large digital footprints, enabling fraudsters to tailor scams using personal data harvested through phishing, data breaches, or social engineering (Button et al., 2024). The positive relationship between routine activity and fraud victimization observed here underscores the importance of proactive cyber hygiene practices, such as multifactor authentication, cautious information sharing, and cybersecurity awareness (Cohen & Felson, 2015; Reynald, 2016; Bank Negara Malaysia, 2025; Cybersecurity Malaysia, 2024).

Low Self-Control and Impulsivity

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

Lastly, low self-control (β = .090, p = 0.050) emerged as a statistically weaker yet still significant predictor. This result aligns with Basto et al., (2024) general theory of crime, which underscores impulsivity and risk-taking as core determinants of criminal behaviour and victimization. Individuals with diminished self-control are more likely to engage in bad/ risky financial behaviours, ignore warning signals, and succumb to fraudulent persuasion techniques (Abdul Jamal, 2022). Although its explanatory power in this model was lower compared to other variables, low self-control remains an important consideration. Prior research shows that individuals with high impulsivity are disproportionately represented among victims of online romance scams, lottery fraud, and speculative investment schemes (Nataraj, 2024). The finding here reinforces the need for psychological and behavioural interventions, such as impulse control training and financial decision-making workshops, to complement broader structural measures against fraud (Birkenmaier et al., 2022; Zhou et al., 2025).

Theoretical and Practical Implications

From a theoretical perspective, this study contributes to the literature by integrating insights from multiple criminological and behavioural theories to explain fraud victimization in a rapidly digitizing economy. It demonstrates that individual-level factors (knowledge, self-control), socio-economic conditions (financial pressure), and lifestyle routines (bad/ risky online behaviours) are interdependent rather than isolated drivers of vulnerability. This provides a more comprehensive model for understanding online fraud, offering avenues for refinement in future empirical testing. Together, these findings offer theoretical and practical insights and validate each of the study's four hypotheses. Theoretically, they provide credence to the usefulness of theories of stress, routine activity, financial literacy, and self-control in explaining fraud victimization in a digitalized financial setting. From a practical standpoint, the results demonstrate the urgent need for comprehensive preventative measures. For example, improving financial literacy can reduce vulnerability right away, while structural adjustments that tackle economic disparity can alleviate financial stress. Similarly, encouraging behavioral self-control and safe online conduct can significantly lower the likelihood of falling victim to fraud. These findings also suggest that, in addition to being a criminal justice issue, fraud should be tackled by lawmakers, banks, and regulators as a behavioral and socioeconomic issue. By addressing underlying weaknesses such as impulsive behaviors, dangerous digital habits, economic stress, and a lack of financial awareness, stakeholders can develop preventive rather than reactive solutions. Together, these strategies could significantly reduce the incidence of fraud over time.

Discussion

All four predictors, Poor Knowledge, Financial Pressure, Bad Routine Activity, and Low Self-Control, have a substantial impact on fraud victimization, according to the regression analysis. The largest significant predictor among these was poor comprehension (β =.541, p < 0.001). This study emphasizes the importance of financial literacy in giving consumers the skills and information they need to identify and thwart fraudulent schemes. People with insufficient financial education frequently exhibit the following characteristics: a lack of understanding of the dangers of investing, an overconfidence in assessing financial offers, and a vulnerability to misleading persuasion techniques (Ahmad, 2025).

In addition to making people more vulnerable to fraud, financial illiteracy also makes it more difficult for victims of fraud to recover their money (Zheng et al., 2024). Given the complexity

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

of online fraud, having a firm grasp of finance is crucial in the digital age (OECD, 2020). Therefore, previous research highlighting the need of financial competence programs and educational interventions to reduce consumer risks is supported by the strong impact of Poor Knowledge (Birkenmaier et al., 2022).

Financial Pressure (β =.185, $p < 0.001$), the second most potent predictor, highlights how financial stress significantly raises the likelihood that people may fall victim to fraudulent schemes. People may become more susceptible during difficult financial circumstances if they are promised quick financial support or investment opportunities with supposedly high returns (Dulisse et al., 2024). Economic downturns, employment insecurity, and rising living expenditures have all been linked to an increase in fraud victimization because stressed individuals are more likely to make riskier financial. In addition, scarcity, according to behavioral economics, makes people more impulsive and less capable of making rational decisions (De Bruijn & Antonides, 2022; Graham et al., 2024), which facilitates fraudsters' ability to exploit others.

For example, during the COVID-19 pandemic, fraudulent schemes targeting financially distressed households surged, demonstrating how economic stressors amplify susceptibility (Button et al., 2022). The significance of financial pressure in this study supports the argument that interventions must also focus on systemic financial stability and support structures, in addition to individual awareness campaigns (Katnic et al., 2024).

The third predictor, bad routine activity ($\beta = .182$, $p < 0.001$), aligns strongly with the Routine Activity Theory proposed by Cohen and Felson (2015). This criminological framework argues that crime occurs when motivated offenders encounter suitable targets in the absence of capable guardians. In the digital environment, increased online presence, frequent social media usage, and engagement with insecure platforms substantially increase exposure to fraudulent actors (Tyagi et al., 2024). Especially during the pandemic era, the surge in online shopping, remote work, and reliance on digital services provided fraudsters with unprecedented access to potential victims (Tasneem & Jabbar, 2024). The evidence suggests that lifestyle choices, such as using weak passwords, responding to unsolicited emails, and engaging with high-risk online spaces, increase vulnerability (Klutsch et al. 2025). The significance of this predictor demonstrates that fraud is not solely a matter of individual cognition but is also shaped by environmental exposure and situational opportunities (Holt & Bossler, 2022).

Finally, low self-control ($\beta = .090$, $p = 0.050$) also showed a significant yet weaker relationship with fraud victimization. This finding is consistent with Ngo et al., (2024), General Theory of Crime, which emphasizes impulsivity, short-term gratification, and poor decision-making as central characteristics that increase susceptibility to victimization. The importance of self-control cannot be emphasized, despite the fact that its magnitude effect was less than that of financial pressure and inadequate knowledge. People who lack self-control are more likely to take risks, make poor financial decisions, and succumb to persuasive manipulation, claim Xu et al. (2024) and Abdul Jamal (2022). Because people may not adjust or learn from past experiences, research also indicates that impulsivity has a role in victimization and recurrent victimization (Snyder & Golladay, 2024). The significance of Low Self-Control as an underlying dispositional risk factor is demonstrated by the fact that it remained when information, pressure, and routine activity were taken into consideration (Kwak & Kim, 2022).

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

When taken as a whole, these results support all four theories and show how a complex interaction of behavioral, psychological, economic, and cognitive elements shapes fraud victimization. While Financial Pressure draws attention to the structural weaknesses that make people more susceptible to fraudulent solicitations, Poor Knowledge's largest influence implies that education and awareness are crucial for fostering resistance. Routine Activity highlights the lifestyle and environmental hazards in digital environments, while Low Self-Control represents persistent personality qualities that impact vulnerability. This multi-theoretical integration is in line with new research that emphasizes fraud is caused by convergent vulnerabilities spanning situational and individual domains rather than a single vulnerability (Ahmad, 2025; Bar Lev, Maha, & Topliceanu, 2022; Whitty, 2025).

Above all, the paper contributes accurate data to ongoing discussions on preventing fraud. These findings emphasize the significance of holistic preventive methods that encompass financial education, socioeconomic support, digital safety practices, and behavioral interventions, even though traditional fraud prevention tactics often concentrate on law enforcement and deterrence. For example, focused financial literacy initiatives can help close knowledge gaps, while systemic adjustments can reduce financial strains by expanding access to social safety nets or reasonably priced loans. Behavioral training can help people develop their self-control and decision-making abilities, while public awareness campaigns regarding safe online conduct can lessen dangerous or harmful activities (Abdul Jamal, 2022; Button et.al., 2024; Zhou et al., 2025).

Recommendations

Industry-Level

The findings indicate that poor knowledge ($\beta = .541$, $p < 0.001$) is the strongest predictor of fraud victimization, highlighting the urgent need for financial institutions to go beyond basic service provision and adopt an educational and preventive role. Banks should integrate financial literacy modules into customer engagement platforms alongside forensic accounting systems and internal controls. Evidence shows that financial education reduces vulnerability to deception and improves resilience (Abdul Jamal, 2022; Birkenmaier et al., 2022; Singh & Misra, 2023; Zhou et al., 2025). Coupling AI-driven fraud detection with proactive consumer education campaigns can simultaneously address systemic fraud detection and cognitive gaps exploited by perpetrators.

Financial pressure ($\beta = .185$, $p < 0.001$) is another significant driver of victimization, requiring early-warning systems to detect financially distressed customers, such as those showing unusual borrowing or transaction patterns. Timely interventions, including restructuring advice, hardship relief, or financial counselling, can reduce risky financial decisions during downturns or crises (Jouali et al., 2024; Graham et al., 2024; Hernandez & Cruz, 2025).

Bad routine activity ($\beta = .182$, $p < 0.001$) underscores the need for secure digital environments. Institutions should strengthen cybersecurity measures, including two-factor authentication, biometric verification, and alerts for unusual online behavior (Antipova & Riurean, 2025). Low self-control ($\beta = .090$, $p = 0.050$) further supports embedding behavioral nudges in online platforms to prompt review of suspicious links, reconsider high-risk transactions, or delay impulsive decisions (Abdul Jamal, 2022; Hernandez & Cruz, 2025; Ong, 2022). Together,

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026
these measures create a multi-layered industry response aligned with the four empirically validated risk factors.

Policy-Level

Comprehensive national digital financial literacy initiatives are essential, including community outreach, workplace training, and school curricula. Policymakers should recognize that fraud prevention requires systemic solutions, such as stronger enforcement against online fraud syndicates, cross-border cooperation, and mandatory authentication for digital transactions (Wall & Williams, 2017). Dedicated hotlines and rapid reporting mechanisms should focus on financially less literate individuals who may be reluctant to self-report (Bar Lev et al., 2022; Bank Negara Malaysia, 2025). During crises, these systems should be paired with public awareness campaigns emphasizing fraud risks (Button et al., 2024).

Regulators must require robust cybersecurity protections, including encryption, antivirus use, and platform restrictions targeting high-risk channels. Multi-factor authentication and strong authentication frameworks significantly lower digital fraud risk (Holt & Bossler, 2022). Policymakers should also adopt behaviorally informed policies, such as default fraud-protection settings and delay mechanisms for high-risk transactions, reflecting the influence of low self-control (Abdul Jamal, 2022; Asher, 2025).

Ultimately, prevention programs addressing behavioral tendencies, economic vulnerabilities, risky online practices, and knowledge gaps must complement reactive enforcement. These recommendations offer a practical roadmap to reduce fraud victimization within increasingly complex financial ecosystems.

Conclusion

This study examines how personal psychology, social pressures, and everyday online habits interact to shape Malaysians' vulnerability to online financial fraud. The results show that poor financial knowledge, low self-control, rising financial pressure, and risky digital routines each heighten the likelihood of victimization, reinforcing the explanatory value of Self-Control Theory, Financial Strain Theory, and Routine Activity Theory in a digital setting.

Poor financial knowledge remains a major concern. Although mobile banking and e-payment systems are widely used, many users still lack the skills needed to distinguish legitimate transactions from fraudulent ones. Consumers often struggle to recognize phishing attempts, deceptive investment proposals, or fake e-commerce platforms. This gap highlights the need for literacy initiatives that move beyond generic awareness messages toward targeted, behaviourally informed training for students, older adults, and rural communities.

Low self-control further contributes to risk, echoing Gottfredson and Hirschi's argument that individuals who are impulsive or focused on immediate gratification tend to make hasty online decisions. In fast-paced digital environments, such users are more likely to click unsafe links, share sensitive data, or accept speculative offers without adequate evaluation, behaviours scammers deliberately exploit by creating situations that evoke urgency or fear. Preventive efforts should therefore include interventions that strengthen self-regulation and decision-making during moments of pressure.

Financial strain also plays a prominent role. In a climate of high living costs, stagnant wages, and rising household debt, individuals under economic stress often pursue quick returns or easy

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

credit, leaving them susceptible to scams disguised as high-yield investments or fast loans. Consistent with Strain Theory, unmet financial goals can push individuals toward risky choices. Addressing this requires not only broader financial resilience programs but also accessible, trustworthy financial services that reduce reliance on dubious alternatives.

Risky online routines complete the picture. Frequent unmonitored transactions, sharing personal information on unsecured platforms, or interacting with unknown contacts increase exposure to motivated offenders. Digital guardianship relies less on physical supervision and more on secure technologies and user awareness, underscoring the importance of stronger cybersecurity infrastructures and safer platform design.

Taken together, these findings point to the need for a holistic fraud-prevention strategy that integrates technology with human-centred and socio-economic interventions. AI-driven fraud detection and public awareness campaigns are valuable, but their impact depends on consumers' capacity to act wisely under pressure. Future research should track whether literacy efforts lead to lasting behavioural change, explore emerging fraud types linked to cryptocurrency and AI, compare risks across regional contexts, and examine how resilience and social support may buffer against victimization.

Overall, combating online financial fraud requires strengthening knowledge, improving self-regulation, easing financial strain, and promoting safer digital habits so Malaysians can participate confidently in the digital economy.

Acknowledgement
The author would like to thank the University Sains Islam Malaysia for funding this research.

References

Abdul Jamal, A. A. (2022). Nudging financial literacy, attitudes and behaviours among low self-control young adults: a randomized controlled trial (Doctoral dissertation, University of Birmingham).

Ahmad, Z. (2025). Investment scams: the effect of bias-induced gullibility on victimization propensity. Crime, Law and Social Change, 83(1), 1-29.

Antipova, T., & Riurean, S. (2025). Bytes and Battles in AI Era. Safeguarding Consumers' Digital World. In Digital Technology Platforms and Deployment (pp. 201-230). Cham: Springer Nature Switzerland.

Asher, J. (2025). Fraud Markers, De-banking, and Financial Crime: A Legal Analysis of Counter-fraud Practices in the UK and Beyond. Taylor & Francis.

Bank Negara Malaysia. (2025). Digital banking: Risk management guidelines for fraud prevention. https://www.bnm.gov.my

Bar Lev, E., Maha, L. G., & Topliceanu, S. C. (2022). Financial frauds' victim profiles in developing countries. Frontiers in Psychology, 13, 999053.

Basto-Pereira, M., Farrington, D. P., & Maciel, L. (2024). Unraveling the sequences of risk factors underlying the development of criminal behavior. Journal of Developmental and Life-Course Criminology, 10(2), 242-264.

Bernama. (2024). AI voice scams on the rise in Malaysia: 38% spike in 2024. Bernama News Agency. https://www.bernama.com

Birkenmaier, J., Maynard, B., & Kim, Y. (2022). Interventions designed to improve financial capability: A systematic review. Campbell Systematic Reviews, 18(1), e1225.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

Boyle, P. A., Wang, T., Mottola, G., Stewart, C., Wilson, R. S., Bennett, D. A., & Yu, L. (2025). Scam susceptibility is associated with a markedly accelerated onset of Alzheimer's disease dementia. Alzheimer's & Dementia, 21(3), e14544.

Button, M., Shepherd, D., Blackbourn, D., & Gill, M. (2022). The fraud justice network in the UK: A review of the fraud landscape and the role of the police. Journal of Financial Crime, 29(2), 331–349.

Button, M., Shepherd, D., Hawkins, C., & Tapley, J. (2024). Disseminating fraud awareness and prevention advice to older adults: perspectives on the most effective means of delivery. Crime Prevention and Community Safety, 26(4), 385-400.

Carcelén-García, S., Narros-González, M. J., & Galmes-Cerezo, M. (2023). Digital vulnerability in young people: gender, age and online participation patterns. International Journal of Adolescence and Youth, 28(1), 2287115.

Cheung, G. W., Cooper-Thomas, H. D., Lau, R. S., & Wang, L. C. (2024). Reporting reliability, convergent and discriminant validity with structural equation modelling: A review and best-practice recommendations. Asia pacific journal of management, 41(2), 745-783.

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

Cohen, L. E., & Felson, M. (2015). Routine activity theory: A routine activity approach. In Criminology theory (pp. 313-321). Routledge.

Cybersecurity Malaysia. (2024). Annual threat landscape report https://www.cybersecurity.my

Czech, K., Ochnio, L., Wielechowski, M., & Zabolotnyy, S. (2024). Financial literacy: Identification of the challenges, needs, and difficulties among adults living in rural areas. Agriculture, 14(10), 1705.

Daigle, L. E., Snyder, J. A., & Fisher, B. S. (2016). Measuring victimization: Issues and new directions. The handbook of measurement issues in criminology and criminal justice, 249-276.

De Bruijn, E. J., & Antonides, G. (2022). Poverty and economic decision making: a review of scarcity theory. Theory and Decision, 92(1), 5-37.

Dulisse, B. C., Connealy, N., & Logan, M. W. (2024). "Get rich quick," scheme or script? The effect of crypto culture on the susceptibility of fraud victimization among cryptocurrency purchasers. Journal of Criminal Justice, 94, 102273.

Europol. (2020). Internet organised crime threat assessment (IOCTA) 2020. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

FBI. (2020). Internet crime report 2020. Federal Bureau of Investigation Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Franceschini, I., Li, L., & Bo, M. (2025). Scam: Inside Southeast Asia's Cybercrime Compounds. Verso Books.

Graham, B. A., Sinclair, R. R., & Munc, A. (2024). The relationship between dispositional affectivity, perceived income adequacy, and financial strain: An analysis of financial stress perceptions. Psychological Reports, 00332941241239267.

Hernandez-Perez, J., & Cruz Rambaud, S. (2025). Uncovering the factors of financial well-being: the role of self-control, self-efficacy, and financial hardship. Future Business Journal, 11(1), 70.

Hofmann, W. (2024). Going beyond the individual level in self-control research. Nature Reviews Psychology, 3(1), 56-66.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026
Holt, T., Bossler, A., & Seigfried-Spellar, K. (2022). Cybercrime and digital forensics: An introduction. Routledge.

Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Advanced data analytics in internal audits: A conceptual framework for comprehensive risk assessment and fraud detection. Finance & Accounting Research Journal, 6(6), 931-952.

Interpol. (2025). Cyber-enabled financial crime: Trends and countermeasures. https://www.interpol.int

Jamil, A. H., Mohd Sanusi, Z., Yaacob, N. M., Mat Isa, Y., & Tarjo, T. (2022). The Covid-19 impact on financial crime and regulatory compliance in Malaysia. Journal of Financial Crime, 29(2), 491-505.

Jouali, Y., El Aboudi, S., EL AFI, R., & Jouali, J. (2024). Anticipating financial distress: Leveraging financial information, financial ratios, and corporate governance for proactive risk management. Edelweiss Applied Science and Technology, 8(4), 683-696.

Katnic, I., Katnic, M., Orlandic, M., Radunovic, M., & Mugosa, I. (2024). Understanding the role of financial literacy in enhancing economic stability and resilience in Montenegro: A data-driven approach. Sustainability, 16(24), 11065.

Klutsch, J., Haehn, L., Kreuder, A., Böffel, C., Frick, U., & Schlittmeier, S. J. (2025). InstaTrust or InstaTrap: How relationships and developmental tasks affect young adults' phishing susceptibility on Instagram. International Journal of Human-Computer Studies, 197, 103456.

Kumar, V. A., Bhardwaj, S., & Lather, M. (2024). Cybersecurity and Safeguarding Digital Assets: An Analysis of Regulatory Frameworks, Legal Liability and Enforcement Mechanisms. Productivity, 65(1), 1-10.

Kwak, H., & Kim, E. K. (2022). The role of low self-control and risky lifestyles in criminal victimization: A study of adolescents in South Korea. International journal of environmental research and public health, 19(18), 11500.

Lamar, M., Arfanakis, K., Kapasi, A., Han, S. D., Bennett, D. A., Yu, L., & Boyle, P. A. (2024). Associations between structural neuroimaging markers of Alzheimer's risk and scam susceptibility. Brain Imaging and Behavior, 18(6), 1491-1498.

Lambert, L. S., & Newman, D. A. (2023). Construct development and validation in three practical steps: Recommendations for reviewers, editors, and authors. Organizational Research Methods, 26(4), 574-607.

Levi, M., & Smith, R. G. (2022). Fraud and pandemics. Journal of Financial Crime, 29(2), 413-432.

McCoy, P. A. (2025). Sharing Risk: The Path to Economic Well-Being for All. Univ of California Press.

Mokhtar, R., & Rohaizat, A. (2024). Cybercrimes and cyber security trends in the new normal. In The New Normal and Its Impact on Society: Perspectives from ASEAN and the European Union (pp. 41-60). Singapore: Springer Nature Singapore.

Muharram, S. S., Suhaimi, M. Z., & Marcus, M. (2022). Cybercrimes in Malaysia. Journal of Education and Social Sciences, 22(1), 34-38.

Nasruddin, M. N. M., Taslim, K. N., Rahman, S. B. A., & Abd Rahman, I. R. (2024). Analyzing The Relationship Between Macroeconomic Indicators and the Incidence of Financial Scams in Malaysia. Journal of Social Sciences and Business, 3(2), 41-49.

Nataraj-Hansen, S. (2024). Blaming Victims of Online Romance and Investment Frauds: An Analysis of Two Theoretical Perspectives (Doctoral dissertation, Queensland University of Technology).

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026
Ngo, F. T., Borja, B. M., Newman, D., & Kim, Y. (2024). The linkage between low self-control, perception of control, and tourist victimization: Bridging the gap between perceived and actual risks. Crime & Delinquency, 00111287241285824.

Nunnally J. C., Bernstein I. H. (1994). Psychometric theory (3rd ed.). New York, NY: McGraw-Hill.

OECD. (2020). OECD Digital Economy Outlook 2020. OECD Publishing.

Ong, A. S. (2022). Think first, act later, or act first, think later: Does the fraud triangle hold when individuals are impulsive?. Journal of Forensic and Investigative Accounting, 14(1), 11-38.

Ogunola, A. A., Sonubi, T., Toromade, R. O., Ajayi, O. O., & Maduakor, A. H. (2024). The intersection of digital safety and financial literacy: Mitigating financial risks in the digital economy. International Journal of Science and Research Archive, 13(02), 673-691.

PwC Malaysia. (2025). Economic crime and fraud outlook 2025. https://www.pwc.com/my

Reale, C., Salwei, M. E., Militello, L. G., Weinger, M. B., Burden, A., Sushereba, C., & Anders, S. (2023). Decision-making during high-risk events: a systematic literature review. Journal of Cognitive Engineering and Decision Making, 17(2), 188-212.

Revicki, D. (2024). Internal consistency reliability. In Encyclopedia of quality of life and well-being research (pp. 3579-3580). Cham: Springer International Publishing.

Reynald, D. M. (2016). Guarding against crime: Measuring guardianship within routine activity theory. Routledge.

Shete, N. L., Maddel, M., & Shaikh, Z. (2024). A comparative analysis of cybersecurity scams: Unveiling the evolution from past to present. In 2024 IEEE 9th International Conference for Convergence in Technology (I2CT) (pp. 1-8). IEEE.

Singh, K. N., & Misra, G. (2023). Victimisation of investors from fraudulent investment schemes and their protection through financial education. Journal of Financial Crime, 30(5), 1305-1322.

Snyder, J. A., & Golladay, K. (2024). More than just a "bad" online experience: Risk factors and characteristics of catfishing fraud victimization. Deviant behavior, 1-21.

Storey, V. C., Baskerville, R. L., & Kaul, M. (2025). Reliability in design science research. Information Systems Journal, 35(3), 984-1014.

Tasneem, R., & Jabbar, M. A. (2024). An Insight into Cybersecurity during the Covid-19 Pandemic. In The Fusion of Artificial Intelligence and Soft Computing Techniques for Cybersecurity (pp. 3-25). Apple Academic Press.

The Star. (2025, August 14). 12bil in losses to online scam in first half of 2025, says Home Ministry. Retrieved from https://www.thestar.com.my/news/nation/2025/08/14/rm112bil-in-losses-to-online-scam-in-first-half-of-2025-says-home-ministry

Tyagi, A. K., Naithani, K., & Tiwari, S. (2024). Security and Possible Threats in Today's Online Social Networking Platforms. Online Social Networks in Business Frameworks, 159-199. U.S. Department of Justice. (2020). Fraud. https://www.justice.gov/fraud

Vetrivel, S. C., Vidhyapriya, P., & Arun, V. P. (2025). Education and Consumer Awareness. In Sustainable Practices in the Fashion and Retail Industry (pp. 231-254). IGI Global Scientific Publishing.

Wall, D. S., & Williams, M. L. (2017). Introduction: Policing cybercrime: networked and social media technologies and the challenges for policing. In Policing Cybercrime (pp. 1-4). Routledge.

Advanced International Journal of Business, Entrepreneurship and SME's
AIJBES
EISSN: 2682-8545
Volume 7 Issue 26 (December 2025) PP. 372-390
DOI 10.35631/AIJBES.726026

Wambugu, J. M., Kavivya, C., & Handa, S. (2024). Risk factors that influence criminal victimisation. Path of Science, 10(9), 2013-2019.

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.

Xu, L., Wen, X., Wang, J., Li, S., Shi, J., & Qian, X. (2024). Psychological predictors of online fraud victimhood in China: a machine learning approach. Psychology, Crime & Law, 1-24.

Zainuddin, M. T. (2016). Marketing: Conventional Approach and Complementary Views from Islamic Perspectives.

Zheng, H., Li, Q., & Xia, C. (2024). Does financial literacy contribute to facilitating residents in safeguarding their rights as financial consumers? A three-stage study based on the perspective of "fraud" phenomenon. International Review of Economics & Finance, 93, 720-735.

Zhi, B. H. J., Connie, T., Ong, T. S., & Teoh, A. B. J. (2025). Classifying Scam Calls through Content Analysis with Dynamic Sparsity Top-k Attention Regularization. IEEE Access.

Zhou, Y. B., Bu, Y. R., Bao, Q., & Zhao, H. J. (2025). Multimodal anti-fraud education improves cognitive emotional and behavioral engagement in older adults. Scientific Reports, 15(1), 29389.