INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 16, Issue 5, (2026) E-ISSN: 2222-6990

Capable Yet Deceived: A Qualitative Exploration of Cognitive and Behavioural Processes in Online Financial SCAM Victimisation in Malaysia

Mohd Akbal Qamas Abdul Basir, Mohamed Hisham Dato Haji Yahya, Hasri Mustafa, Wei Ni Soh

School of Business and Economics, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

Corresponding Author Email: mohdakbalqamas@gmail.com

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v16-i5/28337

Published Date: 30 May 2026

Abstract

Online financial scam victimisation in Malaysia persists despite stronger enforcement, expanded regulatory frameworks and growing public awareness. Individuals with financial knowledge, digital competence and prior scam awareness continue to authorise fraudulent transfers, demonstrating that knowledge-gap explanations alone are inadequate. Drawing on Protection Motivation Theory, this study explores the cognitive and behavioural processes through which victimisation unfolds. An interpretivist qualitative design incorporated in-depth interviews with fifteen scam victims and fourteen Commercial Crime Investigation Department officers, supplemented by thirty publicly available police case reports. Thematic analysis identified three sequential stages. Threat appraisal was disrupted by reward salience, social validation and situational financial pressure. Coping appraisal was suppressed through emotional overload, authority impersonation and convenience framing. Post-victimisation experience produced either adaptive vigilance or excessive trust withdrawal. Together, these stages show that Protection Motivation Theory can explain scam victimisation as a time-based process rather than as a static predictor model, revealing that its constructs shift dynamically across the scam encounter. This explains why knowledge and competence alone do not guarantee protection. The findings advance scam victimisation research and offer practical insights for Malaysian financial regulation, consumer protection and behavioural intervention design, consumer protection policy and behavioural intervention systems that target the moment protective judgement breaks down.

Keywords: Online Financial Scam, Protection Motivation Theory, Threat Appraisal, Coping Appraisal, Victimisation Process, Malaysia, Qualitative Research

Introduction

Malaysia's financial services have moved rapidly into online and mobile channels. Internet use reached 98.0 percent in 2024 compared with 84 percent in 2019 (World Bank, 2025;

Department of Statistics Malaysia, 2025), while mobile banking transactions amounted to approximately RM1.44 trillion in 2023 (Statista, 2024). This level of connectivity has made financial activity faster and more convenient. At the same time, it has created a continuous stream of digital interactions within which fraudulent requests can be received, trusted and acted upon. Online financial scams succeed not because banking systems fail but because deceptive messages are constructed to appear familiar, urgent and legitimate.

In Malaysia, fraud accounted for 5,751 of the 7,616 cyber incidents recorded by CyberSecurity Malaysia in 2025, representing approximately 75.5 percent of all categorised cases (CyberSecurity Malaysia, 2025). Law enforcement data recorded large numbers of cases across telecommunications fraud, investment schemes, e-commerce deception and fictitious loan operations (Bernama, 2025). These cases persist alongside the Criminal Procedure Code (Amendment) Act 2024, the National Scam Response Centre and regulatory oversight by Bank Negara Malaysia and the Securities Commission Malaysia. Continued scam compliance therefore raises a more precise question than awareness alone can answer.

Many victims are educated, employed and familiar with online banking. Some already know that scams exist yet still authorise transfers when the situation appears credible, socially endorsed, financially rewarding, or emotionally urgent. Recent studies confirm that scam victims may include financially active and digitally competent individuals (Du & Chen, 2023; Cuadra et al., 2025). The central issue is therefore not only whether people know about scams. It is how their judgement changes while the scam is unfolding.

Protection Motivation Theory helps explain this process through threat appraisal and coping appraisal (Rogers, 1983). Threat appraisal may weaken when potential danger is displaced by reward, social validation, or institutional impersonation. Coping appraisal may weaken when victims feel rushed, frightened, or unable to verify. In such moments, protective judgement does not disappear. It becomes narrowed, redirected, or temporarily suspended. This makes victimisation better understood as a staged motivational process rather than a single error in judgement.

This study explores the underlying cognitive and behavioural processes that characterise victimisation in online financial scams. The continued occurrence of these scams suggests that awareness alone cannot fully explain why people become victims. This study is therefore motivated by the need to understand what happens during the scam process, especially how victims interpret deceptive situations, respond to pressure and decide whether to comply. The study contributes by explaining online financial scam victimisation as a process that develops over time, involving disrupted threat appraisal, suppressed coping appraisal and post-loss recalibration of protective motivation. This process-based explanation offers a clearer understanding of the behavioural conditions under which scam compliance occurs.

Literature Review

Online Financial Scams and Victimisation Processes

Online financial scams involve deceptive financial activities conducted through online platforms, mobile applications, communication channels and technology-mediated transaction systems. These schemes may take the form of fraudulent investment offers, fictitious loans, e-commerce deception, impersonation, identity misuse, or other digitally

enabled financial solicitations. Although they differ in surface features, they share a common behavioural structure. Victims are persuaded to act under conditions of uncertainty, perceived legitimacy, urgency, or relational trust. Victimisation therefore involves more than exposure to false information. It involves how individuals interpret a request, assess its credibility and decide whether to comply, delay, verify, or withdraw.

A process view is important because online scams are frequently embedded within ordinary financial routines. Routine Activity Theory explains that victimisation becomes possible when a motivated offender encounters a suitable target in the absence of effective guardianship (Cohen & Felson, 1979). In online settings, frequent use of digital platforms can increase exposure to fraudulent contact because conventional boundaries and guardianship mechanisms are weaker or less visible (Elueze & Quan-Haase, 2018; Holtfreter et al., 2008; Van Wilsem, 2013). However, exposure is not equivalent to victimisation. Many individuals receive suspicious messages but do not respond. Others continue to engage even when some warning signs are present. This distinction directs attention away from exposure alone and toward the process of interpretation and appraisal that occurs after contact.

Offender-Centred Explanations and Their Limitations

Financial fraud theories help explain how fraud is structured from the offender side. Fraud Triangle Theory explains fraudulent conduct through pressure, opportunity and rationalisation (Cressey, 1953). Fraud Diamond Theory adds capability as a fourth condition enabling offenders to identify and sustain fraudulent opportunities (Wolfe & Hermanson, 2004). Fraud Hexagon Theory further expands explanation by including stimulus, opportunity, rationalisation, capability, ego and collusion (Vousinas, 2019). These theories explain why offenders act and how fraudulent schemes are organised, but they give insufficient attention to how victims process fraudulent requests, why protective action is delayed, or why payment is authorised despite possible awareness of risk. A victim-side explanation of judgement, appraisal and behavioural response is therefore required.

Protection Motivation Theory and Victim Decision-Making

Protection Motivation Theory provides a suitable framework for explaining victim decision-making during scam encounters. The theory explains protective behaviour through two appraisal processes. Threat appraisal involves perceived severity, perceived vulnerability and the perceived rewards associated with risky behaviour. Coping appraisal involves response efficacy, self-efficacy and response cost in relation to available protective responses (Clubb & Hinkle, 2015; Rogers, 1983; Witte, 1994). PMT is particularly relevant because it links risk recognition with behavioural response. Awareness of scams does not automatically lead to protective action. A person may recognise danger yet comply if the reward appears attractive, the source appears authoritative, or the cost of resisting appears too high.

Research on online security and cybercrime-related behaviour supports the use of PMT in technology-mediated risk contexts. PMT constructs have been used to explain security policy compliance, phishing avoidance and protective measures in digital environments (Crossler & Belanger, 2014; De Kimpe et al., 2022; Jenkins et al., 2014; Martens et al., 2019; Safa et al., 2015; Tsai et al., 2016). Meta-analytic evidence confirms that self-efficacy and response efficacy are among the most significant determinants of protective intentions (Floyd et al., 2000; Milne et al., 2002). Haag et al. (2021) further argue that PMT constructs in information

security should not be treated as fixed personal traits, an insight that is crucial for scam victimisation research because appraisal may shift within minutes under persuasive and emotional pressure.

For online financial scam victimisation, PMT should function as a process framework rather than a static model of predictors. Appraisal may shift across the encounter. Severity may be low at the point of reward, high at the point of legal accusation and confirmed only after financial loss. Vulnerability may be reduced by peer endorsement during engagement and intensified by recognised harm after the fact. Self-efficacy may be strong in routine online banking but temporarily collapsed during intimidation. Response cost may be perceived as unnecessary friction before loss and as worthwhile protection afterwards. This process view explains why scam compliance may occur among individuals who possess financial knowledge, digital familiarity and general awareness of fraud risks.

Financial Literacy, Digital Literacy and Personal Values

Financial literacy refers to the knowledge, behaviour and attitudes that support understanding of financial concepts, management of resources and informed financial decision-making (Huston, 2010; Lusardi and Mitchell, 2007; OECD, 2018; OECD, 2020). In online financial scams, financial knowledge may help individuals evaluate whether a return promise is unrealistic or whether borrowing terms are irregular. However, scammers frequently use familiar financial language, including capital, return, profit and withdrawal, to construct credibility within fraudulent offers. Financial literacy therefore functions as a cognitive resource whose protective role depends on whether it can remain active under urgency, social pressure and emotional disruption.

Digital literacy extends beyond technical ability to include critical evaluation, online safety and recognition of manipulation in digital environments (Eshet, 2004; Ferrari, 2012; Gilster, 1997). Familiarity with online platforms may strengthen coping appraisal by increasing confidence in verification, but the same familiarity may also normalise rapid digital authorisation. Digital literacy becomes protective only when it is translated into active and sustained verification during the scam encounter rather than remaining as background competence.

Personal values, as theorised by Schwartz (1992, 2012), are broad motivational goals that guide judgement and behaviour across situations. Values such as security, benevolence, conformity, achievement and self-direction shape what individuals consider urgent, desirable, or legitimate when confronted with persuasive financial messages. Scam communications are often structured to activate these values in distorted forms, framing compliance as the protective, responsible, or financially prudent action. Values therefore influence threat appraisal by shaping perceived benefit and perceived legitimacy and influence coping appraisal by shaping the perceived cost of resistance or refusal.

The literature provides complementary but incomplete explanations of online financial scam victimisation. Routine Activity Theory explains exposure and opportunity but not compliance (Cohen & Felson, 1979; Elueze & Quan-Haase, 2018; Holtfreter et al., 2008; Van Wilsem, 2013). Financial fraud theories explain offender strategy but not victim judgement (Cressey, 1953; Wolfe & Hermanson, 2004; Vousinas, 2019). Financial literacy and digital literacy

explain available cognitive and technical resources but not why these resources sometimes fail under persuasive pressure (Gilster, 1997; Huston, 2010; Ferrari, 2012; Lusardi & Mitchell, 2007; OECD, 2018; OECD, 2020). Personal values explain motivational orientation but require connection to the real-time appraisal process during the encounter (Schwartz, 1992; Schwartz, 2012). PMT connects these dimensions by placing threat appraisal and coping appraisal at the centre of behavioural response. The literature therefore supports a process-based understanding of victimisation in which compliance emerges from the interaction of exposure, persuasive design, literacy resources, personal values and appraisal processes.

Methodology

Research Design

An interpretivist qualitative design was used to explore how online financial scam victimisation is experienced, interpreted and reconstructed across the encounter. This design was appropriate because the study focuses on process, meaning and decision-making rather than prevalence or statistical association. Qualitative inquiry is suitable when the aim is to understand how participants make sense of complex, contextually embedded experiences (Creswell & Poth, 2018; Denzin & Lincoln, 2011). The interpretivist position allowed different accounts of scam victimisation to be examined as situated perspectives, recognising that how a scam was understood in the moment differs from how it is understood after loss has occurred.

Data Sources and Participants

Three qualitative data sources were used. First, fifteen victims of online financial scams were interviewed. Their accounts provided lived explanations of initial contact, perceived credibility, emotional pressure, payment decisions, loss recognition and later behavioural change. Second, fourteen officers from the Commercial Crime Investigation Department were interviewed during April to May 2021. Their accounts provided institutional observations on scam techniques, recurring victim behavioural patterns and enforcement-related interpretations of scam progression. Third, thirty publicly available police case reports were analysed after data reduction, covering scam typologies from multiple Malaysian states between 2009 and 2022. These reports provided documentary traces of scam sequences, authority impersonation, staged payments and financial loss. Purposive criterion-based sampling was appropriate because the study required participants who could provide information-rich accounts of the phenomenon under investigation (Savin-Baden & Major, 2013). Table 1 summarises the three data sources alongside their respective analytic contributions to the study.

Table 1
Data Sources and Analytic Contribution

Data Source	Number	Analytic Contribution
Scam victims	15	Provided lived accounts of how fraudulent requests were interpreted, how trust and urgency shaped action, how payment decisions were made and how behaviour changed after recognition of loss
Commercial Crime Investigation Department officers	14	Provided institutional interpretation of scam techniques, recurring victim responses, reporting patterns and enforcement observations
Publicly available police case reports retained after data reduction	30	Provided documentary traces of scam typologies, contact routes, persuasion sequences, staged payments, impersonation and financial loss

Data Collection

Semi-structured interviews were used because they allow participants to describe their experiences in their own terms while enabling the researcher to cover comparable issues across cases (Kvale and Brinkmann, 2009). Victim interviews focused on how the scam began, why the request appeared believable, what emotions were experienced, how payment decisions were justified, when suspicion emerged and what changed after the incident. Officer interviews focused on observed scam patterns, persuasion tactics, victim responses and prevention challenges. Interview prompts were designed to support process reconstruction, following the sequence of the scam encounter from first contact through compliance to recognition of loss. Interviews were audio recorded with consent, transcribed verbatim and subject to member checking and participant verification to strengthen credibility (Creswell & Miller, 2000; Lincoln & Guba, 1985).

Document analysis was conducted on thirty publicly available police case reports retained after data reduction. Reports were retained only when they contained sufficient narrative detail to support process tracing, including initial contact, persuasion strategy, payment action and reporting pathway. Reports with unclear or incomplete information were excluded. Qualitative document analysis requires systematic selection, appraisal and interpretation so that documents are used as meaningful evidence rather than as unexamined background material (Bowen, 2009; Schreier, 2012).

Data Analysis and Trustworthiness

Thematic analysis was applied following the six-phase framework of Braun and Clarke (2013). Coding proceeded from descriptive features of scam progression through interpretive sense-making to theoretical linkage with PMT constructs. Findings are presented using analytic paraphrase supported by source identifiers such as Victim 5, Police 10 and R#21 rather than extended verbatim quotation. This approach protects participant sensitivity, reduces overexposure of original testimony and retains visible empirical grounding. Trustworthiness was strengthened through triangulation across victim interviews, officer testimonies and case reports; transcript verification; and systematic comparison across data sources. Credibility, dependability and confirmability were addressed in accordance with Lincoln and Guba (1985) and Creswell and Poth (2018).

Findings

The findings indicate that online financial scam victimisation unfolded as a staged cognitive and behavioural process. Across all three data sources, victimisation was characterised by three interconnected processes. The first involved disruption of threat appraisal, where perceived rewards, social validation and situational pressure reduced the salience of risk. The second involved suppression of coping appraisal, where emotional overload, authority cues and convenience framing weakened victims' perceived capacity to resist. The third involved post-victimisation recalibration, where confirmed loss triggered retrospective reinterpretation and heightened vigilance, although sometimes this extended into broader distrust. Table 2 presents the full thematic structure, including the seven subthemes derived from the analysis, the core process each subtheme captures and the primary data sources supporting each finding.

Table 2
Themes and Subthemes of Online Financial Scam Victimisation

No.	Theme	Subtheme	Core Process	Primary data support
Theme 1	Disruption of threat appraisal	1.1: Reward salience and attentional narrowing	Perceived benefit became more immediate than perceived risk	Victims 5, 11, 15; Police 4, 11; R#7, R#8
		1.2: Social validation and reduced perceived vulnerability	Group participation, testimonials and trusted contacts lowered perceived personal risk	Victims 3, 5, 8; Police 2, 3; R#15
		1.3: Situational stress and temporal prioritisation	Urgent financial or life circumstances shifted attention from long-term risk to immediate relief	Victims 1, 11, 14; Police 2, 10
Theme 2	Suppression of coping appraisal	2.1: Emotional overload and temporary collapse of self-efficacy	Panic, fear, guilt, intimidation and time pressure weakened the ability to pause or verify	Victims 4, 10, 11; Police 3, 6, 11; R#21, R#22
		2.2: Convenience framing and reconfiguration of response cost	Fraudulent routes appeared easier, faster and less demanding than legitimate protection or verification	Victims 3, 11; Police 9, 10
Theme 3	Post-victimisation shift in protection motivation	3.1: Recognition and retrospective reinterpretation	Loss became clear after silence, failed returns, or third-party intervention	Victims 2, 3; police perspectives
		3.2: Trust erosion and adaptive or maladaptive vigilance	Victims became more cautious, but some shifted towards excessive distrust or avoidance	Victims 1, 3, 9, 12; police perspectives

Note Victim identifiers refer to scam victim interview participants. Police identifiers refer to Commercial Crime Investigation Department officer interview participants. R# identifiers refer to publicly available police case reports retained after data reduction. Numbers indicate individual participant or document codes assigned during data collection.

Theme 1: Disruption of Threat Appraisal

The first process concerned the disruption of threat appraisal. Victimisation often began when the perceived benefit of engagement became more prominent than possible danger. Victims did not necessarily enter the scam with no awareness of risk. Rather, risk was pushed to the background when the offer appeared financially attractive, socially validated, or personally urgent.

Subtheme 1.1: Reward Salience and Attentional Narrowing

Reward salience appeared when anticipated financial gain, lifestyle improvement, or urgent financial relief became the dominant focus of attention. Victim 5 framed the decision around rapid financial improvement and early retirement, with imagined future benefit working as a motivational anchor that drew attention away from verification. Victim 11 was drawn to unusually favourable loan terms including fast approval and very low interest, which intensified attraction rather than activating suspicion. Victim 15 linked engagement to lifestyle aspirations and social media influence, indicating that reward was not only financial but also tied to identity and social comparison. Police 11 connected reward-seeking behaviour with financial hardship and exclusion from formal credit systems, observing that some victims turned to online alternatives when conventional financial institutions were difficult to access because of payslip or eligibility constraints. Police 4 acknowledged that third parties could manipulate victims through these aspirations. Documentary evidence supported this pattern at the case level. R#7 recorded an investment promise where a small initial transfer was linked to a very large return within a short period, followed by further commission demands before communication ceased. R#8 showed a multi-level scheme where staged deposits and large package values created the appearance of structured opportunity. In both cases, reward amplification preceded and facilitated financial transfer.

Subtheme 1.2: Social Validation and Reduced Perceived Vulnerability

Social validation reduced perceived vulnerability by making participation appear shared and therefore safer. Victim 5 was influenced by the presence of many people in an online group and by repeated claims from others that returns had been received. Victim 3 gained confidence because friends had joined and provided positive feedback. Victim 8 similarly reported being influenced by a known contact who had already participated. In these accounts, personal vulnerability was lowered through collective participation. Risk felt less personal when others appeared to be participating successfully. Police 3 described social referral as a deliberate structural feature of investment-related scams, noting that friend invitations, commission arrangements and recruitment incentives were embedded into scheme design. This indicates that social validation was not incidental. It was built into the scam architecture. R#15 documented a commission-based scheme involving recruitment through social media where the victim later lost funds after the organiser disappeared and blocked all participants. Peer endorsement and group visibility therefore operated as engineered shortcuts for perceived legitimacy.

Subtheme 1.3: Situational Stress and Temporal Prioritisation

Situational stress disrupted threat appraisal by compressing the decision horizon. Victim 1 linked the loss to savings accumulated for marriage, showing how a major life event intensified the pressure to secure or increase funds quickly. Victim 11 described needing money for urgent household items, which made the loan offer appear practically useful

rather than suspicious. Victim 14 similarly engaged during a period of financial strain. Police 10 observed that some victims may already recognise risk but proceed because they are in a state of desperation for money. Police 2 connected vulnerability with survival-related pressure and limited perceived alternatives, noting that urgent need can override values that would otherwise support cautious behaviour. These accounts indicate that threat appraisal was not absent. Victims could recognise risk existed, but urgency changed the order of priorities. The need to solve an immediate problem made potential harm feel psychologically distant. Scam vulnerability therefore emerged when immediate relief became more important than careful risk evaluation.

Theme 2: Suppression of Coping Appraisal

The second process concerned suppression of coping appraisal. Disruption of threat appraisal explains how initial engagement begins. Suppression of coping appraisal explains how compliance continues and deepens. Victims may have recognised irregularities or felt some hesitation, but their perceived ability to verify, delay, or withdraw was weakened during the interaction.

Subtheme 2.1: Emotional Overload and Temporary Collapse of Self-Efficacy

Emotional overload reduced victims' perceived ability to think clearly and act protectively. Victim 4 described panic after receiving a firm and convincing call, indicating that fear interrupted rational assessment even though prior scam awareness was present. Victim 10 experienced guilt and intimidation when the caller raised his voice and made the victim feel responsible for wrongdoing, shifting attention from evaluating the request to escaping a perceived accusation. Victim 11 described pressure arising from the possibility of losing an opportunity if action was delayed, a time constraint that prevented reflection. These accounts show that self-efficacy weakened when fear, guilt, or urgency took control of the interaction. Police 6 observed that even individuals familiar with online banking and aware of scam tactics may comply when offenders use intimidation, threats of arrest, property confiscation, or legal consequences. Police 11 similarly explained that impersonation of bank staff or police officers can trigger panic and rapid disclosure of sensitive information. Police 3 described cases where victims were informed that their accounts were linked to money laundering, producing immediate fear-driven compliance. These observations are significant because they confirm that knowledge and digital familiarity do not constitute reliable protection when emotional manipulation is simultaneously deployed. Documentary cases reinforced this pattern. R#21 involved a caller claiming to represent Pos Laju and alleging prohibited items under the victim's name, producing fear and compliance. R#22 involved a caller impersonating a bank officer before transferring the call to a person posing as a Bukit Aman police officer who claimed a money-laundering warrant had been issued, leading the victim to transfer money to avoid detention. These cases illustrate how authority impersonation and manufactured legal threat can suppress self-efficacy and make fraudulent compliance appear as a form of self-protection.

Subtheme 2.2: Convenience Framing and Reconfiguration of Response Cost

Convenience framing altered the perceived cost of protective behaviour. Victim 11 was attracted to a loan process that appeared to require no payslips or documents and promised approval within minutes, comparing this favourably with the documentation demands of formal financial institutions. Victim 3 compared the delayed returns of legitimate investment

with the faster returns promised by the scam and the same victim also described two-factor authentication as somewhat troublesome because it required additional time. These accounts suggest that legitimate safeguards were sometimes experienced as inconvenience rather than protection. Police 9 linked this convenience effect to financial exclusion, noting that individuals with poor credit records or blacklisting may seek online alternatives when formal loans are inaccessible. Fraudsters then frame small payments as necessary administrative steps such as processing fees, blacklist release fees, or legal charges, creating incremental compliance in which each payment appears manageable and procedurally routine. Police 10 identified convenience as a primary reason why people became victims, particularly in fictitious loan cases offering low interest and quick approval. Response cost was therefore reconfigured: verification, delay and institutional procedure felt burdensome, while fraudulent compliance felt smooth and immediate.

Theme 3: Post-Victimisation Shift in Protection Motivation

The third process concerned post-victimisation recalibration. Once the scam became undeniable, victims reinterpreted earlier events and adjusted future behaviour. This stage is important because it shows that protection motivation intensified after harm, although the recalibration was not always balanced.

Subtheme 3.1: Recognition and Retrospective Reinterpretation

Recognition often occurred after communication silence, failed returns, or third-party intervention rather than during active engagement. Victim 3 recognised the scam when expected money did not arrive. Victim 2 recognised deception when scammers stopped replying. In both cases, the fraud became visible only after the promised outcome failed to materialise. Police 6 observed that many victims were unaware they had been deceived until communication collapsed or a third party helped them recognise the pattern, noting that scammers deliberately prevent reflective space to sustain compliance. Police 2 observed that victims often do not have time to think rationally during the active encounter. Retrospective reinterpretation followed recognition. Earlier cues that had been dismissed became meaningful after harm was confirmed. This shows that cognitive capacity for identifying warning signs existed throughout the encounter but was not accessible with full force under persuasive and emotional conditions.

Subtheme 3.2: Trust Erosion and Adaptive or Maladaptive Vigilance

After recognition, protection motivation increased. Victim 9 changed how money was managed. Victim 3 began checking reviews and using only verified applications. Victim 12 stopped answering calls from unknown numbers. These changes indicate stronger protective behaviour after loss, consistent with PMT's prediction that confirmed threat experience intensifies perceived severity and vulnerability. However, recalibration was not uniformly adaptive. Victim 1 reported losing trust in all types of investments, extending distrust well beyond the specific scam context. Some victims generalised caution across unfamiliar contacts, online offers and legitimate financial communication alike. Police perspectives confirmed this dual pattern, noting that victims often became more careful after reporting while also observing that shame and embarrassment could constrain disclosure and reduce future financial engagement. Post-victimisation change therefore carries both potential and risk. Loss can strengthen protective behaviour, but it can also narrow future participation if distrust becomes too generalised to support healthy financial activity. Table 3 consolidates

the three-stage process model emerging from the analysis, presenting the appraisal process operating at each stage, the mechanism through which victimisation develops and the defining characteristics of each stage from initial exposure through compliance to post-loss recalibration.

Table 3
Process Model of Online Financial Scam Victimisation

Stage	Appraisal Process	How Victimisation Develops	Process Dimensions
Stage 1	Disrupted threat appraisal	Risk becomes less salient as reward, social proof and urgent need dominate judgement	Reward salience, social validation, reduced perceived vulnerability, situational stress
Stage 2	Suppressed coping appraisal	Victims feel less able to verify, delay, refuse, or withdraw due to emotional and procedural pressure	Emotional overload, authority intimidation, reduced self-efficacy, convenience framing, increased response cost
Stage 3	Recalibrated protection motivation	Loss triggers reinterpretation and stronger caution but may also produce excessive distrust or avoidance	Recognition, retrospective reinterpretation, adaptive vigilance, trust erosion

Discussion

The findings show that online financial scam victimisation is better understood as a staged cognitive and behavioural process than as a simple failure of knowledge or judgement. Victims did not move directly from exposure to financial loss. They first encountered persuasive cues that weakened their assessment of threat. They then faced emotional and procedural pressure that constrained their perceived ability to verify or withdraw. After loss, they reconstructed the event and adjusted future protective behaviour. This staged pattern is consistent with Rogers (1983), who explains protective behaviour through threat appraisal and coping appraisal. Witte (1994) further clarifies that protective response depends not only on perceived danger but also on whether individuals believe available responses are effective and personally manageable.

A Three-Stage Extension of Protection Motivation Theory

Existing Protection Motivation Theory applications in cybersecurity and fraud research predominantly treat its constructs as simultaneous predictors of protective intention measured at a single point in time (Crossler & Belanger, 2014; Floyd et al., 2000; Martens et al., 2019; Tsai et al., 2016). The present findings challenge this static application. Threat appraisal was disrupted during the pre-compliance stage through reward amplification, social validation and situational urgency, consistent with Protection Motivation Theory's recognition of maladaptive rewards as competing motivational forces (Clubb & Hinkle, 2015; Rogers, 1983). Coping appraisal was suppressed during active compliance through emotional overload, authority impersonation and convenience framing, reflecting how self-efficacy and response cost can be situationally undermined (Floyd et al., 2000; Witte, 1994). Protective motivation was then recalibrated during the post-victimisation stage through loss recognition and trust reorganisation, consistent with evidence that prior victimisation heightens

perceived vulnerability and reinforces protective intentions (Wilkinson & Knijnenburg, 2022). Each stage created conditions for the next, meaning that disrupted threat appraisal drew victims into engagement, suppressed coping appraisal sustained compliance and recalibrated protection motivation shaped future behaviour. Together these three stages extend Protection Motivation Theory beyond its original cross-sectional architecture (Haag et al., 2021), providing a temporally sensitive explanation of how ordinary competence is temporarily displaced during fraudulent encounters.

Moving Beyond Knowledge-Deficit Explanations

One significant contribution of the findings is the challenge they pose to knowledge-deficit explanations of scam victimisation. Victims were not simply uninformed. Many had financial knowledge, used online banking and understood that scams existed. Yet these resources did not always protect them during the encounter. Financial literacy research has long emphasised the role of knowledge in supporting informed financial choices (Huston, 2010; Lusardi & Mitchell, 2014). The OECD framework treats financial literacy as a combination of knowledge, behaviour and attitude, which makes it useful for understanding real financial situations rather than abstract concepts alone (OECD, 2018; OECD, 2020). The present findings support this broader view. Victims possessed financial knowledge, but that knowledge became weakened, redirected, or misapplied when the scam was framed as urgent, legitimate, or socially endorsed. The same issue applies to digital literacy. Gilster (1997) introduced digital literacy as the ability to understand and use information from digital sources. Later work expanded the concept to include critical evaluation and safety in online environments (Eshet, 2004; Ferrari, 2012). The findings show that digital familiarity sometimes normalised fast digital action rather than prompting deliberate verification. Digital literacy becomes protective only when it is translated into active evaluation during the encounter rather than remaining as background competence. Personal values shaped how victims interpreted the scam. Values such as security, benevolence, conformity, achievement and self-direction can influence what victims treat as urgent, desirable, or legitimate (Schwartz, 1992; Schwartz, 2012) and scam communications are constructed to activate these values in ways that make compliance appear reasonable.

Disruption of Threat Appraisal

The first stage of victimisation involved disruption of threat appraisal. PMT specifies that threat appraisal includes perceived severity, perceived vulnerability and the perceived rewards of risky action (Rogers, 1983). In the present findings, victims' threat appraisal was weakened when reward, social validation, or immediate pressure became more salient than possible harm. This finding gives particular importance to maladaptive reward. In online financial scams, reward appeared not only as desire for profit but also as relief from financial pressure, avoidance of legal consequences, fulfilment of social obligation, or hope for a better future. When these rewards became immediate and personally meaningful, risk became cognitively less concrete. Social validation further reduced perceived vulnerability by making some scams appear safer through peer participation and testimonials. Routine Activity Theory helps explain how digital routines increase exposure to offenders, but it does not fully explain why social cues become persuasive after contact occurs (Cohen & Felson, 1979; Van Wilsem, 2013). The present findings add that vulnerability may be socially redefined during the encounter. Situational stress also narrowed threat appraisal by shifting attention toward immediate action, relief, or gain, which is consistent with the finding that financial pressure

could override cautious attitudes even among individuals who demonstrated organised financial habits.

Suppression of Coping Appraisal

The second stage involved suppression of coping appraisal. Self-efficacy was reduced by panic, intimidation, guilt and urgency. When scammers impersonated police officers, bank staff, or other authority figures, victims often felt less able to question instructions and compliance was reframed as self-protection. Floyd et al. (2000) show that efficacy beliefs are important predictors of protection motivation and Milne et al. (2002) emphasise that protective action depends on whether individuals believe a recommended response can reduce risk. The present findings extend this logic by showing that scammers actively engineer the conditions under which coping appraisal weakens. They create pressure so that verification appears slow, ineffective, or dangerous. Previous cybersecurity research using PMT has documented how response efficacy, self-efficacy and response cost predict protective behaviour in technology-mediated contexts (Crossler & Belanger, 2014; De Kimpe et al., 2022; Jenkins et al., 2014; Martens et al., 2019; Safa et al., 2015; Tsai et al., 2016). The present study adds a scam-specific explanation. Fraudsters increase the perceived cost of protection and reduce the perceived cost of compliance, making scam authorisation appear easier and more rational than protective verification.

Post-Victimisation Recalibration

The third stage involved recalibration after loss. In PMT terms, direct loss can intensify perceived severity and vulnerability, which should strengthen future protection motivation (Rogers, 1983). Some recalibration was adaptive. Victims became more cautious, monitored accounts more closely and relied more on official verification channels. However, recalibration was not always balanced. Some victims moved from caution to broad distrust, finding legitimate financial communication difficult to accept. This matters because effective prevention should not simply increase fear. Fear may make individuals avoid scams, but excessive fear may also constrain confidence in legitimate financial participation. This bifurcation is consistent with the finding that post-victimisation change could represent either measured vigilance or undue disengagement, depending on whether recalibration was guided by clear action pathways or left unaddressed by institutional support.

Taken together, the three stages reveal that online financial scam victimisation is neither random nor solely the product of ignorance. It follows a structured motivational sequence in which threat recognition is displaced by reward, resistance is engineered away through pressure and convenience, and protective behaviour is rebuilt only after confirmed loss. This sequence explains why enforcement, awareness campaigns and literacy programmes alone remain insufficient. Prevention must intervene at each stage of the process, not only before the encounter begins.

Theoretical Contribution

The findings contribute to Protection Motivation Theory by showing that threat appraisal, coping appraisal and protection motivation operate as shifting processes during online financial scam encounters. While PMT-based research often treats these constructs as predictors of protective intention at a particular point in time, this study shows that scam victimisation requires a more temporal and interactional reading. Threat appraisal may

weaken when reward, social validation and urgency make risk less salient. Coping appraisal may weaken when intimidation, convenience framing and perceived response cost reduce victims' sense of control. Protection motivation may later re-emerge after loss as adaptive vigilance or broader distrust.

This contribution extends PMT by explaining scam victimisation as a sequence of appraisal disruption rather than as a single decision failure. Financial and digital literacy appeared to support victims' capacity to assess risk and verify information, but their protective function depended on whether these resources remained accessible under pressure. By positioning victimisation as a staged process, this study explains why competent individuals may still comply with fraudulent requests. It shows how ordinary competence can be temporarily displaced when persuasive design alters the balance between perceived threat, perceived coping capacity and perceived cost of resistance. This advances PMT beyond a static account of protective intention and demonstrates its value for explaining how vulnerability develops during the scam encounter itself.

Implications And Suggestions

Several theoretical implications arise from the findings. PMT should be applied to online financial scams as a process-oriented framework rather than as a static set of predictors. Measuring threat appraisal and coping appraisal at a single point may overlook how judgement changes between first contact, compliance and post-loss reinterpretation. Maladaptive reward deserves greater analytical attention because reward and relief may become more salient than fear during the early stage of scam engagement. Coping appraisal should be understood as interactionally shaped, since self-efficacy, response efficacy and response cost may be weakened through intimidation, urgency and convenience framing in real time. Methodologically, qualitative designs combining victim accounts, enforcement perspectives and documentary evidence are well suited to revealing the process dimensions of scam victimisation. Future studies may extend this approach by comparing how the three-stage process differs across scam typologies, age cohorts and institutional reporting pathways.

Practical prevention should move beyond generic warnings. Messages that simply advise people to be careful may fail when victims are frightened, rushed, or socially reassured. Scenario-based training should expose learners to realistic scam situations involving urgency, authority claims, reward promises, emotional pressure and social endorsement. Financial institutions and regulators should design protective friction into high-risk transactions through behavioural warnings, cooling-off prompts and delay mechanisms that help restore reflective space when pressure is present. Public messaging should avoid victim-blaming language. Framing victims as greedy, careless, or ignorant oversimplifies the process and deters reporting. Prevention messages should emphasise verification, consultation and delay rather than shame. Interventions can be organised around the three stages. Before compliance, education should train individuals to recognise reward amplification, social proof and urgency framing. During compliance, systems should provide interruption prompts and immediate verification channels accessible under pressure. After victimisation, support should focus on reporting, recovery and rebuilding proportionate confidence rather than leaving individuals to manage distrust and shame alone. Banks, regulators and enforcement agencies should also create low-friction verification tools, clear checklists for loan and

investment offers and public examples of staged payment tactics so that verification feels easier than compliance rather than more burdensome.

Conclusion

This study has explored the underlying cognitive and behavioural processes that characterise online financial scam victimisation in Malaysia. This study was motivated by the need to understand why scam victimisation continues despite public awareness, financial knowledge and digital familiarity. Its main contribution is to explain victimisation as a staged process rather than as a single careless decision. The findings show that victimisation cannot be reduced to ignorance, poor judgement, or lack of awareness. It develops through a staged process in which threat appraisal is disrupted by reward salience, social validation and situational stress; coping appraisal is suppressed by emotional overload, authority impersonation and convenience framing; and protection motivation is recalibrated after loss, producing either adaptive vigilance or, in some cases, excessive distrust. PMT is used in this study to explain why individuals with financial knowledge and online competence may still comply with fraudulent requests. Protective behaviour is shaped not only by awareness, but also by how victims interpret urgency, credibility, fear, cost, convenience and social approval during the scam encounter. The theoretical contribution lies in demonstrating that PMT constructs are contextually sensitive states that shift across the scam encounter rather than fixed cognitive predictors. Future research may test this process model across larger samples or compare how the three stages manifest across investment scams, fictitious loans, e-commerce fraud, romance scams and authority impersonation. Policy and practice should prioritise interventions that help individuals pause, verify and seek support during the encounter itself, because protection that feels slow or costly may fail precisely when it is most needed. Reframing victimisation as a process of appraisal disruption rather than as a label attached to the victim is fairer to participants, stronger for theory and more useful for prevention.

Acknowledgements

The authors wish to express sincere gratitude to the Commercial Crime Investigation Department, Bukit Aman, for institutional cooperation and facilitation of access to research participants. Appreciation is extended to all police officers and scam victims who generously shared their experiences and insights. This study was conducted in accordance with approved ethical protocols governing human subject participation and the handling of sensitive institutional documentation.

References

Bernama. (2025, August 12). Police: Online scams cost Malaysians over RM2.7 billion as of November. https://www.bernama.com/en/news.php/general/crime_courts/news.php?id=2500014

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27-40. https://doi.org/10.3316/QRJ0902027

Braun, V. and Clarke, V. (2013). Successful qualitative research: A practical guide for beginners. Sage.

Clubb, A. C. and Hinkle, J. C. (2015). Protection motivation theory as a theoretical framework for understanding the use of protective measures. Criminal Justice Studies, 28(3), 336-355. https://doi.org/10.1080/1478601X.2015.1050590

Cohen, L. E. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608. https://doi.org/10.2307/2094589

Cressey, D. R. (1953). Other people's money: A study in the social psychology of embezzlement. Free Press.

Creswell, J. W. and Miller, D. L. (2000). Determining validity in qualitative inquiry. Theory Into Practice, 39(3), 124-130. https://doi.org/10.1207/s15430421tip3903_2

Creswell, J. W. and Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). Sage.

Crossler, R. E. and Belanger, F. (2014). An extended perspective on individual security behaviours: Protection motivation theory and a unified security practices instrument. The DATA BASE for Advances in Information Systems, 45(4), 51-71. https://doi.org/10.1145/2691517.2691521

Cuadra, J. M., Mandras, Y. S., Raya, M. R., Belardo, H. B., Lopez, R. P., and Rodriguez, J. G. E. (2025). Experiencing investment scams in the Philippines: An interpretative phenomenological analysis of victims' financial decision-making. Review of Behavioral Finance, 17(5), 769-784. https://doi.org/10.1108/RBF-03-2025-0116

CyberSecurity Malaysia. (2025). MyCERT incident statistics. https://www.mycert.org.my/portal/statistics-content

De Kimpe, L., Walrave, M., Verdegem, P., and Ponnet, K. (2022). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour and Information Technology, 41(8), 1796-1808. https://doi.org/10.1080/0144929X.2021.1905066

Denzin, N. K. and Lincoln, Y. S. (2011). The SAGE handbook of qualitative research (4th ed.). Sage.

Department of Statistics Malaysia. (2025). ICT use and access by individuals and households survey report 2024. https://www.dosm.gov.my

Du, W. and Chen, M. (2023). Too much or less? The effect of financial literacy on resident fraud victimization. Computers in Human Behavior, 148, 107914. https://doi.org/10.1016/j.chb.2023.107914

Elueze, I. and Quan-Haase, A. (2018). Privacy attitudes and concerns in the digital lives of older adults: Westin's privacy attitude typology revisited. American Behavioral Scientist, 62(10), 1372-1391. https://doi.org/10.1177/0002764218787026

Eshet, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. Journal of Educational Multimedia and Hypermedia, 13(1), 93-106.

Ferrari, A. (2012). Digital competence in practice: An analysis of frameworks. Publications Office of the European Union.

Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. Journal of Applied Social Psychology, 30(2), 407-429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Gilster, P. (1997). Digital literacy. Wiley.

Haag, S., Siponen, M., and Liu, F. (2021). Protection motivation theory in information systems security research. ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 52(2), 25-67. https://doi.org/10.1145/3462766.3462770

Holtfreter, K., Reisig, M. D., and Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. Criminology, 46(1), 189-220. https://doi.org/10.1111/j.1745-9125.2008.00101.x

Huston, S. J. (2010). Measuring financial literacy. Journal of Consumer Affairs, 44(2), 296-316. https://doi.org/10.1111/j.1745-6606.2010.01170.x

Jenkins, J. L., Grimes, M., Proudfoot, J. G., and Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. Information Technology for Development, 20(2), 196-213. https://doi.org/10.1080/02681102.2013.814040

Kvale, S. and Brinkmann, S. (2009). Interviews: Learning the craft of qualitative research interviewing (2nd ed.). Sage.

Lincoln, Y. S. and Guba, E. G. (1985). Naturalistic inquiry. Sage.

Lusardi, A. and Mitchell, O. S. (2007). Baby boomer retirement security: The roles of planning, financial literacy, and housing wealth. Journal of Monetary Economics, 54(1), 205-224. https://doi.org/10.1016/j.jmoneco.2006.12.001

Lusardi, A. and Mitchell, O. S. (2014). The economic importance of financial literacy: Theory and evidence. Journal of Economic Literature, 52(1), 5-44. https://doi.org/10.1257/jel.52.1.5

Martens, M., De Wolf, R., and De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams, and cybercrime in general. Computers in Human Behavior, 92, 139-150. https://doi.org/10.1016/j.chb.2018.11.002

Milne, S., Orbell, S., and Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. British Journal of Health Psychology, 7(2), 163-184. https://doi.org/10.1348/135910702169420

OECD. (2018). OECD/INFE toolkit for measuring financial literacy and financial inclusion. OECD.

OECD. (2020). OECD/INFE 2020 international survey of adult financial literacy. OECD.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo and R. E. Petty (Eds.), Social psychophysiology: A sourcebook (pp. 153-176). Guilford Press.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., and Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers and Security, 53, 65-78. https://doi.org/10.1016/j.cose.2015.05.012

Savin-Baden, M. and Major, C. H. (2013). Qualitative research: The essential guide to theory and practice. Routledge.

Schreier, M. (2012). Qualitative content analysis in practice. Sage.

Schwartz, S. H. (1992). Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. In M. P. Zanna (Ed.), Advances in experimental social psychology (Vol. 25, pp. 1-65). Academic Press. https://doi.org/10.1016/S0065-2601(08)60281-6

Schwartz, S. H., Cieciuch, J., Vecchione, M., Davidov, E., Fischer, R., Beierlein, C., Ramos, A., Verkasalo, M., Lonnqvist, J. E., Demirutku, K., Dirilen-Gumus, O., and Konty, M. (2012). Refining the theory of basic individual values. Journal of Personality and Social Psychology, 103(4), 663-688. https://doi.org/10.1037/a0029393

Statista. (2024). Mobile banking transaction value in Malaysia. https://www.statista.com

Tsai, H.-Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., and Cotten, S. R. (2016). Understanding online safety behaviours: A protection motivation theory perspective. Computers and Security, 59, 138-150. https://doi.org/10.1016/j.cose.2016.02.009

Van Wilsem, J. (2013). Bought it, but never got it: Assessing risk factors for online consumer fraud victimization. European Sociological Review, 29(2), 168-178. https://doi.org/10.1093/esr/jcr053

Vousinas, G. L. (2019). Advancing theory of fraud: The S.C.O.R.E. model. Journal of Financial Crime, 26(1), 372-381. https://doi.org/10.1108/JFC-12-2017-0128

Wilkinson, D. and Knijnenburg, B. P. (2022). Many islands, many problems: An empirical examination of online safety behaviors in the Caribbean. *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, Article 87, 1–15. https://doi.org/10.1145/3491102.3517643

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model. Communication Monographs, 61(2), 113-134. https://doi.org/10.1080/03637759409376328

Wolfe, D. T. and Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. The CPA Journal, 74(12), 38-42.

World Bank. (2025). Individuals using the Internet (% of population): Malaysia. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=MY