# Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand

**Teera Kulsawat**
College of Innovation and Management, Suan Sunandha Rajabhat University, Thailand
Author: teera@buu.ac.th

**Tanapol Kortana**
Faculty of Political Science and Law, Burapha University, Thailand
Corresponding: tanapol.ko@ssru.ac.th

| Received: February 06, 2026 | Revised: March 05, 2026 | Accepted: March 31, 2026 |
|---|---|---|

**Abstract**
Investment scams have become one of the most financially damaging forms of cyber-enabled fraud in Thailand and across Southeast Asia. Much of the available evidence is survey- or administrative-data driven (e.g., Kraiwanit, 2025), which is well suited to estimating prevalence and correlates but less able to reconstruct the psychological mechanisms and interactional scripts that sustain victim commitment during the offence. This qualitative case study addresses that gap by examining (i) how perpetrators orchestrate investment deception, (ii) why individuals become victims, (iii) the multi-dimensional impacts of victimization, and (iv) practical prevention measures at individual, platform, banking, and policy levels. Using purposive sampling, we conducted in-depth semi-structured interviews with 27 key informants: 17 victim-survivors, 5 officials/scholars involved in victim assistance and prevention, and 5 individuals who reported participation in scam operations. The analysis indicates a staged scam lifecycle: exposure and grooming on social platforms; credibility engineering via 'team leader' narratives, testimonials, and simulated returns; onboarding to controlled apps or web platforms; escalation through top-up pressure and borrowing; and lock-in via withdrawal blocks, fabricated fees, and threats. Risk factors cluster around low investment and digital literacy, social proof from acquaintances, persuasive legitimacy cues, and time-pressure tactics that amplify fear of missing out. Impacts extend beyond financial loss to indebtedness, psychological distress, family conflict, and erosion of trust in digital services. Building on these findings and recent international evidence on industrial-scale scam centres in Southeast Asia (e.g., UNODC, 2025), we propose an integrated prevention framework with four core components: (1) recognition through scenario- and script-based education ('cyber vaccine'); (2) containment through platform verification, advertising controls, and rapid takedown of repeat recruitment accounts; (3) transactional friction through risk-scored banking safeguards (e.g., step-up verification and cooling-off delays) at high-risk transfer moments; and (4) rapid response through simplified reporting, fast freezing/recall protocols, and victim-support pathways (Akesson et al., 2023; Global Anti-Scam Alliance & Feedzai, 2024; INTERPOL, 2025; Payment Systems Regulator, 2025; UNODC, 2025).
**Keywords:** **C**yber-enabled fraud; Investment scams; Pig butchering; Scam centres; Authorised push payment (APP) fraud; Social engineering; Behavioural economics; Qualitative interviews; Thailand; Prevention

## Introduction

Cyber-enabled investment scams have expanded rapidly as offenders exploit the scale of social platforms, the intimacy of messaging apps, and the speed of modern payment rails. Unlike traditional fraud that depends on face-to-face interaction or localized deception, online investment scams can be operated as semi-industrial systems: scripted outreach, standardized persuasion sequences, and controlled interfaces that simulate trading or investment performance. In Southeast Asia, investigative journalism and international monitoring reports increasingly describe scam centres as transnational and organized, with laundering infrastructure and cross-border mobility that frustrate single-jurisdiction enforcement. The United Nations Office on Drugs and Crime (UNODC) has highlighted a major "spillover" in which scam operations originally concentrated in border areas expand into broader regions and diversify targets globally (UNODC, 2025) (Europol, 2025; European Payments Council, 2025).

Thailand is not immune to these dynamics. Victims routinely encounter investment pitches promising returns that exceed regulated financial products, often framed as algorithmic trading, cryptocurrency, foreign exchange, or "exclusive" online opportunities. In this study, "investment scams" refers to cyber-enabled schemes that induce victims to transfer funds to offenders under the pretense of investing, including fake trading platforms, digital Ponzi schemes, and relationship-based long-cons that culminate in a fabricated investment interface (often termed 'pig butchering') (Han & Button, 2025; UNODC, 2025). The most dangerous aspect is not only the initial deception but the escalation pathway: after the first deposit, victims are encouraged to add funds repeatedly, sometimes borrowing from relatives or taking loans, because the platform displays unrealized gains and frames additional payment as the only route to withdrawal.


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

Recent administrative data underscore the scale of the problem. Thailand's Anti-Online Scam Operation Center (AOC 1441) reported that between November 2023 and October 2024, it received 1,176,512 hotline calls, suspended 348,006 suspicious accounts, and prevented approximately THB 19 billion in potential losses (Public Relations Department, 2024). Consistent with international evidence that rapid freezing is time-sensitive (Akesson et al., 2023; UNODC, 2025), these figures suggest that prevention and response capacity in Thailand must be evaluated not only by awareness metrics but also by operational indicators such as time-to-suspend accounts and time-to-freeze transfers.

Although awareness campaigns exist, many interventions focus on generic cautions (e.g., "don't trust strangers") rather than the process mechanisms by which victims are persuaded, escalated, and kept engaged. Qualitative research is particularly useful for reconstructing those mechanisms in detail, including moment-to-moment decision points, emotional states, and the scripts that defeat generic warnings. This study contributes a Thailand-focused, triangulated qualitative model based on three informant groups (victims, responders, and self-reported scam participants) to explain how exposure pathways, credibility cues, behavioural biases (e.g., sunk-cost and escalation dynamics), and payment/infrastructure features interact to produce escalation and lock-in, and to translate those mechanisms into concrete, stage-specific prevention measures suitable for evaluation (Federal Trade Commission, 2024; Payment Systems Regulator, 2025).

## Literature Review

### Online investment fraud as a scripted persuasion process

Recent peer-reviewed work on scam victimization emphasizes that modern fraud frequently operates through structured sequences rather than single deceptive messages. Childs (2024), for example, analyzes how cryptocurrency communities discuss scams and develop norms and countermeasures, illustrating how scam narratives become a shared interpretive resource in online settings. Qualitative research on other fraud types, such as romance fraud, also documents multi-dimensional impacts and the role of emotion and shame in shaping reporting and recovery (Cole, 2024; Drew & Webster, 2024). While romance fraud differs in content, it shares key persuasion mechanisms with investment scams: trust-building, social proof, authority performance, and time pressure (Han & Button, 2025; Wang et al., 2024).

Investment scams often exploit credibility cues that approximate institutional legitimacy: professional dashboards, fabricated licensing claims, controlled "customer service," and staged proof-of-payment. In long-con forms, offenders may even allow a small withdrawal early to convert uncertainty into commitment. The logic is straightforward: once a victim believes the system is real and has personally experienced a payout, subsequent warnings lose credibility, and the victim's confidence rises, increasing willingness to deposit more (Xiao et al., 2025; UNODC, 2025).

### Victimization risk, routine activity, and the role of literacy

Victimization research frequently links fraud risk to exposure patterns and routine online activities. Studies grounded in Routine Activity Theory (RAT) emphasize that everyday online routines, platform choice, and the availability of persuasive contact points create opportunity structures for fraud (Cohen & Felson, 1979). Complementing these approaches, research also highlights the importance of financial and digital literacy. In Thailand, Kraiwanit (2025) uses survey data and logistic regression to identify predictors of digital fraud exposure, including demographic and behavioral variables such as device use and social media engagement. Such findings reinforce the relevance of exposure pathways, but they often cannot specify the micro-process of how persuasion unfolds across time. Qualitative case evidence can supply that missing mechanism: which cues shift a person from "curious" to "committed," which pressures trigger escalation, and why victims may continue paying after doubts emerge (Akesson et al., 2023; European Banking Authority & European Central Bank, 2025). These mechanism-focused insights also align with situational crime prevention perspectives that prioritize practical, stage-specific levers to reduce opportunity and increase the effort and risk faced by offenders (Clarke, 1995).

### Behavioral economics, commitment, and escalation

Behavioural economics helps explain why losses can compound after an initial deposit. Under conditions of uncertainty and manipulated feedback, victims may exhibit sunk-cost reasoning, escalation of commitment, and loss aversion: paying an additional "fee" is framed as the least-bad route to recover what has already been transferred (Kahneman & Tversky, 1979; Staw, 1976). Policy-oriented research on authorised push payment (APP) fraud similarly highlights how time pressure, authority cues, and


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

transaction design interact with these biases to reduce verification and increase compliance (Payment Systems Regulator, 2025). These mechanisms support an interpretation of escalation as predictable behaviour under engineered conditions, which helps move the analysis beyond simplistic victim-blaming explanations and toward testable, designable prevention levers (Akesson et al., 2023).

Industrialization and transnational scam centres (Global Initiative Against Transnational Organized Crime, 2025; INTERPOL, 2025)

Beyond individual-level risk, the broader governance context matters. UNODC (2025) documents industrial-scale scam centres, underground banking, and illicit online marketplaces in Southeast Asia, highlighting both the rapid adaptability of criminal networks and the convergence of scam operations with other forms of organized crime. This industrialization changes prevention requirements: it is unrealistic to treat scams as isolated incidents. Instead, effective response requires coordinated interventions across platforms, financial institutions, and cross-border enforcement, as well as victim-support services that reduce under-reporting and secondary harms (Global Initiative Against Transnational Organized Crime, 2025; Asia/Pacific Group on Money Laundering, 2024).

In Thailand, the prevention landscape has been shaped by both institutional coordination and legal measures that target the payment and telecommunications enablers of scams. Alongside the establishment of the AOC 1441 one-stop hotline and coordination mechanisms (Public Relations Department, 2024), the Royal Decree on Measures for the Prevention and Suppression of Technological Crime B.E. 2566 (2023) provides a legal basis for coordinated action against technology-enabled fraud and the use of mule accounts (Royal Decree on Measures for the Prevention and Suppression of Technological Crime B.E. 2566, 2023). Situating the present findings within this Thai policy context clarifies how lifecycle-based prevention can complement existing mandates (e.g., by operationalizing script-based warnings and measurable time-to-freeze indicators).

Recent developments also indicate a shift from 'traditional' scam scripts toward AI- and deepfake-enabled deception that can accelerate credibility engineering and impersonation. Analyses of Asia-Pacific fraud trends highlight how synthetic media, voice cloning, and deepfake video can be integrated into scam workflows to raise perceived legitimacy and reduce victims' willingness to verify (Global Initiative Against Transnational Organized Crime, 2024; INTERPOL, 2025). This evolution strengthens the case for prevention strategies that rely on verifiable provenance (credential checks, account verification, and transaction-level safeguards) rather than subjective impressions of professionalism.

Countermeasures: education, friction, and rapid response (European Central Bank, 2024; European Payments Council, 2025; Australian Competition and Consumer Commission, 2024)

Evidence from policy and applied research suggests that prevention works best when it is layered. Education is necessary but insufficient if delivered abstractly. Scenario-based warnings that match real scripts and decision points are more likely to trigger verification behavior. Banking and payments interventions can add "friction" at high-risk moments through step-up authentication, cooling-off delays for suspicious transfers, and rapid freezing protocols. Platform interventions include tighter controls on high-risk investment advertising, verification for entities promoting financial products, and detection of recruitment patterns consistent with organized abuse. Importantly, victim-centred reporting pathways, with easy evidence preservation, no-blame communication, and rapid banking coordination, can reduce time-to-intervention and improve recovery chances (Akesson et al., 2023; Federal Trade Commission, 2024; Payment Systems Regulator, 2025).

## Methodology

### Design

This research uses a qualitative case study design and semi-structured in-depth interviews to reconstruct the process of investment scams and identify prevention levers. A qualitative approach was selected because investment scams involve interactional and emotional dynamics that are difficult to capture using survey instruments alone.

### Participants and sampling

Purposive sampling was used to recruit informants with direct experience relevant to the study aims. The final sample comprised 27 participants in three groups: (1) 17 victim-survivors of investment scams; (2) 5 officials/scholars involved in fraud response, prevention, or victim support; and (3) 5 individuals who self-reported participation in scam operations. Recruitment pathways reflected these groups: victim-survivors were approached through victim networks and referrals; officials/scholars through institutional and professional networks; and self-reported scam participants through snowball


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

referrals (Table 1). Inclusion criteria required that participants be adults (18+), capable of providing informed consent, and able to describe concrete episodes or workflows relevant to at least one stage of the scam lifecycle (exposure, credibility engineering, onboarding, escalation, lock-in, and aftermath). Because operational participation was self-reported and legally sensitive, interviews with scam-operation informants focused on general scripts, platform workflows, and decision logic rather than soliciting identifying details about specific organizations, locations, or accomplices; analytic claims are therefore interpreted in conjunction with victim and official accounts as part of a triangulated case model.

**Data collection**

Interviews followed a semi-structured guide covering exposure pathways, persuasion tactics, platform features, transaction sequences, emotional responses, reporting experiences, and prevention recommendations. Interviews were conducted in Thai to support participant comfort and narrative detail; transcripts were analyzed in Thai, and analytic summaries and illustrative excerpts were translated into English for reporting. To maintain conceptual equivalence across languages, translations prioritized meaning-based rendering of key constructs (e.g., "team leader," "VIP level," "fee to withdraw") and were iteratively reviewed against the original Thai phrasing during analysis and write-up.

**Data analysis and trustworthiness**

Transcripts were coded using iterative thematic analysis. First-cycle coding identified tactics, cues, emotions, decision points, and outcomes. Second-cycle coding grouped these codes into themes aligned with the scam lifecycle (exposure, trust-building, onboarding, escalation, lock-in, aftermath) and mapped them to prevention levers. Trustworthiness was strengthened through triangulation across informant groups, analytic memoing, and negative case analysis.

**Ethics**

All participants provided informed consent. Confidentiality protections were applied, including de-identification and removal of potentially identifying details. The study received institutional ethics approval (Approval No. HU097/2566-C2). Given the potential for distress when recounting victimization, interviews with victim-survivors used a trauma-informed approach: participants could decline any question, take breaks, or stop the interview at any point; interviews were paced to prioritize safety; and participants were provided with information on available support services if they experienced distress during or after the interview. For self-reported scam-operation informants, the protocol avoided collecting identifying details that could increase legal risk while still enabling discussion of general scripts and operational workflows.

## Results

**Exposure and entry channels: how victims first encounter the scam**

Victims described three main entry channels. The first involved social media advertisements that promised unusually high returns while presenting investment as simple and accessible. These advertisements often used polished visuals, screenshots of trading dashboards, and narratives that implied a limited-time opportunity. Some victims reported that ads framed the opportunity as "safer than banks" or as an "exclusive method" that ordinary people could finally access. The second channel involved unsolicited direct messages. Victims described contacts initiating conversation with friendly, low-risk prompts ("wrong number," casual friendship, or business networking), gradually shifting the topic toward investment. The third and especially powerful channel involved acquaintances. In these cases, victims interpreted the invitation as a social recommendation rather than a commercial pitch. Group chats amplified this effect by creating a visible audience of apparent participants, reinforcing the sense of legitimacy.

Across channels, exposure did not immediately translate into loss. Many victims described a short "curiosity window" in which they explored the opportunity, asked questions, and observed others. This window is crucial for prevention because it is the stage at which verification is still psychologically and financially cheap. Once deposits begin, the victim's mental model changes: the goal becomes recovery or growth, not evaluation. Therefore, interventions that target exposure must be designed to enter the victim's attention during this curiosity window through timely warnings, recognizable red flags, and easy verification tools.

**Credibility engineering: how legitimacy is manufactured**


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

Credibility engineering refers to the layered construction of legitimacy cues that reduce suspicion and create perceived safety. Victims described identity cues (mentor status, professional titles, claims of affiliation), platform cues (interfaces that resemble legitimate trading systems), and social cues (testimonials, "success stories," and visible group participation). In some narratives, credibility was reinforced through procedural complexity: forms, "KYC checks," "compliance requirements," and "customer service" interactions that looked like regulated processes. This complexity can paradoxically increase trust because it mimics bureaucratic legitimacy. Victims may reason that a scam would not invest in such elaborate procedures (Global Initiative Against Transnational Organized Crime, 2024).

A particularly influential technique was the staged payout. Several victims described being able to withdraw a small amount early. This experience functioned as personal evidence: it transformed the victim's uncertainty into confidence. Scam participants described this technique as strategic: allowing a small withdrawal is viewed as an investment that increases the probability of large downstream deposits. Once the victim has personally received money, warnings become less persuasive because the victim can point to "proof" and interpret skepticism as ignorance. In psychological terms, the payout creates a private anchor that is hard to dislodge.

Credibility engineering also included "technical theatre." Victims described charts, signals, and market commentary that created an impression of expertise. Even when victims did not fully understand the technical content, they interpreted complexity as competence. This observation is consistent with the broader fraud literature: when people lack domain knowledge, they rely more heavily on peripheral cues such as confidence, professionalism, and social endorsement. Therefore, literacy-building remains important, but it should be paired with tools that reduce reliance on peripheral cues by making verification simple and concrete.

**Escalation: urgency, 'VIP' progression, and sunk-cost dynamics**

Escalation began after the first deposit. Victims described a shift from exploration to performance: they were encouraged to "follow instructions" to maximize profit, often through tasks that required additional deposits. A recurring structure was the 'VIP' progression. Victims were told that higher deposit tiers unlock better returns, better algorithm access, or faster withdrawals. Scarcity framing was used to compress decision time: limited slots, limited-time bonuses, or a market window that would close. In group contexts, escalation was socially reinforced: participants congratulated each other on reaching higher tiers, and hesitation was reframed as missing out.

Sunk-cost reasoning became a central mechanism. After victims deposited money, they increasingly believed that withdrawal was the only rational endpoint. When the platform introduced new fees, victims faced a painful choice: accept loss or pay additional fees to recover the original investment and accumulated "profits." Many chose the latter, interpreting fees as an unfortunate but temporary obstacle. Scam participants recognized and exploited this logic by designing the system to keep withdrawal just within reach, close enough to motivate payment, but never achievable without additional charges. This pattern produces compounding loss and is one reason investment scams can be financially catastrophic.

Escalation was also linked to borrowing. Some victims described borrowing from friends or taking loans because they believed they were "close to withdrawal." This is a key harm multiplier: the victim's loss is no longer limited to savings but expands into debt. Therefore, transactional friction at the banking layer is especially valuable during escalation. Even short delays or step-up verification can create a pause that interrupts urgency and allows victims to consult others.

**Lock-in: withdrawal obstruction, fees, and threats**

Lock-in refers to mechanisms that prevent withdrawal and maintain victim engagement after suspicion emerges. Victims reported that when they attempted to withdraw substantial funds, the platform introduced new requirements: taxes, verification fees, security deposits, "anti-money-laundering" reviews, or account upgrades. Requirements changed over time and were applied inconsistently, which created confusion and reduced the victim's ability to evaluate legitimacy. Support channels often responded with scripted reassurance and shifted blame onto the victim ("you entered the wrong code," "your account is flagged," "the bank rejected your withdrawal"). These explanations encouraged the victim to treat the barrier as procedural rather than fraudulent.

Some victims described threats or intimidation, especially when they expressed doubt. Others reported being removed from group chats after questioning the scheme. Officials emphasized that shame and fear of blame delay reporting; victims sometimes attempted to solve the problem privately, paying


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

fees repeatedly, before approaching banks or police. This delay is crucial because recovery chances often decline rapidly over time as funds are laundered through multiple accounts.

Lock-in can be interpreted as a conversion from persuasion to coercion. Early stages rely on positive reinforcement (profits, praise, community), while lock-in relies on negative pressure (threats, fear of loss, procedural obstacles). Understanding this shift helps design interventions: victims in lock-in may not respond to educational messages, but they may respond to concrete guidance about immediate steps to stop paying fees, preserve evidence, contact the bank immediately, and report through a simplified pathway.

**The tipping point: when suspicion emerges**

Across victim narratives, suspicion most commonly emerged at the transition from escalation to lock-in, when the victim attempted a substantial withdrawal and encountered inconsistent explanations, shifting requirements, or demands to pay additional fees to "unlock" funds. Early doubts were often suppressed after a small initial payout or after reassurance from group-chat peers; however, repeated fee requests, sudden account "flags," or support responses that blamed the victim (e.g., "wrong code" or "bank rejected") increased cognitive dissonance and prompted some victims to consult friends, search online, or contact banks. These moments constitute actionable 'friction points' for prevention: well-timed, script-matched warnings and mandatory verification steps at attempted high-value withdrawals or repeated top-ups may interrupt the urgency loop and shorten the delay between suspicion and reporting (Akesson et al., 2023; Payment Systems Regulator, 2025).

**Impacts: financial loss, indebtedness, psychological harm, and social rupture**

Impacts were multi-dimensional. Financial harm ranged from manageable losses to life-altering debt. Victims reported losing savings, selling assets, and borrowing from relatives. Debt-related consequences included the inability to pay rent, the disruption of family finances, and long-term repayment burdens. Psychological harm included acute stress, insomnia, rumination, fear, and depressive symptoms. These harms were not merely emotional reactions; they shaped behavior by reducing problem-solving capacity and increasing avoidance. Several victims described difficulty concentrating at work and a persistent sense of shame.

Social harms included family conflict, blame, and erosion of trust. In cases where victims borrowed from relatives, relationships were strained or ruptured. Some victims avoided disclosure, which increased isolation and delayed reporting. Officials and scholars described a recurring pattern: victims often appear at police stations only after losses are severe, when recovery chances are low. This sequence reinforces public discouragement ("reporting is useless"), further reducing future reporting.

Finally, victims described long-term erosion of trust in digital finance. Even when they returned to online banking and legitimate platforms, they reported heightened suspicion and reduced willingness to invest. This "trust damage" has broader social costs because it can reduce participation in legitimate digital services and undermine confidence in institutions. These findings are consistent with international qualitative work that documents the broad impact of scam victimization beyond financial loss (Cole, 2024; Drew & Webster, 2024).

**Evaluation-ready indicators (how to measure prevention success)**

One advantage of a lifecycle-based model is that it yields clear outcome indicators. For platform interventions, indicators include: reduced exposure to scam recruitment (measured by takedown rates and user reports), reduced ad reach for unverified investment promoters, and reduced recurrence of identified recruitment accounts. For banking interventions, indicators include: reduced repeated-transfer sequences, increased completion of verification steps after warnings, reduced average transfer size during suspected escalation episodes, and increased successful recall/freezing events.

For public education and victim-support interventions, indicators include: improved recognition of core scam scripts, increased use of verification tools, reduced average delay between suspicion and reporting, and improved victim satisfaction with reporting pathways. At the system level, agencies can track time-to-freeze as a key performance indicator because it directly relates to recoverability. These indicators can be monitored over time to support iterative improvement and resource allocation.

**Implementation Playbook (one-page operational steps)**

This section converts the recommendations into a compact playbook that agencies and institutions can adapt.

Step 1: Define the high-risk script library. Compile the most common persuasion scripts observed in this study (e.g., "team leader mentorship," "VIP level unlock," "fee to withdraw," "today-



**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

only market window"). For each script, create: (a) a plain-language description, (b) example messages, (c) the recommended user action (pause, verify, report), and (d) the corresponding institutional action (platform review, bank friction, law enforcement referral). Maintain the library as a living document updated quarterly.

Step 2: Embed "pause-and-verify" prompts at decision points. Public campaigns should be synchronized with platform and banking prompts so users see consistent messages. For example, when a transfer is flagged as suspicious, the warning should not merely say "be careful"; it should match the script: "Scammers often show profits but block withdrawals and demand fees. Do not pay fees. Contact your bank now." Consistency across channels reduces confusion.

Step 3: Establish rapid response routines. Banks should implement a standard operating procedure for suspected scam transfers: collect minimum information (transfer receipt, beneficiary account, platform name/URL, chat identifiers), initiate internal fraud escalation, and if criteria are met, trigger freezing/recall attempts and notify designated law enforcement contacts. Agencies should provide standardized forms and ensure victims can complete them with minimal burden.

Step 4: Protect victims and normalize reporting. Design reporting pathways that minimize shame: no-blame language, clear explanation that manipulation is the offender's strategy, and reassurance that early reporting is always worthwhile. Provide referrals for counselling and debt-management services to reduce secondary harms and improve cooperation.

Step 5: Audit and iterate. Use the evaluation indicators in Section 11 to monitor performance. Conduct quarterly reviews to identify bottlenecks (e.g., delays in freezing, low completion of verification steps, high recurrence of recruitment accounts). Implement targeted improvements and retest. Because scam operations adapt, prevention must also adapt.

**Extended Discussion: linking Thailand evidence to global trends**

The Thai narratives documented here reflect global trends, but also highlight localized mechanisms. Globally, organized scam operations increasingly combine relationship-building with fabricated financial interfaces. Childs (2024) shows how cryptocurrency communities interpret scam risk and attempt self-protection, indicating that scams are embedded in online ecosystems rather than isolated events. UNODC (2025) further emphasizes the scale and adaptability of scam centres, underscoring that national prevention cannot rely solely on local policing; it requires cross-border cooperation and disruption of laundering infrastructure.

Locally, Thailand-specific credibility cues were notable. Victims often evaluated legitimacy using everyday heuristics: whether others in a group chat appeared successful, whether the mentor used professional language, and whether the platform resembled familiar financial apps. These heuristics are understandable responses to uncertainty, especially among individuals with limited investment literacy. However, offenders exploit them systematically. This insight implies that literacy programs should teach not only "facts about investing" but also "how legitimacy is faked," including the strategic use of complexity, testimonials, and staged withdrawals.

Another implication concerns the ethics of terminology. If society frames victims as "greedy" or "careless," victims will conceal losses and delay reporting. The narratives indicate that shame is a practical barrier to intervention because it increases time-to-reporting. Therefore, victim-sensitive messaging is a prevention tool, not only a humanitarian preference. The most effective messaging balances accountability with empathy: it encourages verification and caution while acknowledging that offenders are skilled and organized.

Finally, the study emphasizes the need to integrate platform governance with financial regulation. Many scams begin with platform recruitment but culminate in bank transfers. If platforms and banks act separately, offenders exploit gaps. Coordinated protocols, shared warning scripts, aligned verification requirements, and synchronized reporting pathways can reduce the offender's advantage. This "systems alignment" is particularly important under conditions of industrialized scam centres, where offender adaptation is rapid, and displacement is common.

**Plain-Language Summary (for practitioners and the public)**

This study explains how many investment scams work as a step-by-step process. First, scammers contact people through social media ads, direct messages, or someone the victim knows. Then they build trust by acting like a mentor and showing a professional-looking "investment" platform. They may allow


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

the victim to withdraw a small amount at the beginning to prove the system is "real." After that, they pressure the victim to deposit more money using urgency ("only today," "limited slots") and tiered ...

When the victim tries to withdraw a large amount, the platform suddenly blocks the withdrawal and asks for more payments, such as "tax," "verification," or "security deposits." Victims often pay because they believe it is the last step to get their money back. Losses become larger when victims borrow money or take loans. Many victims feel ashamed, so they delay reporting, and delays reduce the chance of freezing funds. The best response is to stop early: verify licences, avoid installing apps outside official ...

**Sensitivity Analysis of the Qualitative Frequency Tables**

Tables 4 and Figures 2–3 present qualitative frequency counts and normalized salience indicators. These values are included to improve transparency and to help readers see how strongly particular themes appeared across the three informant groups. However, such counts should not be interpreted as population prevalence or as statistical effect sizes. They depend on interview structure, narrative richness, and the analytic choice to count "mentions" rather than "participants."

To check robustness, we considered whether the main conclusions depend on any single counting rule. The lifecycle model is robust because it emerges from process descriptions rather than counts: exposure, credibility engineering, onboarding, escalation, lock-in, and collapse were present as narrative sequences even when individual tactics varied. Likewise, the cross-group convergence conclusion is robust because scam participants independently described designing credibility cues and urgency scripts, while officials independently described delayed reporting and freezing bottlenecks. These convergences remain visible even if counts are removed.

Future mixed-method work can formalize these signals by constructing survey measures of stage exposure (e.g., "Was a small withdrawal allowed?" "Were you asked to pay fees before withdrawal?") and by modeling escalation pathways quantitatively. The qualitative counts here, therefore, serve as scaffolding for testable measurement, not as final inference.

**Table 1. Participant profile (n = 27)**

| Group | n | Typical age range | Recruitment channel | Analytic contribution |
|---|---|---|---|---|
| Victim-survivors | 17 | 20–60+ | Victim networks/referrals | Decision points, losses, impacts |
| Officials/Scholars | 5 | 30–60 | Institutions / professional networks | Reporting, response capacity, and prevention |
| Self-reported scam participants | 5 | 20–40 | Snowball/referrals | Operational scripts, platform control |

Analysis of Table 1: The sample was designed to triangulate lived victim experience with system-level response and operational insight. Victims provided detailed timelines and emotional states; officials highlighted bottlenecks in reporting and fund freezing; and self-reported scam participants clarified scripted tactics and the logic of staged payouts and withdrawal obstruction.

**Scam lifecycle: stages, tactics, and warning cues**


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

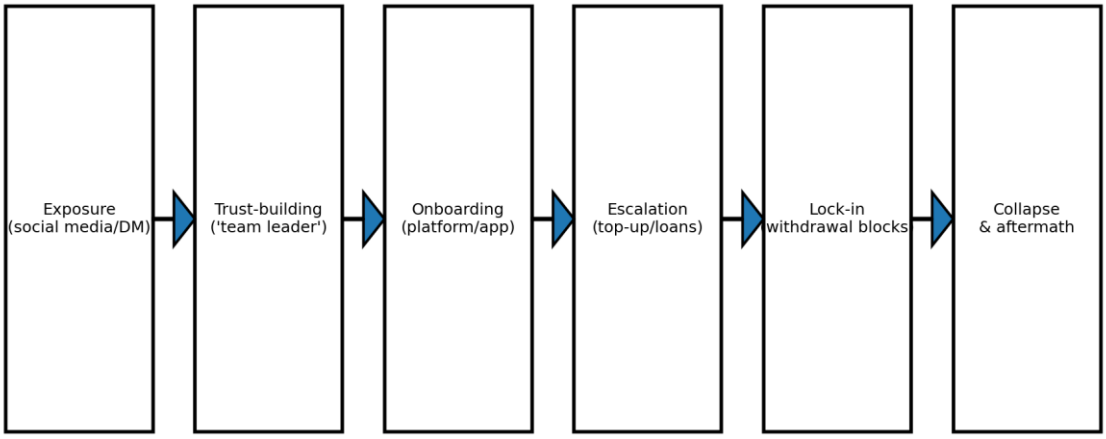



Figure 1. Conceptual lifecycle of cyber-enabled investment scams derived from interview narratives

Interpretation of Figure 1: Accounts across participant groups converged on a staged lifecycle. Victims were initially exposed through ads, direct messages, or acquaintances. Trust-building relied on a mentor-like 'team leader' identity, testimonials, and staged demonstrations of profit. Onboarding shifted victims into a controlled environment (apps or websites) that simulated trading. Escalation was driven by urgency scripts and 'VIP' progression that normalized repeated deposits. Lock-in occurred when victims attempted large withdrawals and were confronted with new fees, identity checks, or threats. The cycle ended with disappearance, blame-shifting, or attempts to recycle victims into new schemes.

Table 2. Core themes and operational definitions from thematic coding

| Theme | Definition | Illustrative indicators |
|---|---|---|
| Credibility engineering | Tactics used to create perceived legitimacy and reduce suspicion. | Fake licences, mentor identity, testimonials, and early small payouts |
| Escalation pressure | Techniques that increase deposits over time via urgency and sunk-cost dynamics. | Deadlines, 'VIP levels', loan encouragement, repeated top-ups |
| Social proof via ties | Use of acquaintances/community cues to normalize participation. | Friend invitations, group chat hype, perceived consensus |
| Platform control and lock-in | Mechanisms to prevent withdrawal and prolong engagement. | Withdrawal fees, 'tax' demands, frozen accounts, scripted support |
| Multi-layered harm | Financial and psychosocial consequences after scam collapse. | Debt, anxiety, family conflict, stigma, reduced trust |
| Prevention levers | Interventions that can disrupt the lifecycle at specific stages. | Scenario warnings, verification, banking friction, and rapid freezing |

Analysis of Table 2: Themes form a coherent persuasion sequence. Credibility engineering initiates engagement, escalation pressure amplifies commitment, and platform control sustains lock-in. Because prevention levers map directly to these phases, interventions can be evaluated by where they interrupt the lifecycle (e.g., reduced onboarding completion, reduced repeated top-ups, shorter time-to-reporting).

Table 3. Scam lifecycle stages and predominant tactics (with suggested counteractions)


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

| Stage | Primary objective | Common tactics (examples) | Observable warning cues | Counter-actions |
|---|---|---|---|---|
| Exposure | Initiate contact and curiosity | Targeted ads, unsolicited DMs, 'investment tip' hooks | Unrealistic returns; unknown accounts | Pause and verify: check regulator/firm registration; distrust guaranteed high returns; report suspicious ads/accounts. |
| Trust-building | Reduce suspicion; create rapport | Mentor identity, testimonials, group chat hype | Pressure to move to private channels | Do not rely on group-chat 'success' claims; insist on independent verification; discuss with a trusted third party before transferring funds. |
| Onboarding | Shift the victim to a controlled interface | Fake apps/websites, guided registration, 'KYC' scripts | Sideloading; nonstandard URLs; opaque company details | Avoid installing apps outside official stores; check domain ownership and company details; stop if the platform cannot be verified. |
| Escalation | Increase deposit size/frequency | Top-up tasks, 'VIP' progression, borrowing suggestions | Deadlines; "account upgrade" pressure | Set a 'stop rule' for additional payments; treat "VIP upgrade" pressure as a red flag; contact your bank before any further transfer. |
| Lock-in | Prevent withdrawal; prolong deposits | Fees/taxes, frozen account claims, threats | Ever-increasing fees; inconsistent explanations | Never pay fees/taxes to unlock withdrawal; stop transferring immediately; preserve chats/receipts and request bank freezing/recall and report to AOC/police. |


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

| Stage | Primary objective | Common tactics (examples) | Observable warning cues | Counter-actions |
|---|---|---|---|---|
| Collapse | Exit/recycle victim | Ghosting, account deletion, blame-shifting | Disappearing contacts; no verifiable entity | Document losses and reporting steps; monitor accounts/credit; seek psychological and debt-support services; support follow-up investigations. |

Analysis of Table 3: Stage-specific warning cues suggest stage-specific interventions. The added counteractions column translates diagnostic cues into practical, stage-matched behaviours (e.g., verification during exposure/onboarding; 'stop rules' and bank consultation during escalation; and no-fee-to-withdraw guidance plus rapid reporting during lock-in). Early stages are best addressed through platform controls and scenario-based education, while escalation and lock-in require rapid banking coordination and clear reporting channels to reduce time-to-freeze.

**Salient risk factors and cross-group convergence**

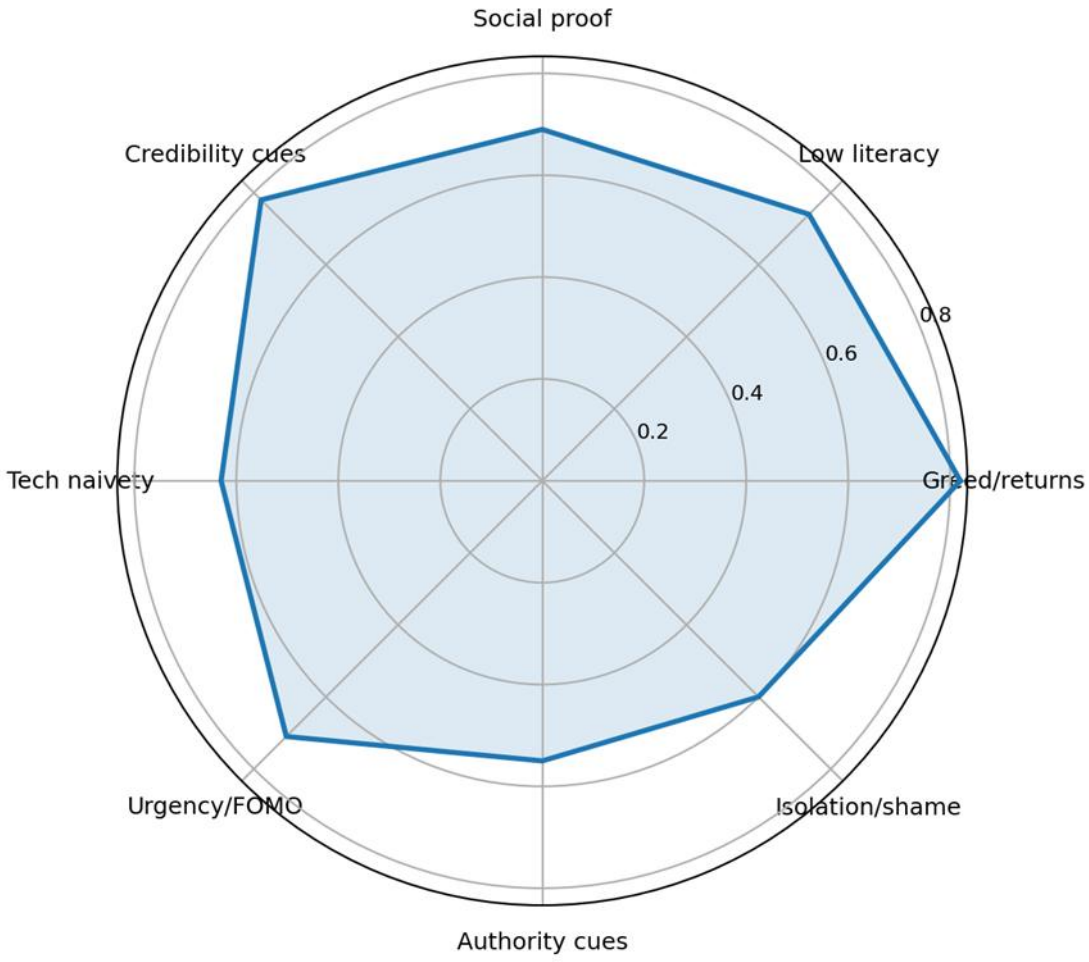



Figure 2. Theme salience across coded interviews (normalized)

Interpretation of Figure 2: 'High returns/greed' and 'credibility cues' were most salient, indicating that motivational pull and perceived legitimacy jointly drive escalation. 'Urgency/FOMO'



**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

was also prominent, consistent with time-pressure scripts. 'Isolation/shame' becomes more visible in lock-in and aftermath, shaping delayed reporting and social harm.

Table 4. Cross-group convergence on risk factors (mentions by group; qualitative frequency counts)

| Risk factor | Victims (n=17) | Officials/Scholars (n=5) | Scam participants (n=5) | Interpretive note |
|---|---|---|---|---|
| Low investment literacy | 14 | 5 | 4 | Misjudged risk/returns; scammers script 'education.' |
| High-return lure | 15 | 4 | 5 | Anchored against bank deposit rates and 'guarantees.' |
| Social proof via ties | 12 | 4 | 3 | Entry often via acquaintances and group chats |
| Credibility engineering | 13 | 5 | 5 | Fake evidence and staged withdrawals |
| Urgency and scarcity | 11 | 3 | 5 | Deadlines and 'VIP' progression compress decisions |
| Tech naivety/interface trust | 10 | 3 | 4 | Sideloaded apps and fake URLs bypass intuition |
| Shame and under-reporting | 9 | 4 | 2 | Stigma delays reporting; increases losses |

Analysis of Table 4: Convergence across informant groups strengthens credibility. Scam participants explicitly described designing credibility cues and urgency scripts, while officials emphasized under-reporting and delays in freezing funds as major amplifiers of loss. Frequency counts are presented as analytic aids rather than statistical inference.

**Co-occurrence of tactics and impacts**


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

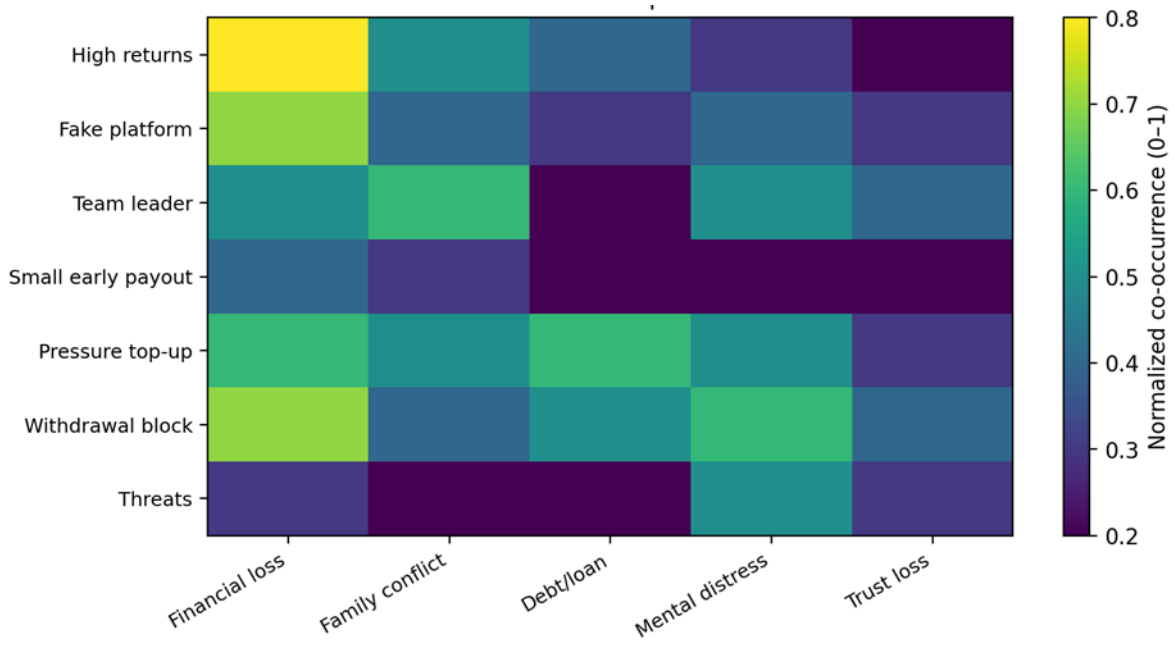



Figure 3. Co-occurrence of tactics and impacts in coded narratives

Interpretation of Figure 3: Withdrawal blocks and top-up pressure co-occur strongly with indebtedness and psychological distress, reflecting escalation beyond initial deposits. Mentor/'team leader' tactics co-occur with family conflict and trust loss, consistent with the role of social manipulation in isolating victims from alternative advice.

**Prevention recommendations mapped to stakeholders.**

Table 5. Prevention recommendations mapped to stakeholders and scam stages

| Stakeholder | Action | Targeted stage(s) | Implementation notes |
|---|---|---|---|
| Individuals | Pause-and-verify rules; verify licences; avoid 'fee to withdraw' logic | Exposure–Trust-building | Use regulator registries and bank advisories |
| Platforms/social media | Restrict high-risk ads; label unverified 'investment mentors'; detect recruitment patterns. | Exposure | Identity verification and abuse detection |
| Banks/payment providers | Risk-scored friction; step-up checks; cooling-off delays; rapid freezing protocols | Escalation–Lock-in | Hotlines and standardized reporting forms |
| Law enforcement | Specialized cyber units; cross-border cooperation; evidence preservation; victim-friendly reporting | All stages | Reduce reporting burden; improve triage |
| Education/public sector | Scenario-based 'cyber vaccine' campaigns and community outreach | Exposure–Trust-building | Target high-risk groups; normalize early reporting |


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

Analysis of Table 5: Recommendations are designed to interrupt the lifecycle early (platform governance and scenario-based education), reduce escalation (bank friction and limits), and minimize harm through rapid response (freezing and reporting). Because UNODC (2025) documents industrial-scale and transnational scam infrastructures, interventions require coordinated implementation across stakeholders rather than isolated campaigns.

## Discussion

The findings support a process-based view of investment scams in which persuasion and platform control reinforce each other. Credibility engineering is not merely cosmetic: it is a strategic investment that converts suspicion into commitment. The staged payout mechanism described by participants functions as behavioral proof, transforming victims' subjective uncertainty into confidence. Once confidence is established, escalation scripts exploit urgency, and sunk-cost reasoning, and victims become willing to pay additional fees because they interpret payment as a step toward recovering their initial deposits. Similar multi-stage logic is visible in global descriptions of long-con investment frauds and in qualitative analyses of scam victimization and community responses (Childs, 2024; Cole, 2024; Europol, 2025; INTERPOL, 2025; UNODC, 2025)

Cross-group triangulation helps explain why warnings often fail. Victims frequently recognize that returns are unusually high, yet credibility cues (mentor identity, testimonials, professional dashboards) and social proof from acquaintances create a sense that the opportunity is both legitimate and socially endorsed. The group-chat environment functions as social infrastructure: it supplies constant reinforcement, creates perceived consensus, and can isolate victims from dissenting advice. Officials' accounts further indicate that shame and fear of blame delay reporting, increasing losses as funds are rapidly laundered through multiple accounts. Taken together, these mechanisms challenge a simple victim-blaming narrative of "greed" and instead indicate that sophisticated, organized social engineering and transaction design make victimization a systemic governance issue (Cole, 2024; Payment Systems Regulator, 2025; UNODC, 2025).

At a policy level, the lifecycle model implies measurable intervention points. If platform controls reduce recruitment reach, fewer people enter the trust-building stage. If banking friction interrupts repeated top-ups and triggers 'time to think' during escalation, compounding losses may drop. If reporting channels are simplified and stigma is reduced, time-to-freeze can be shortened. These are evaluation-ready outcomes: onboarding completion rates, repeated-transfer patterns, time-to-reporting, and recovery success. Importantly, these outcomes align with the governance challenge described by UNODC (2025): industrialized scam centres and underground banking require multi-agency and cross-border coordination.

Thailand-specific infrastructure further shapes the lifecycle. PromptPay—a national real-time payment rail that enables instant transfers using identifiers such as mobile numbers or citizen IDs—has expanded convenience and transaction speed, but it also compresses the time available for verification and recovery once a victim is pressured into an authorised push payment (Bank of Thailand, n.d.; Bank of Thailand, 2024). Bank of Thailand reporting highlights the centrality of mule accounts to scam operations and documents large-scale suspension efforts and the institutional ecosystem required for rapid coordination (Bank of Thailand, 2024). At the communications layer, scam operations commonly rely on large inventories of SIM cards and device infrastructure to sustain mass outreach and account cycling, as documented in regional reporting on scam compounds (Reuters, 2026). These dynamics reinforce the need for aligned platform-banking-telecom interventions rather than isolated public awareness messaging.

## Practical Implications

### Public communication: from generic warnings to script-based 'cyber vaccine.'

Public messaging should prioritize recognizable scripts and decision points rather than abstract slogans. Victims repeatedly described being persuaded by early small withdrawals and the authority of a 'team leader'. Campaign materials can therefore highlight diagnostic red flags: requests to install apps outside official stores; pressure to move to private channels; 'guaranteed' high returns; and any demand to pay fees or taxes to unlock withdrawals. To increase effectiveness, distribution should be anchored to high-risk decision points: embed script-matched warnings directly into banking and payment apps during transfers to new beneficiaries or during repeated top-ups, and pair them with simple 'pause-and-


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

verify' actions (Akesson et al., 2023; Payment Systems Regulator, 2025). Platform-level interstitial warnings (e.g., when users click investment advertisements or join high-risk group chats) can further extend this 'cyber vaccine' approach beyond general PR into context-specific prevention.

**Banks and payment providers: friction, triage, and rapid freezing**

Banks can use behavioural signals to trigger protective friction: repeated transfers that increase in amount, transfers to newly opened accounts, unusual timing, or transfers following a spike in customer support contact. Beyond generic warnings, a practical option is a tiered 'Safe Mode' for high-risk behaviours (e.g., large transfers to new beneficiaries or rapid repeated transfers) that requires step-up authentication (e.g., biometric or multi-factor checks), imposes a short mandatory cooling-off period, and prompts customers to confirm that no one is instructing them to transfer funds (Associated Press, 2025; Bank of Thailand, 2024). Rapid-response pathways—clear evidence checklists, dedicated hotlines, and standardized forms—can reduce time-to-freeze and improve recovery chances, particularly in real-time payment environments (Akesson et al., 2023; UNODC, 2025).

**Platforms and app ecosystems: identity, ads, and recruitment detection**

Platforms play a major role in the exposure stage. High-risk investment advertisements should be restricted, and entities promoting financial products should be required to undergo stronger identity and credential verification. Recruitment detection can focus on mass outreach behavior, repeated scam-related keyword patterns, and abnormal complaint signals. App ecosystems can support users by issuing prominent warnings for sideloading and highlighting developer verification in a way that is easy for non-experts to interpret.

**Ethical and Victim-Support Considerations**

A victim-centred response is part of prevention because delayed reporting increases losses. Reporting pathways should be designed to reduce stigma and simplify action: what evidence to preserve (chat logs, transaction receipts, platform identifiers), where to report, and what steps banks can take. Victims may also need psychological support and debt-management services, because financial harm often triggers distress, family conflict, and secondary harms that can undermine recovery and cooperation with investigations (Cole, 2024; Drew & Webster, 2024). Integrating referral pathways (e.g., from AOC/bank hotlines to counselling and financial advice) can therefore improve both welfare outcomes and system effectiveness.

An additional ethical issue is the regional context of scam centres. UNODC (2025) emphasizes that scam operations can intersect with trafficking and coercion, complicating offender-victim boundaries. This does not reduce the harm inflicted on victims, but it suggests that policy responses should integrate law enforcement with human-security safeguards.

## Limitations

This study is limited by its qualitative design and purposive sampling strategy. The findings are intended for analytic generalization—explaining mechanisms and decision points—rather than statistical estimation of prevalence. Second, recall bias may influence retrospective narratives, particularly regarding the timing of suspicion and deposits. Third, the study could not access or verify active perpetrators within operating scam centres; instead, operational perspectives come from individuals who self-reported participation in scam operations, which may involve selective disclosure and may not capture the full range of coercion and organizational complexity described in regional reporting (INTERPOL, 2025; UNODC, 2025). Nevertheless, triangulation across three informant groups, along with convergence checks and negative case analysis, supports the robustness of the identified lifecycle and prevention levers.

## Future Research Directions

Future studies should extend this work through mixed-method designs. Large-scale surveys and administrative datasets can estimate prevalence and test predictors of escalation, complementing the process evidence offered here. Field experiments can evaluate the effectiveness of friction interventions (e.g., transfer delays, targeted warnings) on high-risk transactions while monitoring unintended effects on access and inclusion. Comparative cross-national research can examine how local credibility cues and platform ecologies shape scam scripts and victim responses.


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.

Qualitative research should also focus on under-studied populations, older adults, rural communities, migrant workers, and on the long-term aftermath, including employment consequences, family dynamics, and trust in digital finance.

A lifecycle-based prevention framework

To translate the lifecycle findings into implementable practice, we propose a four-layer prevention framework aligned with the stages in Figure 1. Layer 1 is **recognition**: scenario-based education that teaches people to identify diagnostic scripts (e.g., "guaranteed high returns," "install this app outside the official store," "pay fees to unlock withdrawal," "VIP upgrade," "today-only window"). Layer 2 is **containment**: platform governance that reduces recruitment reach through ad controls, identity verification, and rapid takedown of repeat recruitment accounts. Layer 3 is **transactional friction**: banking safeguards (step-up verification, cooling-off delays, risk-scored warnings) that interrupt repeated top-ups during escalation. Layer 4 is **rapid response**: simplified reporting, evidence preservation, and fast coordination to freeze funds and connect victims with support services.

This layered design anticipates displacement and adaptation. As UNODC (2025) notes, organized scam operations move quickly when a channel becomes costly. A defense-in-depth approach ensures that if exposure occurs, later layers can still reduce harm. The framework is also evaluation-ready. Recognition can be assessed through improvements in script recognition and verification behavior; containment through takedown speed and recurrence rates; transactional friction through reductions in repeated transfers after warnings; and rapid response through time-to-freeze and recovery success rates.

## Conclusion

This qualitative case study provides a triangulated, Thailand-specific model of cyber-enabled investment scams as a staged lifecycle involving credibility engineering, escalation pressure, and platform control. Victimization produces compounding financial and psychosocial harm, often amplified by shame and delayed reporting. Effective prevention requires layered interventions: scenario-based public education, platform governance to reduce recruitment, banking friction, and rapid freezing protocols to interrupt escalation, and cross-border enforcement and victim support to address industrialized scam infrastructures. Because the lifecycle contains distinct decision points, the recommended interventions can be operationalized and evaluated using measurable indicators such as repeated-transfer reduction, time-to-reporting, and recovery success. (European Banking Authority & European Central Bank, 2025; Australian Competition and Consumer Commission, 2024)

## Acknowledgements, Funding, and Declarations

Acknowledgements: The author gratefully acknowledges the financial support provided by the Faculty of Political Science and Law, Burapha University, Thailand, through the research project "Cyber Crime: A Case Study of Investment Scams," which made this study possible.

Funding: This article is based on the research project entitled "Cyber Crime: A Case Study of Investment Scams" and was financially supported by the Faculty of Political Science and Law, Burapha University, Thailand. The funding body had no role in the design of the study; the collection, analyses, or interpretation of the data; the writing of the manuscript; or the decision to publish the results.

Author Contributions: The author solely conceived, designed, and conducted the study, collected and analyzed the data, and was responsible for writing and approving the final version of the manuscript.

Data Availability Statement: The raw data supporting the conclusions of this article are not publicly available to protect the privacy and confidentiality of the participating individuals, in accordance with the ethical approval granted for this study and the informed consent agreements.

Informed Consent Statement: Written informed consent was obtained from all of the subjects involved in the study. The research protocol, including the consent procedure, was reviewed and approved by the Institutional Review Board of Burapha University, Thailand (Approval No. HU097/2566-C2). Participants were assured of confidentiality, anonymity, and their right to withdraw.

## References

Akesson, J., Gathergood, J., & Quispe-Torreblanca, E. (2023). Preventing Payments Fraud in the FinTech Era: New Evidence from a Behavioural Experiment (CeDEx Discussion Paper 2023-08). University of Nottingham. https://www.nottingham.ac.uk/cedex/documents/papers/cedex-discussion-paper-2023-08.pdf

Asia/Pacific Group on Money Laundering. (2024). APG Yearly Typologies Report 2024. https://apgml.org/sites/default/files/documents//2024_APG_Typologies_Report.pdf
Associated Press. (2025). UN researchers warn that Asian scam operations are spreading across the rest of the world. https://apnews.com/article/494b1832f330d6a9690b083411809f93
Associated Press. (2025, August 20). Thailand requires banks to cap most online transfers at $1,500 daily to thwart scammers. https://apnews.com/article/ed6b5454e737f3cc35c05d6bca62d81f
Australian Competition and Consumer Commission. (2024). Targeting scams: Report of the National Anti-Scam Centre on scams data and activity 2024. https://www.scamwatch.gov.au/system/files/targeting-scams-report-2024.pdf
Bank of Thailand. (2024). The BOT's Mission Against Financial Threats. Annual Report 2024. https://www.bot.or.th/en/research-and-publications/reports/annual-report/report-2024/box07.html
Bank of Thailand. (n.d.). PromptPay. https://www.bot.or.th/en/financial-innovation/digital-finance/digital-payment/promptpay.html
Childs, A. (2024). 'I guess that's the price of decentralisation…': Understanding scam victimisation experiences in an online cryptocurrency community. *Journal of Social and Personal Relationships*. https://doi.org/10.1177/02697580231215840
Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice, 19*, 91-150. https://doi.org/10.1086/449230
Cohen, L. E., & 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
Cole, R. (2024). A qualitative investigation of the emotional, physiological, financial, and legal consequences of online romance scams in the United States. *Forensic Science International: Mind and Law*. https://www.sciencedirect.com/science/article/pii/S2949791424000605
Drew, J. M., & Webster, J. (2024). The victimology of online fraud: A focus on romance fraud victim narratives. *Forensic Science International: Mind and Law*. https://www.sciencedirect.com/science/article/pii/S2949791424000058
European Banking Authority, & European Central Bank. (2025). EBA and ECB Report on Payment Fraud (2025). https://www.eba.europa.eu/sites/default/files/2025-12/1709846a-84d9-47cf-86a0-b155efb34d66/EBA%20and%20ECB%20Report%20on%20Payment%20Fraud.pdf
European Central Bank. (2024). Report from the ERPB Working Group on Fraud Prevention. https://www.ecb.europa.eu/paym/groups/pdf/erpb/202404_erpb_wg_fraud_report.pdf
European Payments Council. (2025). Payments Threats and Fraud Trends Report 2025. https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2025-12/EPC162-24%20v2.0%202025%20Payments%20Threats%20and%20Fraud%20Trends%20Report_0.pdf
Europol. (2025). EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025: The changing DNA of serious and organised crime. https://www.europol.europa.eu/publications-events/main-reports/eu-serious-and-organised-crime-threat-assessment-eu-socta-2025
Federal Trade Commission. (2024). Stopping scams and fraud before they happen: Using FTC data and research to protect consumers. https://www.ftc.gov/system/files/ftc_gov/pdf/prevention-messaging-committee-report.pdf
Global Anti-Scam Alliance, & Feedzai. (2024). Global State of Scams Report 2024. https://a.storyblok.com/f/134103/x/6317097d59/global-state-of-scams-report-2024.pdf
Global Initiative Against Transnational Organized Crime. (2024). Rogue replicants: How AI deepfakes are boosting fraud in the Asia-Pacific. https://globalinitiative.net/analysis/rogue-replicants/
Global Initiative Against Transnational Organized Crime. (2025). Compound crime: Cyber scam operations in Southeast Asia (Report). https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/
Han, J., & Button, M. (2025). An anatomy of pig butchering scams: Coercion, cultivation, and conversion. Deviant Behavior. https://openresearch.surrey.ac.uk/esploro/outputs/journalArticle/An-anatomy-of-pig-butchering-scams-Coercion-cultivation-and-conversion/99571455102346

INTERPOL. (2023). INTERPOL Annual Report 2023. https://www.interpol.int/content/download/23005/file/INTERPOL%20Annual%20Report%202023.pdf
INTERPOL. (2025). Crime Trend Update: Human trafficking-fueled scam centres. https://www.interpol.int/content/download/23175/file/INTERPOL%20Crime%20Trend%20Update%20-%20Human%20trafficking-fueled%20scam%20centres.pdf
Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263-291. https://doi.org/10.2307/1914185
Kraiwanit, T. (2025). Predictors of digital fraud: Evidence from Thailand. *Journal of Risk and Financial Management, 18*(12), 671. https://doi.org/10.3390/jrfm18120671
Lertsatitpirote, K., & Kanyajit, S. (2023). Causes and types of online fraud victimization in Thailand. International Journal of Criminal Justice Sciences, 18(2), 387–400. https://doi.org/10.5281/zenodo.4756325
Payment Systems Regulator. (2025). Using behavioural economics to understand and prevent authorised push payment (APP) fraud. https://www.psr.org.uk/media/efpdiwpk/using-behavioural-economics-to-understand-and-prevent-app-fraud.pdf
Public Relations Department, Thailand. (2024, November 18). DE's 1441 hotline successfully suspends 340K+ suspicious accounts and prevents THB19 billion in losses. https://thailand.prd.go.th/en/content/category/detail/id/2078/iid/340595
Reuters. (2025). Billion-dollar cyberscam industry spreading globally, UN says. https://www.reuters.com/world/china/cancer-billion-dollar-cyberscam-industry-spreading-globally-un-2025-04-21/
Reuters. (2026, February 2). Cambodian scam compound yields trove of fraud evidence, Thai military says. https://www.reuters.com/world/asia-pacific/cambodian-scam-compound-yields-trove-fraud-evidence-thai-military-says-2026-02-02/
Royal Decree on Measures for the Prevention and Suppression of Technological Crime B.E. 2566 (2023). (In Thai). https://www.senate.go.th/assets/portals/93/fileups/257/files/korpor/mix267_66.pdf
Staw, B. M. (1976). Knee-deep in the big muddy: A study of escalating commitment to a chosen course of action. *Organizational Behavior and Human Performance, 16*(1), 27-44. https://doi.org/10.1016/0030-5073(76)90005-2
Sun, J. (2025). Responsive policing for cyberfraud prevention. Police Practice and Research. https://www.tandfonline.com/doi/full/10.1080/10439463.2025.2548237
United Nations Office on Drugs and Crime (UNODC). (2025). *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*. https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf
Wang, J., Zhang, L., Xu, L., & Qian, X. (2024). The dynamic emotional experience of online fraud victims during the process of being defrauded: A text-based analysis. Journal of Criminal Justice, 94, 102231. https://doi.org/10.1016/j.jcrimjus.2024.102231
Xiao, J., Xiao, Q., & Shen, H. (2025). “It Felt Real”: Victim perspectives on platform design and longer-running scams. arXiv. https://arxiv.org/abs/2510.02680


**Citation:** Kulsawat, T., & Kortana, T. (2026). Cyber Crime: A Qualitative Case Study of Investment Scams in Thailand. International Journal of Development Administration Research, 9 (1), 33-50.