

Article

Authority Impersonation and Digital Victimization in a Transnational Cyber Fraud Network: Evidence from Vietnam

Thang Ngoc Dinh ¹, Huu Trong Ho ¹ and Hai Thanh Luong ^{2,*} 

¹ College of Social Science and Humanities, Vinh University, 182 Le Duan Street, Vinh 460000, Vietnam; thangdn@vinhuni.edu.vn (T.N.D.); huuht@vinhuni.edu.vn (H.T.H.)

² School of Criminology and Criminal Justice, Griffith University, 170 Kessels Road, Nathan, QLD 4111, Australia

* Correspondence: h.luong@griffith.edu.au

Abstract

This article examines authority impersonation as a structured mechanism of digital victimization through an in-depth qualitative case study of a Vietnamese transnational cyber fraud network. Drawing on a pseudonymized criminal judgment concerning the PVP network, the study reconstructs how offenders recruited Vietnamese workers, operated from Cambodia-based scam facilities, and targeted victims in Vietnam through a hierarchical D1-D2-D3 division of labour. The findings show that victimization was produced through a staged process of legitimation, criminal suspicion, simulated legal authority, and compliance-based extraction. Victims were not primarily deceived by technical hacking or promises of financial gain; rather, they were induced to comply through trust in state institutions, fear of criminal liability, secrecy instructions, and digitally mediated banking procedures. The case demonstrates how social engineering, organised cybercrime, and institutional impersonation converge to generate substantial financial and psychological harm. The article contributes to cybercrime and victimization scholarship by showing that authority-based fraud operates as a socio-technical process in which simulated legality transforms victim compliance into financial extraction. It also highlights the need for digital literacy programs that move beyond generic scam awareness toward procedural literacy, authority verification, and victim-centred support.

Keywords: authority impersonation; digital victimization; cyber fraud; crime script; simple job high salary; Vietnam



Academic Editor: James O. Finckenaue

Received: 27 July 2026

Revised: 7 September 2026

Accepted: 15 September 2026

Published: 17 September 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

The growth of digital communication has changed social, economic, and government interactions, while creating new criminal opportunities where cyber fraud is now among the most common and costly crimes, crossing borders and platforms ([UNODC 2024](#); [USIP 2024](#)). A troubling trend is authority-impersonation scams, in which offenders pose as police, courts, banks, or government agencies to trick victims into sharing information, transferring money, or granting access to digital accounts ([GITOC 2025](#); [UNODC 2025](#)). These are socio-technical crimes combining communication tools, personal data, psychological tricks, and institutional symbols to manipulate victims.

Increasing research on cybercrime shows that many online scams rely more on social engineering than on complex hacking techniques, in which perpetrators manipulate trust, urgency, fear, and information gaps to persuade victims to act against their own best

interests (Button and Cross 2017; Franceschini et al. 2025; Franceschini et al. 2026; Lazarus et al. 2026; Leukfeldt and Holt 2020). Authority-impersonation scams are particularly effective because they rarely target greed or financial temptation; instead, they leverage fears of legal consequences and trust in public institutions (Cheurprakobkit et al. 2026; Lazarus et al. 2025; Yu et al. 2023). Accordingly, victims often think they are assisting a legitimate investigation rather than engaging with criminals (Luong and Ngo 2024; Norris et al. 2019). This difference is crucial because it shifts the focus from deception alone to the social, psychological, and procedural processes that foster compliance (Asyali et al. 2026; Robert et al. 2026).

Existing research also highlights a notable imbalance in the study of fraud and scams within cybercrime (Button et al. 2026). Much of the literature focuses on offenders, technologies, or criminal markets, while comparatively less attention is given to how victims are manipulated into complying with fraudulent demands, which increasingly questions victim-blaming explanations (Han and Button 2026; Whittaker et al. 2024). Victims are often portrayed as gullible, careless, or digitally inept; however, empirical research shows that victimization usually results from sophisticated offender tactics and situational pressures rather than personal shortcomings (Button and Cross 2017; Norris et al. 2019). Carter (2023) demonstrates how fraudsters use interaction routines to draw victims into an alternate reality where compliance seems reasonable. Similarly, Liu et al. (2024) reveal that institutional impersonation fraud depends on offenders presenting themselves as authoritative figures while positioning victims as individuals in need of official intervention. These studies are important because they show that authority-driven fraud works by changing victims' perceptions of risk, obligation, and trust in real time. Digital victimization is not merely the result of deception; it often stems from a series of interactions that gradually shape how victims perceive risk, authority, and obligation (Asyali et al. 2026; Robert et al. 2026). Understanding these processes is especially vital for authority-impersonation scams because victims often believe they are responding to genuine requests from law enforcement or other government agencies. As a result, victims may voluntarily share personal details, reveal banking credentials, transfer funds, or liquidate assets, thinking they are part of an official investigation (Jansen and Leukfeldt 2016; Norris et al. 2019).

Research on organized cybercrime highlights the importance of role differentiation, social connections, and criminal specialization. Crime script analysis, introduced by Cornish (1994), provides a framework to understand how crimes evolve through successive stages. Hutchings and Holt (2015) demonstrate the effectiveness of crime scripting for analyzing cybercrime markets in which various actors fulfill complementary roles. Similarly, studies on organized financial cybercrime show that cybercriminal networks are structured entities with technical, social, and organizational capabilities (Holt and Lee 2022; Leclerc and Morgenthaler 2023; Lee 2021; Leukfeldt et al. 2017; Leukfeldt and Yar 2016). These ideas are particularly relevant to current Southeast Asian scam operations, which often involve call centers, scripted interactions, digital platforms, and specialized labor roles (GITOC 2025; UNODC 2025). The latest UNODC report found that in Southeast Asia, increased attention has been given to transnational scam operations based in Cambodia, Myanmar, Laos, and nearby jurisdictions (UNODC 2026). These operations typically use digital communication, multilingual staff, online banking exploitation, and organized labor divisions to target victims on a large scale. Despite growing concern, there is limited empirical research on how authority impersonation operates within these organized cyber-fraud networks in Southeast Asian countries. Specifically, there is a scarcity of case-based evidence explaining how organizational structures, scripted offender roles, and victim vulnerability come together to cause digital victimization. This gap is critical because authority-impersonation scams do more than make false claims; they often create a simulated legal environment in which

victims believe that cooperation is essential to avoid arrest, prosecution, asset seizure, or reputational damage.

This article explores a major Vietnamese cyber fraud network through an in-depth qualitative case study. To protect privacy and reduce re-identification risks, all individuals mentioned in the judgment are anonymized with pseudonymous identifiers. The case centers on a transnational scam operation based in Sihanoukville, Cambodia, which recruited Vietnamese nationals into a structured call-center system to systematically target victims in Vietnam using authority-impersonation schemes. Instead of viewing authority impersonation as merely a deceptive trick, this article argues that it serves as a structured method of digital victimization, warranting further research to compare it with previous studies such as ‘simple job, high salary’ (Luong 2025). By simulating legal authority, procedural legitimacy, and criminal investigation, offenders create a coercive environment where victims see compliance as rational and necessary. The case illustrates how trust in public institutions can be manipulated into a criminal resource, enabling large-scale cyber fraud without physical force. Overall, this study contributes to emerging research on cybercrime and digital victimization by demonstrating how authority-based social engineering operates in a transnational cybercrime context.

Drawing on crime script analysis, organizational analysis, and victimization pathway analysis, the study seeks to answer the following research questions (RQ):

RQ1: How was the Vietnamese cyber fraud network organized, and what modus operandi enabled authority-impersonation fraud?

RQ2: How did authority impersonation function as a mechanism of digital victimization within Vietnam’s fraud process?

RQ3: What Vietnamese victim vulnerabilities were exploited in the cyber fraud network?

2. Research Methods

This study uses a qualitative case study (Yin 2018) to explore how impersonation of authority fosters digital victimization within a transnational cyber-fraud network. It helps investigate hidden organizational structures, transnational actors, and evolving cybercrime techniques, offering rare insights into offender behavior, victimization, and operational dynamics.

2.1. Research Design and Case Selection

This study follows Stake (1995)’s definition of an instrumental case study, focusing on a specific case not solely for its uniqueness but to gain a deeper understanding of a significant social issue. The goal is not just to report on a fraud case in Vietnam, but to analyze how impersonating authority serves as a tool for digital victimization within organized cyber-fraud networks. We examine a single case from Judgment No. 181/2025/HS-ST of the People’s Court of Nghệ An Province, Vietnam (the PVP cyber-fraud network). To ensure privacy and minimize re-identification risks, all individuals are referred to with pseudonymous identifiers, except that the names of unidentified foreign actors in the judgment are indicated with *italicized* pseudonyms (see more details in Appendix A). The choice of a single case is methodologically justified for several reasons, including the need to avoid potential misunderstandings with this method (Flyvbjerg 2006). Firstly, it is a critical case that offers detailed evidence on offender recruitment, organizational hierarchy, criminal scripting, victim-offender interactions, financial schemes, and judicial outcomes. The judgment details over thirty participants within a structured cyber fraud network based in Cambodia, targeting victims across Vietnam. Secondly, the case exemplifies a common form of authority impersonation fraud in Southeast Asian scam operations. It features elements found in international reports, such as cross-border activities, special-

ized divisions, VoIP communications, messaging apps, fake law-enforcement identities, exploitation of digital banking, and substantial financial losses. Thirdly, it offers valuable insights into the victimization process. Unlike many cybercrime studies that rely solely on outcome data or victim reports, the court judgment reconstructs multiple stages of the fraud, highlighting how authority impersonation, fear, procedural legitimacy, and compliance facilitate financial victimization. Finally, all co-authors are Vietnamese with a strong background in criminology and criminal justice, and we are familiar with the linguistic, cultural, and legal issues involved in reading, coding, recoding, and analyzing this case. The value of single-case research has long been recognized in qualitative inquiry. Yin (2018) argues that a single case may be sufficient when it is critical, revelatory, extreme, or particularly informative. Similarly, Flyvbjerg (2006) notes that carefully selected cases can generate substantial theoretical and analytical contributions despite the absence of large samples. The present case meets these criteria because it provides rare access to the internal organization and operational practices of a transnational cyber fraud network.

2.2. Data Collection and Analysis

The main source of data is the publicly available judgment issued by the People's Court of Nghệ An Province upon the authors' request. The judgment contains detailed information about offender recruitment, organizational structure, command relationships, operational procedures, digital communication methods, victim testimonies, financial losses, and judicial findings. The court record documents a cyber fraud network that operated from February 2023 to January 2024 and used facilities in Sihanoukville, Cambodia. The network used a structured D1-D2-D3 hierarchy (see Table 1) and targeted Vietnamese victims through authority-impersonation schemes involving false allegations of banking debt, money laundering, and drug trafficking. Documented losses to victims exceeded VND 14 billion. Judicial records are a valuable source of qualitative data because they provide various accounts assessed through adversarial legal procedures. Although legal documents do not capture every aspect of offender behavior, they provide details on criminal actions, organizational arrangements, and victims' experiences.

Table 1. Organizational Architecture of the PVP Cyber Fraud Network.

Role	Function	Primary Objective
(AM, BM)	Foreign organizers who support the syndicates in infrastructure, finance, and strategic oversight	Maintain scam operations
PVP	Boss and main offender; Recruitment and network management	Operational coordination
D1	Initial victim contact	Lead generation
D2	Authority impersonation	Psychological manipulation
D3	Asset extraction	Financial victimization
(AT, AH)	Technical Operators: Banking access and account takeover	Fund transfer and laundering

Notes: D1/D2/D3 are the Vietnamese offenders/accomplices with PVP, who are the central offenders in this case; meanwhile, all *italicized* letters (AM, BM, AT, and/or AH) are the foreign organizers who are at large and not yet prosecuted under the Vietnamese criminal code. All of them are pseudonymous identifiers for anonymous individuals.

Based on the crime script analysis (Cornish 1994), three analytical aims were targeted. First, it views offending as decision sequences across stages, aiding in the reconstruction of criminal processes and intervention points, specifically by mapping authority-impersonation fraud from recruitment to financial extraction. Second, analyzing the fraud network's structure focuses on division of labor, role differentiation, hierarchy, and coordi-

nation, assessing how organization affects success. Third, examining victim experiences and compliance mechanisms explores how offenders guide victims through identity verification, criminal accusations, authority confirmation, asset disclosure, and financial extraction, revealing how impersonation fosters compliance and victimization. These points have been derived by combining (1) facts accepted by the court, (2) testimony reported in the judgment, (3) allegations or offender accounts, and (4) interpretations subsequently made by our co-authors.

3. Findings

3.1. *The Vietnamese Cyber Fraud Network: Organizational Structure and Modus Operandi (RQ1)*

Findings reveal the PVP network was a structured transnational enterprise based in Sihanoukville, Cambodia, involving Vietnamese recruits, foreign organizers, technicians, and translators, organized around D1, D2, and D3. It operated through recruitment from Vietnam with social trust and economic incentives, and targeted victims via authority-impersonation scripts related to police, courts, banking debt, drug trafficking, money laundering, fake warrants, and digital banking. This shows it functioned as both a labor-recruitment network and a cyber fraud system.

3.1.1. Recruitment, Mobility, and Structure

The PVP network was formed through collaboration between PVP and an unidentified foreign organizer referred to here as AM. According to the judgment, AM presented himself as the operator of companies engaged in fraud targeting Vietnamese citizens by impersonating state agencies, including the police, prosecutors, and courts. PVP agreed to cooperate with AM, with AM responsible for securing premises, equipment, internet systems, phones, computers, and technical infrastructure in Cambodia, while PVP was responsible for recruiting and managing Vietnamese workers.

Recruitment in Nghê An Province primarily relied on kinship, friendship, and local networks. PVP contacted relatives, friends, and trusted contacts, encouraging them to invite others in Cambodia. Early recruits were close contacts and relatives, and recruitment later expanded through word of mouth in districts like Yên Thành, Thanh Chương, and Con Cuông. The message promised “simple job, high salary,” with the company covering costs such as transportation, travel, and food, thereby reducing barriers for vulnerable individuals. Recruits were told to obtain passports and exit Vietnam legally via Tân Sơn Nhất Airport or the Mộc Bài border crossing. This relied on social trust, local ties, economic hopes, and known contacts, not force or abduction, but exploitation of relationships and economic aspirations. Early operations depended on trust and deception. Once in Cambodia, the pattern changed. PVP and recruits went to Phnom Penh and then to Sihanoukville, operating from the 17th floor of a high-rise. They lived, ate, and worked together in a confined environment, with movement managed and outside access restricted. New recruits’ passports and phones were collected, with passports transferred to foreign managers for admin and phones kept to prevent leaks. Phones were returned only occasionally, allowing contact with family. This shows that, despite initial claims of voluntary work, the environment involved significant control over mobility, communication, and privacy.

The judgment details the network’s organized structure, describing a systematic, multi-department system with foreign and Vietnamese staff in roles such as organizers, managers, and technical personnel. Divided into D1, D2, and D3 groups, each had a specific function in a scripted call-center system, where each stage depended on the others. D1 initiated contact, D2 built authority, and D3 managed high-value victims and sensitive data. This architecture is key to understanding the modus operandi of the operation. In particular, D1 personnel served as frontline operators, contacting victims via Voice over Internet Protocol

(VoIP) using personal data such as names, addresses, identification numbers, and phone numbers, making 100–300 calls daily. D2 personnel, posing as investigators from cities like Hanoi, used advanced tactics such as video calls, fake documents, and staged police interactions. D3 personnel at the highest level impersonated prosecutors and police officers to facilitate asset disclosure, obtain bank details, and direct fund transfers. These roles were interdependent, requiring coordination for the fraud process, with no single operator completing it alone.

3.1.2. A Hierarchical Division of Criminal Labor with Specific Modus Operandi

Unlike conventional fraud schemes carried out by individual offenders, the PVP network exhibited an extensive division of labor. The judgment identifies three operational tiers labeled D1, D2, and D3, each responsible for distinct stages of the fraud process.

D1 was the main operational group, serving as the primary contact layer in the network. D1 workers sat in a large room with workstations separated by partitions. Each worker received an iPhone 6s with the Bria Mobile VoIP Softphone app, along with a headset, charger, pen, paper, and a list of Vietnamese citizens, including details such as name, date of birth (DOB), address, phone number, and ID. They aimed to call 100–300 people daily. The script focused on establishing legitimacy, pretending to be police to verify information or update records. After the victims confirmed their details, D1 operators claimed a debt of VND 58.986 million, threatening asset freezes or legal action. If victims denied responsibility, D1 suggested that information might be leaked or misused and offered to connect them with higher-level police authorities. The role was strategic: D1 operators rarely took money but aimed to verify data, create a believable issue, and pass victims to the next stage. Records show D1 used the “##” keypad command to transfer victims to D2 once they agreed to report or clarify with higher authorities. D1 also noted victim details on paper to hand to D2 for further interaction.

D2 built authority with experienced, fluent personnel who used formal tones and impersonated police, especially from Hanoi, via Zalo calls (the most common free app in Vietnam), video calls, and staged procedures, creating a fictional official investigation. They escalated fraud by linking victims’ info to criminal activities like drug trafficking and money laundering, sometimes using fake communication devices or images of arrests, turning an administrative issue into a criminal investigation. This changed victims’ perceptions from banking problems to police investigations involving serious crimes, and they were instructed to stay secret and isolated.

D3 formed the final extraction layer, consisting of highly experienced personnel promoted from D2 who impersonated officials to handle larger assets. They converted fear into asset disclosure and bank credential capture using two methods: instructing victims to transfer money into controlled bank accounts and collecting banking credentials and OTPs to transfer funds. Technical operators, sometimes called PC operators, then accessed accounts, transferred money to Vietnamese accounts, and coordinated with foreign management via Telegram. The network combined social engineering with digital financial exploitation, relying on banking systems, communication platforms, VoIP, and coordinated account takeover, rather than advanced hacking.

Figure 1 illustrates this sequence, showing how each stage contributed to the fraud process. Recruitment supplied labor (1); mobilization placed workers in Cambodia (2); training standardized scripts (3); D1 made contact (4); D2 built police impersonation’s authority and fear (5); D3 stole banking info and assets (6); technical operators executed account takeovers and transfers (7); and they caused physical and psychological losses (8). The network operated via routine training, supervision, and performance control. Workers received scripts and studied them before work. PVP then assigned workers to D1, D2, or

D3 based on ability, skill, experience, and trustworthiness. This shows active assessment and matching of workers. The schedule resembled a disciplined call center, with work Monday to Friday, 7:30 a.m. to 4:00 p.m., with a short lunch. Saturdays, work continued into late morning; Sundays were rest days or for script learning. D2 and D3 staff worked beyond hours when manipulating victims.

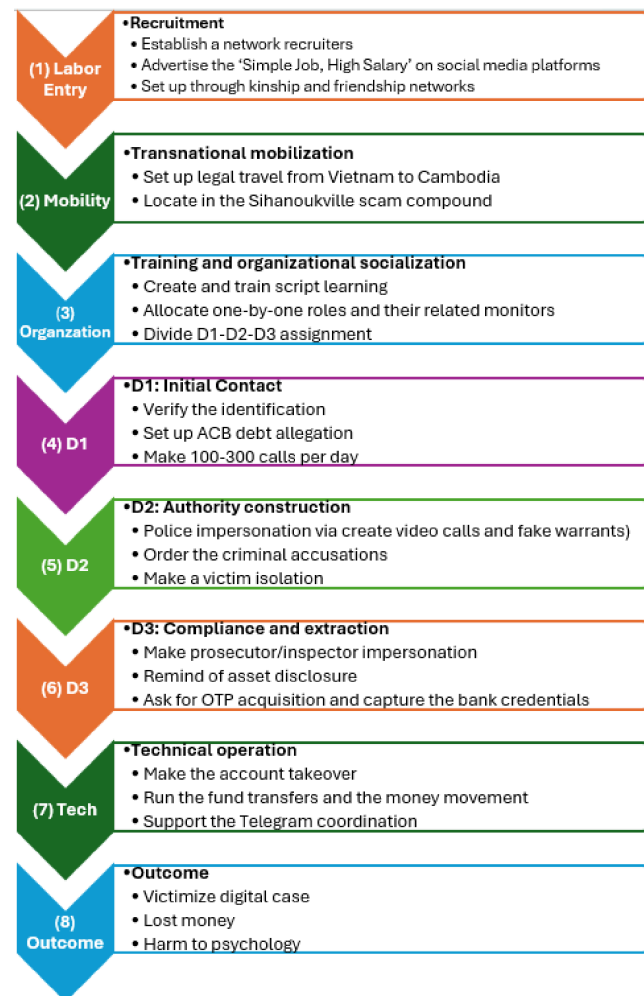


Figure 1. Crime Script of the PVP Cyber Fraud Network.

Daily meetings reinforced discipline and fraud performance, with collective gatherings at 6:00 p.m. on workdays to report successful cases, review errors, and share experiences. Workers who erred listened to call recordings, rewrote scripts, or copied scams until late. This built institutionalized learning and quality control, turning individual experience into shared knowledge. Payment structures further incentivized performance: D1 workers earned about USD 600 per month, plus a USD 200 attendance bonus and a 4% commission. D2 workers received USD 600 quarterly and a 5% commission, while D3 workers had no fixed salary but a 4% commission on successful cases. This system tied income to victim extraction, encouraging maximization of harm. Wage retention during holidays helped control mobility; employees could return to Vietnam, but 50% of that month's salary was retained until their return, integrating financial incentives with control to ensure labor continuity.

These findings reveal that the PVP network functioned like a formal workplace—with recruitment, roles, training, monitoring, wages, bonuses, penalties, and supervision—which was central to its large-scale authority-impersonation fraud. The case supports viewing this fraud as organized cybercrime relying on offline recruitment, transnational mobility, call-center discipline, digital platforms, scripted authority, and banking exploitation. This

organizational model underpins the next section on how authority impersonation functions as digital victimization.

3.2. *The Fraud Process of Authority Impersonation (RQ2)*

The PVP network used staged authority impersonation rather than technological intrusion to produce digital victimization. Aligning with and building on CSA's Cornish (1994), victims shifted from routine contact to fear-based compliance and financial loss through four organized stages: legitimizing contact, creating suspicion, mimicking legal authority, and extracting money via asset disclosure, OTP, and account takeover.

3.2.1. Stage 1: Legitimizing Initial Contact

The first victimization stage involved turning an unexpected phone call into what seemed like legitimate contact from a state institution. D1 operators used VoIP systems and victim lists containing personal details such as names, birthdays, addresses, phone numbers, and citizen IDs to verify information with official credibility. They often impersonated police, administrative, or records officers, framing calls as routine identity checks or administrative tasks. This pretext lowered victims' suspicion before introducing more serious allegations.

LNL's case illustrates the initial process of legitimization. A D1 operator, claiming to be a police officer, called LNL about a detected ACB credit card debt. When LNL denied responsibility, the caller suggested that personal information might have been leaked or misused and offered to connect LNL to police in Hanoi for clarification. This was strategic, as it redefined the offender as a protector rather than a threat. The operator did not demand money at first, but created a problem, invited denial, and offered access to higher authority to help resolve it.

A similar pattern emerged in the LTO case. LTO received a call from a D1 operator claiming ties to police records and court summons procedures. After confirming personal details and denying the ACB debt, the operator suggested possible identity theft and offered to involve police in Hanoi. The DVC and TTTH cases followed a similar sequence, starting with identity verification, appearing to have official knowledge of personal details, and involving an administrative issue related to ACB debt or identity records before escalating to criminal accusations.

These examples demonstrate that initial contact was deliberate and scripted. It was designed to build trust in authority before instilling fear. Accurate personal details served as proof, making the call seem real and the later claims more believable.

3.2.2. Stage 2: Manufacturing Criminal Suspicion

After establishing initial legitimacy, D1 operators handed victims over to D2 operators, who then shifted the interaction from a routine administrative matter to a criminal suspicion. This shift was crucial in the victimization process because it changed the victim's perceived role from a citizen seeking help to a suspect trying to demonstrate innocence.

The recurring mention of an alleged ACB debt of about VND 58.986 million served as a key narrative device. This amount appeared in many victims' stories and served more as a standard script element than as a specific case detail. The debt claim had multiple roles: it presented a tangible financial issue for victims to acknowledge or deny; denial, in turn, allowed offenders to imply identity theft or misuse of personal data; and claims of identity misuse opened the door to more serious crimes, such as money laundering, drug trafficking, illegal bank accounts, and financial fraud.

In the LNL case, after the ACB debt allegation was denied, D2 claimed that LNL's personal information was linked to drug trafficking and money laundering. The offender staged communication with a fictitious "central command" and claimed there was an arrest

warrant. In the DVC case, the same pattern occurred: DVC was told about an alleged ACB debt, then informed that personal information was connected to drug trafficking and money laundering, and that police had enough grounds to investigate in Hanoi. The TTTH case shows a more advanced version of this escalation. TTTH was told a TTTH account was linked to a VND 6 billion debt, related to drug trafficking and money laundering. Offenders claimed that suspected individuals implicated TTTH or family members in unlawful financial activity. The LTO case followed this pattern too: LTO was first accused of an ACB-related debt, then told police needed to investigate and verify finances. Though the financial loss was less, the basic script was similar.

This stage shows how the PVP network created criminal suspicion by gradually escalating the situation. Victims were not asked to transfer money right away. Instead, they were gradually drawn into a false legal narrative in which their assets, identity documents, and bank accounts were portrayed as potential evidence of a crime.

3.2.3. Stage 3: Simulating Legal Authority

The third stage involved reinforcing criminal suspicion through the simulation of legal authority, a key feature of the PVP network's victimization. Offenders did not just claim to be police; they reproduced signs of legitimacy, including ranks, badges, department names, official addresses, video calls, uniforms, Zalo accounts, warrants, and internal communications. D2 operators often used Zalo accounts with police-style names to communicate via voice, text, and video. Some video calls showed police-style clothing, workspaces, or pre-made images to appear official. In the LNL case, D2 used Zalo and video calls to reinforce police authority by showing an image of a person in police uniform, convincing LNL that the call was real. D2 also used fake walkie-talkie communication with a 'central command' to confirm criminal links. The case also shows the switch from D2 to D3, where PVP, acting as a police officer, took over, using Zalo accounts with official-sounding names to suggest higher authority. In the LTO case, D2 provided police rank, ID, department, and address, using Zalo and visual cues to make the impersonation more convincing.

In the TTTH case, the authority simulation was layered. TTTH was moved through multiple officials, including police or senior investigators, creating the impression of escalation within a formal hierarchy. Secrecy instructions also simulated legal authority, telling victims not to inform family or others, as disclosure could harm the investigation or lead to arrest. The instruction to stay isolated served two purposes: maintaining the illusion of an official legal process and preventing access to informal protective networks. While family or acquaintances might challenge this, secrecy is necessary to limit such challenges.

This stage shows that the PVP network's impersonation of authority was more than just verbal deception; it was an institutional performance. Offenders created a procedural environment with ranks, records, warrants, evidence, investigative commands, and hierarchy, transforming victim fear into procedural obedience.

3.2.4. Stage 4: Asset Disclosure and Financial Extraction

The final stage involved converting compliance into financial extraction. Once victims accepted the investigation's legitimacy and believed their assets needed verification, D3 operators directed them to disclose financial information, transfer money, open accounts, register for online banking, provide login details, or reveal a one-time password (OTP).

The judgment identifies two major extraction methods. The first involved direct transfer of money to bank accounts controlled by the fraud network under the pretext of asset verification. Victims were told that the money would be returned after authorities confirmed that the funds were not linked to criminal activity. The second method involved account takeover. Victims were instructed to provide online banking credentials, OTP

codes, or new banking information. D3 operators then relayed these details via Telegram or internal channels to technical operators, who accessed accounts and transferred funds to multiple recipient accounts. The LNL case illustrates the second pathway in detail. Under D3 direction, LNL was instructed to purchase a new mobile phone, acquire a new SIM card, download banking applications, and modify online banking access. PVP observed or obtained the login credentials and transferred the information to technical personnel, who took control of the account and moved funds through multiple accounts. LNL lost approximately VND 8.74 billion.

The evidence shows authority impersonation as a structured form of digital victimization, where victims were embedded in a fake legal process that made cooperation seem necessary and legitimate. The PVP network's process involved organizational and psychological manipulation: D1 established legitimacy, D2 created suspicion and fear, D3 converted fear into disclosure, and technical operators executed account takeovers and fund transfers. This four-stage process moved victims from legitimation to compliance-based extraction, highlighting that victimization relied more on social, institutional manipulation than advanced hacking. The network exploited digital platforms such as VoIP, Zalo, online banking, OTP, and Telegram, turning trust in institutions into financial harm when victims believed fraudulent instructions were legitimate legal obligations.

3.3. Victim Vulnerabilities and Digital Harms (RQ3)

The findings show victimization in the PVP case was not mainly due to hacking or greed. Instead, offenders exploited trust in authority, fear of criminal liability, and their elder-age vulnerability to complex instructions, triggered by scripted interactions turning citizens into victims.

3.3.1. Trust in Institutional Authority

The PVP network exploited victims' trust in state institutions, with offenders repeatedly impersonating police, courts, or authorities. This was a core part of their tactic, using a D1-D2-D3 hierarchy: D1 as local police, D2 as investigative officers, and D3 as higher-ranking figures like prosecutors or inspectors.

The judgment shows victims were not deceived by isolated false statements but were manipulated into a staged performance of state authority. Offenders used accurate personal data, official-sounding ranks, video calls, fake uniforms, fabricated warrants, police-style Zalo accounts, and references to investigative procedures, creating a facade of a legitimate bureaucratic process. The case of LNL exemplifies this: the initial caller, claiming to be a police officer, told LNL about a credit card debt linked to ACB. When LNL denied responsibility, the caller suggested misuse of personal information and offered a police connection in Hanoi, reframing the offender as a helper. Transferred to D2, the call used Zalo, video imagery, and fictitious "central command" to fool LNL into believing they were interacting with real police.

The authority-building strategy in the LTO case involved a caller asserting police ties, then transferring the call to a second individual who provided a police rank and additional details to bolster credibility. Offenders used visual cues, such as police uniforms or warrants, often via Zalo video calls, to deceive victims. In the LNL case, an image depicting a person in police attire reinforced the illusion, whereas in TTTH, offenders escalated police ranks to emulate a layered investigative process. This finding illustrates that authority impersonation functioned as a form of "institutional social engineering." The offenders did not merely solicit victims' trust on a personal level; rather, they sought to induce trust in the institutional symbols they mimicked. In this context, victim vulnerability was rooted not in ignorance or recklessness but in socially embedded trust in police, courts,

and official procedures. The PVP network exploited this trust by transforming the perceived legitimacy of state authorities into a mechanism for digital victimization.

3.3.2. Fear of Criminal Liability

A second vulnerability exploited in the case was the fear of criminal liability. Once offenders established apparent institutional legitimacy, they escalated the interaction from administrative verification to serious criminal accusations. Victims were not just told they owed money or had made a mistake; they were told they were involved in crimes such as money laundering, drug trafficking, illegal banking activity, or fraudulent account use.

The ACB debt of approximately VND 58.986 million served as the basis for more serious accusations. Perpetrators exploited victims' denial of the debt, framing it as identity theft and linking it to broader criminal activities, particularly in cases of LNL, LTO, DVC, and TTTH. The LNL case shows how fear can lead to escalation: after denying responsibility, LNL was told that their information was connected to drug trafficking and money laundering, with staged communications and a fake arrest warrant, turning a banking dispute into a criminal investigation. DVC faced a similar tactic. After confirming personal details, DVC was informed about an alleged ACB debt and then accused of involvement in drug trafficking and money laundering. The attacker claimed DVC could be brought to Hanoi for investigation and advised DVC to stay silent, act alone, withdraw savings, and transfer funds for verification. DVC ultimately lost VND 443 million. In TTTH's case, the perpetrators intensified their accusations, claiming TTTH was linked to a bank account with a VND 6 billion debt and connected to drug trafficking and money laundering. TTTH was instructed to disclose bank accounts and assets so that police could verify whether they were linked to criminal activity. Ultimately, TTTH opened a new bank account, shared login and OTP details, and lost approximately VND 2.179 billion.

Fear was reinforced through instructions demanding secrecy and isolation. Victims were told not to inform family, friends, or others, as disclosure could hinder the investigation or cause arrest. In the LNL case, after funds were taken, the offender instructed LNL not to reveal the matter and warned that disclosure could lead to detention. In the DVC case, the victim was told to go alone, maintain contact with the offender, and transfer money secretly. This secrecy removed potential protective interventions, such as family, bank staff, or community members might question the victims if consulted. By isolating victims, offenders limited independent verification and increased dependence on fraudulent authority.

The judgment shows that fear of criminal liability was an operational tool, converting victims' desire to avoid arrest, shame, and damage into compliance. Victims acted not for personal gain but to avoid legal harm. This distinguishes authority-impersonation fraud from opportunity fraud, in which fear, obligation, and legal necessity drive victimization.

3.3.3. Financial Harm and Psychological Entrapment for Older Adults

The third major finding relates to victim profile, financial harm, and psychological entrapment. The judgment shows victims were older adults who were targeted by scammers to defraud them of their savings or assets.

The financial losses were significant, totaling over VND 14.171 billion across five cases. LNL lost about VND 8.74 billion after being guided to buy a new phone, register a SIM, and download banking apps, which allowed offenders to steal login details and transfer funds. TTTH lost around VND 2.179 billion by opening a new account, consolidating savings, and sharing login and OTP info, enabling attackers to seize control. DVC transferred VND 400 million and was pressured to send more until family intervention halted further losses. LTO, involved in criminal activity and pressured via police impersonation, transferred about VND 87 million. These cases show digital victimization involved prolonged

psychological pressure, fear, and repeated instructions, with victims often linked to criminal accusations like money laundering or arrest warrants. Offenders exploited victims' fears to prolong contact, steal assets, and direct financial transactions. Accordingly, victims were drawn into a fake legal process, disclosing assets, reorganizing finances, modifying bank accounts, sharing digital credentials, and obeying secrecy. This shows victim vulnerability was situational and interactional, not inherent. Offenders made compliance seem legally necessary, secrecy required, and financial disclosure rational. The PVP case reveals how authority-impersonation fraud harms through trust, fear, and digital financial extraction.

4. Discussions

4.1. Organized Cyber Fraud as a Scripted and Specialized Criminal Enterprise

The initial finding indicates that the PVP network was a structured, cross-border cyber fraud organization rather than a loose or opportunistic group of offenders. This strongly supports crime script theory, which views offending as a series of planned, ongoing actions, covering preparation, execution, and aftermath, rather than a single criminal event. [Cornish \(1994\)](#)'s crime script framework is especially useful for analyzing the PVP case because the judgment outlines a clear sequence: recruitment, mobilization to Cambodia, script-based training, role assignment, D1 victim contact, D2 authority building, D3 extraction, technical account takeover, and fund transfer.

The PVP case also reflects [Hutchings and Holt's \(2015\)](#) crime script analysis of online stolen-data markets. Their research indicates that organized cybercrime is often supported by complementary services, clear role divisions, and staged processes connecting data acquisition, monetization, and laundering. In this case, D1 operators handled lead generation and initial contact; D2 operators addressed administrative issues that raised criminal suspicions; D3 operators extracted assets and banking credentials; and technical operators managed account takeovers and money transfers via digital banking and Telegram coordination. This division of tasks shows that the network's success relied more on organizational specialization than on individual callers' persuasiveness.

This finding also enhances the broader study of organized cybercrime. [Leukfeldt et al. \(2017\)](#) argue that financial cybercrime exists along a continuum of organization, from loosely connected offenders to more structured criminal networks with defined roles and social links. The PVP case supports this view but also introduces a Southeast Asian scam-compound aspect. The judgment documents detail recruitment through kinship and friendship networks in Nghê An; legal travel to Cambodia; accommodation and work in Sihanoukville; script learning; daily performance meetings; role assignment; salary and commission structures; and continuity across different locations and organizers.

This case thus builds upon previous research by illustrating how social connections, physical moves, and digital infrastructure function together as a single operational system. The recruitment process was rooted in social networks, but the fraud activities were facilitated through technology. The network depended on VoIP calls, Zalo accounts, online banking access, OTP capture, and Telegram communication, but its main strength was in coordinating human labor. This supports the idea that many modern cyber frauds are not just technical crimes but also involve social and technical elements in which people, scripts, platforms, and financial systems interact.

In this context, the PVP case enhances the existing literature on organized cybercrime by illustrating how organizational structure directly affects victimization outcomes. The D1-D2-D3 system was not just about dividing tasks for efficiency; it also reflected institutional hierarchy for victims. Each transfer of responsibility contributed to the illusion of progression within a legitimate legal process. This indicates that the organizational frame-

work itself became part of the deception. The criminal group did not just mimic police authority; it also arranged itself to make impersonation of authority more convincing.

4.2. Authority Impersonation as a Mechanism of Digital Victimization

The second finding indicates that authority impersonation was a structured form of digital victimization rather than a straightforward fraud tactic. This aligns with [Carter \(2023\)](#)'s analysis of fraudster-victim interactions, showing that fraudsters deploy language and social routines to gradually secure victims' compliance while diminishing their ability to recognize danger. [Carter \(2023\)](#) describes this as fraudsters creating an "alternate reality" in which victims see their role as reasonable, safe, or essential. The PVP case supports this view but also introduces an institutional aspect: this alternate reality was not only interpersonal but also bureaucratic and legal.

In the PVP case, victims were drawn into a staged process that started with establishing administrative legitimacy and ended with financial extraction. Offenders first verified personal information, then introduced the repeated ACB debt claim of about VND 58.986 million, and then escalated the situation to involve alleged money laundering, drug trafficking, arrest warrants, and asset verification. This sequence shows that victimization happened through a gradual reinterpretation of the situation. Victims were not immediately asked to transfer money; they were first led to believe they were participating in a legitimate legal process.

The findings align with [Liu et al. \(2024\)](#)'s research on institutional impersonation fraud, which shows scammers build identities using "self-styling" and "other-styling", posing as professionals and portraying targets as problematic or in need of help. The PVP case illustrates this pattern: D1 operators labeled victims as potentially misused identities; D2 called victims suspects; D3 convinced victims to cooperate to prove innocence. This is seen in cases like LNL, TTTH, DVC, and LTO, where victims lost millions through fake police accounts, warrants, and coercion, with the amounts being VND 8.74 billion, VND 2.179 billion, VND 443 million, and VND 87 million, respectively.

The PVP case also aligns with [Norris et al. \(2019\)](#)'s systematic review of internet fraud victimization, which concludes that susceptibility is not due to simple individual weakness but results from the interplay of message, experiential, and dispositional or situational factors. In this case, message factors stood out prominently: official pretexts, criminal accusations, urgent instructions, fake documents, police-style identities, and secrecy demand. These messages were particularly effective because they merged credibility, fear, urgency, and procedural obligations.

This discovery also calls into question approaches to cybercrime that overemphasize technical expertise. The PVP network used tools such as VoIP, Zalo, online banking, OTP codes, and Telegram, but its key strength was not in high-level hacking. Instead, the offenders tricked victims into willingly giving digital access. This supports [Jansen and Leukfeldt's \(2016\)](#) qualitative research on online banking crimes, which showed that many victims were aware of scams or had security measures in place but still shared credentials or codes during specific interactions. The PVP case shows that simply being aware is not enough when victims feel legally pressured.

4.3. Victim Vulnerability, Digital Harm, and Digital Literacy Implications

The third key point relates to victim vulnerability, digital harm, and the consequences for victim-centered digital literacy programs. The PVP case notably supports victimological research that dismisses simple victim-blaming narratives. [Button and Cross \(2017\)](#) highlight that cyber fraud victims are often unfairly depicted as naive, greedy, or careless, while little emphasis is placed on offender ingenuity, social engineering tactics, and the emotional and psychological effects of fraud. [Cross \(2016\)](#) also notes that older victims are frequently

caught in two harmful narratives: being labeled as weak and vulnerable due to age or being blamed as gullible because they were deceived.

The PVP judgment provides strong evidence against victim-blaming interpretations. The principal victims were not pursuing unrealistic rewards or speculative profits. They were responding to perceived legal threats involving arrest, detention, money laundering, drug trafficking, asset seizure, and criminal prosecution. Their compliance was therefore driven by fear and perceived duty, not by greed. This distinction is essential for victim support, because victim-blaming narratives can deepen shame, discourage reporting, and reduce access to help. Cross (2016)'s research on older fraud victims emphasizes that stigma and victim-blaming can themselves become secondary harms.

The PVP case also extends routine activity approaches to cybercrime victimization. Leukfeldt and Yar (2016)'s empirical analysis of routine activity theory in cybercrime found that visibility, accessibility, and guardianship have varying relevance across cybercrime types, with visibility playing a clear role in victimization. The PVP case shows that guardianship was actively neutralized during the interaction. Victims were instructed to remain silent, avoid family consultation, speak in private spaces, act alone when visiting banks, and follow instructions continuously. This means vulnerability was not merely pre-existing; it was produced through offender strategy.

The implications for digital literacy are therefore significant. Standard digital literacy programs often focus on identifying suspicious links, avoiding unknown senders, recognizing poor grammar, protecting passwords, and not sharing OTP codes. These remain important, but the PVP case shows that such programs are insufficient when victims believe they are dealing with legitimate authorities. Jansen and Leukfeldt's (2016) study of victims of online banking found that awareness and protective measures do not always prevent victimization, as individuals may still struggle to assess risks in context or apply protective knowledge under pressure. Norris et al. (2019) similarly found that fraud messages often exploit cognitive pressure, urgency, and credibility cues, meaning that knowledge alone may not translate into safe behavior during high-stress interactions.

Digital literacy programs for authority-impersonation fraud should therefore move beyond generic warnings and develop procedural literacy. Victims need to know not only "do not share OTP codes" but also what legitimate police, courts, prosecutors, banks, and regulators will never do. For example, programs should explicitly teach that legitimate authorities do not ask citizens to transfer money for verification, provide OTP codes, open new accounts for investigation, keep legal proceedings secret from family, or require them to remain on continuous calls while visiting banks. This is directly supported by the PVP case, in which offenders repeatedly instructed victims to disclose assets, provide banking credentials, open new accounts, share OTP codes, and maintain secrecy.

A second implication is that digital literacy must include authority-verification routines. Victims should be trained to pause, disconnect, and independently verify claims through official phone numbers, local police stations, bank branches, or trusted family members. The PVP case shows that offenders sustained control by keeping victims inside the communication channel controlled by the fraud network, especially through VoIP and Zalo. Effective digital literacy should therefore teach victims that verification must occur outside the channel initiated by the caller.

A third implication concerns older adults and relational support. Several principal victims in the PVP case were older adults with significant savings, including LNL, TTTH, DVC, and LTO. Cross's research cautions against treating older victims only through deficit-based assumptions, yet it also shows that isolation and support barriers can intensify fraud vulnerability. Digital literacy programs should therefore be community-based and relational, involving families, banks, local police, senior associations, and community

organizations. The goal should not be to make older adults solely responsible for detecting sophisticated fraud, but to strengthen social guardianship so that consultation becomes normal rather than shameful.

A fourth implication is that digital literacy must address shame and reporting. If victims believe that being deceived is embarrassing or that reporting will expose them to blame, they may delay seeking help. The previous scholarship on online fraud victims shows that shame, stigma, and poor reporting experiences can worsen harm and reduce support-seeking (Button and Cross 2017; Han and Button 2026; Lee 2021). The PVP case reinforces this concern because secrecy was central to fraud. Victims were explicitly instructed not to tell others. Digital literacy programs should therefore include messaging that normalizes reporting, emphasizes offender manipulation, and reassures victims that early disclosure can prevent further loss.

Overall, the PVP case advances research on digital victimization by demonstrating that vulnerability is interactional, situational, and organizationally produced. Victims were not simply deficient in knowledge. They were placed in a controlled communication environment where institutional trust, legal fear, social isolation, and digital banking procedures were combined to produce compliance. This suggests that effective digital literacy must be practical, authority-specific, relational, and trauma-informed (Luong and Ngo 2024; Whittaker et al. 2024). It must teach people not only how to recognize scams, but how to exit coercive communication environments, verify authority independently, and seek help without shame.

5. Conclusions

This article has examined authority impersonation as a structured mechanism of digital victimization through an in-depth qualitative case study of a Vietnamese transnational cyber fraud network. Using the PVP case as the primary empirical foundation, the article has shown that cyber fraud victimization cannot be adequately understood as a simple consequence of technological deception, individual gullibility, or isolated offender behavior. Rather, the case demonstrates how digital victimization was produced through the interaction of organized criminal labor, scripted communication, institutional impersonation, psychological pressure, and digitally mediated financial extraction. The judgment provides unusually detailed evidence of a cyber fraud network operating from Cambodia, recruiting Vietnamese workers, assigning specialized D1-D2-D3 roles, and targeting victims in Vietnam through VoIP calls, Zalo communication, fake police identities, fabricated legal threats, OTP capture, and online banking exploitation.

The first contribution of this article lies in its organizational analysis of authority-based cyber fraud. The PVP case demonstrates that the fraud network operated as a disciplined and specialized criminal enterprise rather than a loose group of scammers. Recruitment through kinship and friendship networks, legal movement from Vietnam to Cambodia, script-based training, performance monitoring, commission-based incentives, passport and phone control, daily meetings, and the use of D1, D2, D3, and technical operator roles all show how cyber fraud was industrialized through organizational structure. This finding contributes to cybercrime scholarship by linking crime script analysis to organized cyber fraud, showing that role specialization not only improved internal efficiency but also strengthened the credibility of the authority-impersonation process.

The second contribution concerns the mechanism of digital victimization. The article has shown that authority impersonation operated through a staged process of legitimation, criminal suspicion, simulated legal authority, and compliance-based extraction. Victims were first contacted through administrative pretexts and accurate personal information, then confronted with fabricated debt allegations, money laundering claims, drug trafficking

accusations, fake warrants, police-style video calls, secrecy instructions, and demands to disclose assets or banking credentials. These findings advance existing work on fraud compliance by showing that victims were not simply deceived into trusting offenders. They were progressively embedded in a fictitious legal process in which cooperation appeared necessary to avoid arrest, prosecution, or asset seizure.

The third contribution relates to victims' vulnerability and harm. The PVP case challenges victim-blaming explanations that portray fraud victims as careless, greedy, or digitally incompetent. The principal victims were responding to perceived legal threats, not pursuing speculative rewards. Their compliance was shaped by fear of criminal liability, trust in state institutions, secrecy instructions, and uncertainty about how legitimate investigations operate. The documented losses were substantial with total documented losses exceeding VND 14.171 billion. Yet the harm was not only financial. Victims were subjected to fear, isolation, reputational anxiety, procedural confusion, and dependency on fraudulent authority figures. This supports victimological scholarship arguing that online fraud produces social and psychological harms that are often underestimated or worsened by shame and victim-blaming responses.

The article also has practical implications for digital literacy and victim protection. Standard digital literacy messages that focus only on suspicious links, unknown senders, passwords, or OTP protection are necessary but insufficient. The PVP case shows that victims may know basic digital safety rules yet still comply when they believe that a police officer, prosecutor, court, or investigative agency is making a lawful demand. Digital literacy programs must therefore incorporate procedural literacy: citizens need to know what legitimate authorities will never do, including requesting OTP codes, asking citizens to transfer money for verification, requiring new bank accounts for investigation, demanding secrecy from family members, or keeping victims on continuous calls while they visit banks. This shift from generic awareness to authority-specific verification is essential because the decisive vulnerability in the PVP case was not simply poor technical knowledge, but uncertainty about legitimate legal procedure.

The study also contributes to the aims of the Special Issue on cybercrime and digital victimization by providing a detailed, case-based account of offenders' methods, victims' vulnerabilities, financial and psychological harms, and implications for prevention and victim support. The Special Issue emphasizes the need for high-quality research on cybercriminal motives and methods, victim impacts, vulnerability analysis, and policy innovation. This article responds directly to that agenda by demonstrating how a single judicial case can reveal the internal organization of a cyber fraud network and the interactional processes through which digital victimization unfolds. The article is necessarily limited by its reliance on one court judgment. Judicial records are shaped by evidentiary rules, prosecutorial framing, and the legal categories through which conduct is interpreted. They may not capture all victim experiences, offender motivations, or organizational dynamics. Nevertheless, the PVP judgment provides an unusually rich and systematically documented account of a transnational cyber fraud network. Its value lies not in statistical generalization, but in analytical generalization: it offers a detailed empirical basis for understanding how authority impersonation operates as a mechanism of digital victimization in organized cyber fraud.

Author Contributions: Conceptualization, T.N.D., H.T.H. and H.T.L.; methodology, H.T.L.; validation, T.N.D., H.T.H. and H.T.L.; formal analysis, T.N.D., H.T.H. and H.T.L.; resources, T.N.D. and H.T.H.; writing—original draft preparation, H.T.L.; writing—review and editing, T.N.D., H.T.H. and H.T.L.; visualization, H.T.L.; supervision, H.T.L.; project administration, H.T.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable due to our study not involving humans.

Informed Consent Statement: Not applicable due to our study not involving humans.

Data Availability Statement: If requested by the editors or reviewers, the full judgment (Vietnamese) can be provided confidentially for verification purposes only and should not be published, circulated, or included as Appendix A. Any shared version should be treated as a restricted-review document, with personal identifiers handled in accordance with the manuscript's pseudonymization protocol. The published article uses only anonymized identifiers because the analytical contribution depends on the organizational structure, crime script, and victimization process, not on publicly identifying individuals.

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

Appendix A. Pseudonymization's Table of the PVP Cyber-Fraud Network

Vietnamese defendants and victims are identified using initials derived from their names. Where initials collide, an additional letter, role marker, or birth-year marker is added to preserve clarity. Unidentified foreign relators are identified using italicized pseudonyms, and no nationality descriptor should be used unless definitively established by the judgment.

Table A1. Vietnamese defendants and proposed manuscript pseudonyms.

No.	Pseudonym	Role/Status in Judgment	Notes
1	PVP	Primary Vietnamese organiser/manager; recruited workers and coordinated Vietnamese staff	Use PVP throughout; do not use real name in manuscript
2	DVTg	Manager/participant; delegated management and salary functions in later operation	DVTg avoids confusion with DVTu
3	NTTho	D2/D3 participant in authority-impersonation process	Longer form avoids collision with other Nguyen names
4	NTS	D1 participant; initial-contact role in LNL case	
5	NDQ	Participant across D1-D3 roles	
6	LTNH	D1 participant; initial-contact role in TTTH case	
7	BKT	Participant/defendant	
8	NVD	Technical/PC-related role; prepared or supported fake documents in LNL narrative	
9	HCT	Participant/defendant	
10	NTTh98	Participant/defendant	Birth year marker distinguishes from another Nguyen Thi Thuy
11	PTT	Participant/defendant	
12	DDQ	D2 participant; authority-construction role in TTTH case	
13	HTTu	Participant/defendant	Final letter distinguishes from Hoang Thi Sinh victim
14	TTHu	Participant/defendant	Distinguishes from TTTH victim
15	TVTt	Participant/defendant	
16	TTVi	Participant/defendant; absent/fugitive in trial record	
17	THV	D1/D2 participant	
18	PTN	D1 participant; initial-contact role in LTO case	
19	TVQ	Participant/defendant	
20	NVQ	Participant/defendant	
21	NTHa	Participant/defendant	

Table A1. *Cont.*

No.	Pseudonym	Role/Status in Judgment	Notes
22	TTTh	Participant/defendant; D1 role in DVC case	Distinguish from Nguyen Thi Thuy defendants
23	TTX	Participant/defendant	
24	TVTo	Participant/defendant	
25	DTN	Participant/defendant	
26	DVTu	D1-D3 participant; D3/authority role in TTTH case	DVTu avoids confusion with DVTg
27	PVM	Participant/defendant	
28	TVP	Participant/defendant	
29	NVH	D2/D3 participant	
30	TSV	D2 manager/participant	Birth year marker distinguishes from NTTh98
31	PTBN	Participant/defendant	
32	LVT	Participant/defendant	
33	NTTh95	Participant/defendant	

Table A2. Victims and proposed manuscript pseudonyms.

No.	Pseudonym	Role/Status in Judgment	Notes
1	LNL	Principal victim; loss approximately VND 8.740 billion	Use LNL; optionally describe as older adult victim
2	LTO	Principal victim; loss approximately VND 87 million	
3	HTS	Principal victim; loss approximately VND 2.722 billion	
4	DVC	Principal victim; loss approximately VND 443 million	
5	TTTH	Principal victim; loss approximately VND 2.179 billion	

Table A3. Unidentified foreign or non-fully identified actors and italicized pseudonyms.

No.	Pseudonym	Role/Status in Judgment	Notes
1	AM	Unidentified foreign organiser; associated with first Sihanoukville operation	Use italicised pseudonym; avoid nationality claim unless directly quoting judgment
2	AT	Unidentified foreign manager/technical actor associated with first operation	Use italicised pseudonym
3	BM	Unidentified organiser associated with second Sihanoukville operation	Use italicised pseudonym; avoid identifying descriptors
4	AH	Unidentified technical/PC actor associated with second operation	Use italicised pseudonym
5	VY	Interpreter/translator in first operation	Use italicised pseudonym
6	LY	Interpreter/translator referenced in LNL account	If same person as VY is uncertain, retain separate pseudonym
7	BO	Interpreter/managerial support in second operation	Use italicised pseudonym
8	BB	Managerial/D3 role under second organiser	Use italicised pseudonym

References

- Asyali, Ayşe Nur, Muriel-Larissa Frank, and Pol Hölzmer. 2026. Fake it till you make it: The psychological and communication tactics behind “Pig Butchering” scams. *Journal of Cybersecurity* 12: tyag003. [\[CrossRef\]](#)
- Button, Mark, and Cassandra Cross. 2017. *Cyber Frauds, Scams and Their Victims*. London: Routledge.
- Button, Mark, Suleman Lazarus, Branislav Hock, Paul Gilmour, Durgesh Pandey, and James Bugbilla Sabia. 2026. Evolutionary fraud, the global scamming ecosystem and a typology of actors. *International Journal of Law, Crime and Justice* 84: 100825. [\[CrossRef\]](#)
- Carter, Elisabeth. 2023. Confirm Not Command: Examining Fraudsters’ Use of Language to Compel Victim Compliance in Their Own Exploitation. *The British Journal of Criminology* 63: 1405–22. [\[CrossRef\]](#)
- Cheurprakobkit, Sutham, Dhanakorn Mulaphong, Patreeya Kitcharoen, and Porntida Visaetsilapanonta. 2026. Scammers’ roles and online fraud process: Perspectives of the elder victims in Thailand. *International Review of Victimology*, 1–18. [\[CrossRef\]](#)
- Cornish, Derek. 1994. The Procedural Analysis of Offending and Its Relevance for Situational Prevention. In *Crime Prevention Studies*. Edited by Ronald V. Clarke. New York: Criminal Justice Press, vol. 3, pp. 151–96.
- Cross, Cassandra. 2016. They’re Very Lonely’: Understanding the Fraud Victimisation of Senior. *International Journal for Crime, Justice and Social Democracy* 5: 60–75. [\[CrossRef\]](#)
- Flyvbjerg, Bent. 2006. Five misunderstandings about case-study research. *Qualitative Inquiry* 12: 219–45. [\[CrossRef\]](#)
- Franceschini, Ivan, Caitlin Wyndham, Luong Le, Ling Li, Carlota Torres Lliró, Jhinuk Mukhopadhyay, and Mark Bo. 2026. Imperfect Victims: Comparing Chinese and Vietnamese Survivors of Forced Criminality in Southeast Asia’s Online Scam Industry. *Asian Journal of Criminology* 21: 28. [\[CrossRef\]](#)
- Franceschini, Ivan, Ling Li, and Mark Bo. 2025. *Scam: Inside Southeast Asia’s Cybercrime Compounds*. London: Verso Books.
- GITOC. 2025. *Compound Crime: Cyber Scam Operations in Southeast Asia*. Geneva: Global Initiative Against Transnational Organized Crime (GI TOC). Available online: <https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf> (accessed on 10 December 2025).
- Han, Bing, and Mark Button. 2026. An Anatomy of ‘Pig Butchering Scams’: Chinese Victims and Police Officers’ Perspectives. *Deviant Behavior* 47: 635–53. [\[CrossRef\]](#)
- Holt, Thomas J., and Jin R. Lee. 2022. A Crime Script Analysis of Counterfeit Identity Document Procurement Online. *Deviant Behavior* 43: 285–302. [\[CrossRef\]](#)
- Hutchings, Alice, and Thomas J. Holt. 2015. A Crime Script Analysis of the Online Stolen Data Market. *British Journal of Criminology* 55: 596–614. [\[CrossRef\]](#)
- Jansen, Jurjen, and Rutger Leukfeldt. 2016. Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *International Journal of Cyber Criminology* 10: 79–91. [\[CrossRef\]](#)
- Lazarus, Suleman, Mina Chiang, and Mark Button. 2025. Assessing Human Trafficking and Cybercrime Intersections Through Survivor Narratives. *Deviant Behavior* 47: 1252–69. [\[CrossRef\]](#)
- Lazarus, Suleman, Mina Chiang, Rossitza Stefanova Dimitrova, Theint Theint Thu, and Enobong Essien. 2026. What Do We Know About Human Trafficking and Scam Compounds in Southeast Asia (2020–2025)? A Qualitative Meta-Synthesis of Coercive Deviant Enterprises. *Deviant Behavior* 47: 1091–123. [\[CrossRef\]](#)
- Leclerc, Benoit, and Elena Morgenthaler. 2023. Examining Emerging Fraud Facilitated by the Internet Through Crime Scripts. *Trends & Issues in Crime and Criminal Justice* 680: 1–28.
- Lee, Claire. 2021. How Online Fraud Victims are Targeted in China: A Crime Script Analysis of Baidu Tieba C2C Fraud. *Crime & Delinquency* 68: 2529–53. [\[CrossRef\]](#)
- Leukfeldt, Rutger, and Majid Yar. 2016. Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior* 37: 263–80. [\[CrossRef\]](#)
- Leukfeldt, Rutger, and Thomas Holt, eds. 2020. *The Human Factor of Cybercrime*. London: Routledge.
- Leukfeldt, Rutger, Anita Lavorgna, and Edward R. Kleemans. 2017. Organised Cybercrime or Cybercrime that Is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Crime Policy and Research* 23: 287–300. [\[CrossRef\]](#)
- Liu, Mengna, Xiqiao Liang, and Jinshi Chen. 2024. Constructing identities in institutional impersonation fraud: Self-styling and other-styling practices through stances. *Humanities and Social Science Communications* 11: 1467. [\[CrossRef\]](#)
- Luong, Hai Thanh. 2025. “Simple job, high salary”: Unveiling the complexity of scam-forced criminality in Southeast Asia. *Humanities and Social Science Communications* 12: 1305. [\[CrossRef\]](#)
- Luong, Hai Thanh, and Hieu Minh Ngo. 2024. Understanding the Nature of the Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam’s Perspective. *Laws* 13: 70. [\[CrossRef\]](#)
- Norris, Gareth, Alexandra Brookes, and David Dowell. 2019. The psychology of Internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology* 34: 231–45. [\[CrossRef\]](#)
- Robert, James, Varsha Singh, Ravi P. Pandey, and Bismirty Bhuyan. 2026. Digital arrest in the cyber age: A psychological perspective on fear, authority, and consciousness. *Frontiers in Psychology* 17: 1726740. [\[CrossRef\]](#)

- Stake, Robert. 1995. *The Art of Case Study Research*. Thousand Oaks: Sage.
- UNODC. 2024. *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape*. Vienna: United Nations Office on Drugs and Crime (UNODC). Available online: https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf (accessed on 10 December 2025).
- UNODC. 2025. *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*. Vienna: United Nations Of Drugs and Crime (UNODC).
- UNODC. 2026. *An Interconnected Criminal Ecosystem: Transnational Organized Crime Threat Assessment for South-East Asia*. Vienna: United Nations Office on Drugs and Crime (UNODC). Available online: https://www.unodc.org/roseap/uploads/documents/Publications/2026/TOCTA_South-East_Asia_2026.pdf (accessed on 25 August 2026).
- USIP. 2024. *Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security*. Florence: United States Institute of Peace (USIP).
- Whittaker, Jack M., Suleman Lazarus, and Taidgh Corcora. 2024. Are fraud victims nothing more than animals? Critiquing the propagation of “pig butchering” (Sha Zhu Pan, 杀猪盘). *Journal of Economic Criminology* 3: 100052. [CrossRef]
- Yin, Robert. 2018. *Case Study Research and Applications: Design and Methods*, 6th ed. Thousand Oaks: Sage.
- Yu, Lei, Gary Mottola, Christine N. Kieffer, Robert Mascio, Olivia Valdes, David A. Bennett, and Patricia A. Boyle. 2023. Vulnerability of Older Adults to Government Impersonation Scams. *JAMA Network Open* 6: e2335319. [CrossRef]

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