laws

MDPI

Article

Understanding the Nature of the Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam's Perspective

Hai Thanh Luong [1,*] and Hieu Minh Ngo [2]

[1] School of Criminology and Criminal Justice, Griffith University, Mt Gravatt, QLD 4122, Australia
[2] National Cyber Security Center, Hanoi VN100000, Vietnam; hieu.ngo@chongluadao.vn
* Correspondence: h.luong@griffith.edu.au

Abstract: Practical challenges and special threats from scam-related fraud exist for regional and local communities in Southeast Asia during and after the COVID-19 pandemic. The rise in pig-butchering operations in Southeast Asia is a major concern due to the increased use of digital technology and online financial transactions. Many of these operations are linked to organized crime syndicates operating across borders, posing challenges for law enforcement. As a first study in Vietnam, we combined the primary and secondary databases to unveil the nature of transnational scam-related fraud. Findings show that scammers are using advanced methods such as phishing, fraudulent investments, and identity theft to maximize their sophisticated tactics for achieving financial possession. There are organized crime rings operating in Vietnam and Cambodia, with Chinese groups playing a leading role behind the scenes. Social media and its various applications have become common platforms for these criminal activities. This study also calls for practical recommendations to consider specific challenges in combating these crimes, including building a strong framework with clear policies, encouraging multiple educational awareness campaigns in communities, enhancing effective cooperation among law enforcement and others, and supporting evidence-based approaches in research and application. While we recognized and assumed that pig-butchering operations with scam-related fraud are a complex problem that requires a well-rounded and coordinated response, the exact approach would depend on each country's specific circumstances.

Keywords: online scam; fraud; pig-butchering; victims; cybercrime; Vietnam

check for updates

Citation: 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. https://doi.org/10.3390/laws13060070

Academic Editor: Kyung-Shick Choi

Received: 28 October 2024
Revised: 16 November 2024
Accepted: 20 November 2024
Published: 21 November 2024

1. Introduction

Among different approaches with their related typologies in cybercrime, contemporary literature focuses toward two levels of cybercrime: cyber-dependent and cyber-enabled (Brewer et al. 2019; Grabosky and Smith 2017; Wall 2001). Meanwhile, the former can be conducted only with the use of technology; the latter includes traditional crimes that can be transformed in their scale and consequence by the adoption of technology (Choi 2008; Choo and Smith 2008). Online scam and fraud behaviors, as the second aspect of cybercrime (cyber-enabled crime), are often considered the final stages after a series of earlier deviant acts through connecting and building trust on social media platforms between offenders and victims (Lee 2020; Nguyen and Luong 2021). In particular, scammers and/or fraudsters gain access to cardholder funds after completion of hacking, phishing, or skimming aimed at stealing bank card data (Choi et al. 2017). In a digitalized world, scam-related frauds are not limited by physical borders and are, therefore, best described as transnational crimes. Cybercriminals may obtain victims' identity information from a distant place using malicious software via masked links. Identity information, such as bank card information, can be used to make online purchases from other countries.

Recently, there have been complex practices of cross-border movement of people involved in different geographical sites that require careful attention; scam crime is conducted via cooperation among criminals located in different countries (Leukfeldt and Holt 2020;

Lusthaus 2020a). The phenomenon in which identity crime is committed by criminals from one country against a victim in another country, who is either of a similar nationality to criminals or not, is described in this paper as transnational scam-related fraud; it usually includes situations where there are multiple offenders located in different countries (Lusthaus and Varese 2021; Nguyen and Luong 2021). A significant number of detected cases in a range of jurisdictions has demonstrated the complex way scam-related crimes are conducted through physical and online cross-border cooperation. In addition, police in several countries have found that international cybercriminals have established bases to commit identity crimes, especially in some developing countries in Southeast Asia, such as the Philippines, Myanmar, Thailand, Indonesia, Cambodia, and Vietnam (Chang 2017; Luong et al. 2019a, 2019b; Lusthaus 2020b).

Transnational scam-related fraud has become a global threat due to the widespread application of information communication technology (ICT). The unprecedented ICT revolution has allowed the remote commission of scam-related fraud via the Internet and wireless communications. Thus, online scammers/fraudsters no longer need to travel across borders with visas and passports to approach victims; instead, they can set up scam-related fraud schemes and obtain money when sitting at one location. One specific example is the pig-butchering operation, which refers to an online investment scam where fraudsters use fictitious online personas to entice victims into bogus investment schemes. It refers to scammers' practices of "fattening up" victims by building trust over time before "slaughtering" them and stealing their money through establishing a series of scripts and layers (Cross 2023, 2024). According to the latest report from the Global Anti-Scam Alliance (GASA 2024), 25.5% of the global population (49,459 individuals from 43 countries) were defrauded, as USD 1.026 trillion was stolen by scammers in 2023. Accordingly, 78% of those participants experienced at least one scam in the last few years, with a dominant occurrence of shopping scams (27%), followed by identity theft (21%) and investment fraud (20%) in multiple forms, in which phone (60%) and text/SMS messages (58%) are continuing to be the highest channels for scam attempt. Over two decades ago, as Peter Grabosky (2001, p. 243) illustrated, while virtual criminality is an old bottle of new wine, the unprecedented capacity of technology to facilitate criminal behaviors has resulted in the novelty of cybercrime. It is an exact confirmation of new threats of transnational scam-related fraud scenarios in Southeast Asia recently. The previous studies have provided notable insights into the commission of crimes in other regions and also demonstrated that cybercriminals participating in networks use various forms (e.g., phones, emails, and banking) and aspects of technology to defraud their victims (Holt and Lee 2022; Hutchings and Holt 2018; Nguyen 2021; Wang et al. 2021).

However, few studies have presented an in-depth discussion of the role of technology in defrauding the cross-border victims of transnational scam-related fraud in Vietnam's, which is presented in this study (i.e., the first study of this kind in the Southeast Asia region). The following are some of the main reasons why Vietnam was chosen over Cambodia as the first study of this kind in this area: Our study uses Vietnam as the exemplar case to explain why criminal networks recruit Vietnamese victims to be involved in the scam compounds in Cambodia. Accordingly, regarding geography, Vietnam and Cambodia share a border, either land or sea. Also, during the post-COVID-19 period, the unemployment rate in Vietnam was very high and, thus, scam compounds in Cambodia took advantage of the simple jobs and high salaries to look for laborers. Particularly, some Vietnamese criminals in Cambodia, who were also victims in the first scenario, have been ready to join the scam activities against the Chinese high-ranking accomplices. Through those actors, the criminal network finds it easier to recruit new Vietnamese victims. Inspired by Dick Hobbs' (1998) analysis that emphasized local aspects of organized crime over transnational ones, the purpose of this paper is to examine whether cybercrime and human trafficking overlap, particularly scam-forced criminality in Vietnam, meeting the criteria of organized crime set out under existing international and domestic legal frameworks. In this qualitative analysis, we combined primary and secondary sources. For the former, we used the latest report, December 2022–December 2023, from the Global Anti-Scam Alliance (GASA), coordinated by the Chongludadao project[1] and with open-access permission from the members, which reflects the state of scams in Vietnam. Some case studies are excerpted from the second author's resources while handling scam-related fraud cases, which are also stored in a personal database with two compressed (zipped) folders, including a thousand photos/videos/conversations. Many of these unique materials have been converted and reported to law enforcement agencies to disrupt the recent rescues. For the latter, we use gray literature from Vietnam's reports, newspapers, and social media to illustrate case studies that are only available in Vietnamese. Also, we reflect on our participants' observations when joining and sharing their experiences at the latest conferences/workshops in the region (Thailand) and national (Vietnam) in 2023–2024.

2. Scam-Related Fraud in Vietnam: Facts and Figures

Within the past two decades of the Internet officially launching in Vietnam (1997), the penetration rate reached nearly 80% of the total population in 2023, or about 80 million users (Nguyen 2024b). Primarily driven by the growing number of Internet users and ICT applications, in 2023, the annual gross merchandise volume of the Internet economy in Vietnam was recorded as the leading rank among all Southeast Asian nations and reached USD 30 billion (Nguyen 2024a). The government has also identified ICT as the key factor in developing the country into one of the leading modern technology centers in the region by 2045. However, the expansion of ICTs and increased Internet penetration have also raised concerns about cyber-enabled crimes, especially since Vietnam is among the top countries in the world to suffer a negative reputation concerning scam-related frauds.

The latest report from the Global Anti-Scam Alliance (GASA 2024), co-coordinated by the Chongluadao project, revealed that Vietnam was the second-worst country globally hit by fraudsters in 2023, with 3.6% of its GDP lost to fraudsters, while Kenya was the worst, as it lost nearly 4.5% of its GDP to scams, followed by Brazil and Thailand (3.2%). To be estimated, a staggering total loss of approximately VND 391.8 trillion (around USD 16.23 million) was recorded in Vietnam.[2] This report is built on a comprehensive survey of 1063 Vietnamese participants, aged from 18 to 54 years, mainly in the group 25–34 (35%), providing valuable insights into the complex network of scams impacting individuals nationwide. Accordingly, most Vietnamese received scams via text/SMS messages and phone calls as the highest and most popular forms, accounting for between 57% and 80%, respectively (see Figure 1).

A substantial 55% of Vietnamese respondents express confidence in their ability to detect scams, while a modest 14% admit to having no confidence at all. At the time of the survey, Vietnamese citizens were confronting scams at an alarming rate—a staggering 70% reported encountering scams at least once a month. The seriousness of the situation is underscored by the concerning statistics that indicate that 49% have witnessed an increase in scams over the past 12 months, highlighting the pervasive and evolving nature of this issue.

Among the 12 selected options for communication channels to be exploited by scammers, Figure 2 shows that Facebook and G-mail are notably the main platforms for scams, with a significant 71% of survey respondents encountering scams through these widely used channels. Following closely, Telegram (28%), Google (13%), and TikTok (13%) are ranked as the third-to-fifth most-exploited channels. Investment scams are reported as the most widespread, cited by 13% of respondents. Interestingly, despite the prevalence of scams, a substantial 56% claim to have experienced no scams in the last year, with an average of 0.8 scams per participant. The impact of scams is deeply felt, especially in cases of identity theft (21%) and shopping scams (21%), leaving lasting effects on victims.

[1] It is one of the leading non-profit organizations in Vietnam focused on preventing cybercrime, and the second author is the founder and main contributor to this report.

[2] The rate of currency and its equivalent exchanges in our article (between VND and USD) are based on the report's collection.

Heartbreaking stories vividly illustrate not only financial losses but also emotional distress, with some victims struggling with thoughts of suicide. The financial impact of scams is substantial, with 29% of participants confirming monetary losses averaging VND 17.7 million (USD 734) per individual. When extrapolated to the national scale, the total loss is estimated to be approximately VND 391.8 trillion (USD 16.23 billion), representing a significant 3.6% of the nation's GDP. However, the limits of the recovery efforts, with only 1% of participants successfully recovering all lost funds, demonstrate what and how the authorities face practical challenges to address these concerns. This point resulted in victim's silent approach, i.e., not reporting the issue to law enforcement (66% out of those respondents). Consequently, this main obstacle requires the authorities to have clearer reporting mechanisms to call citizens for further consideration in sharing and updating data.

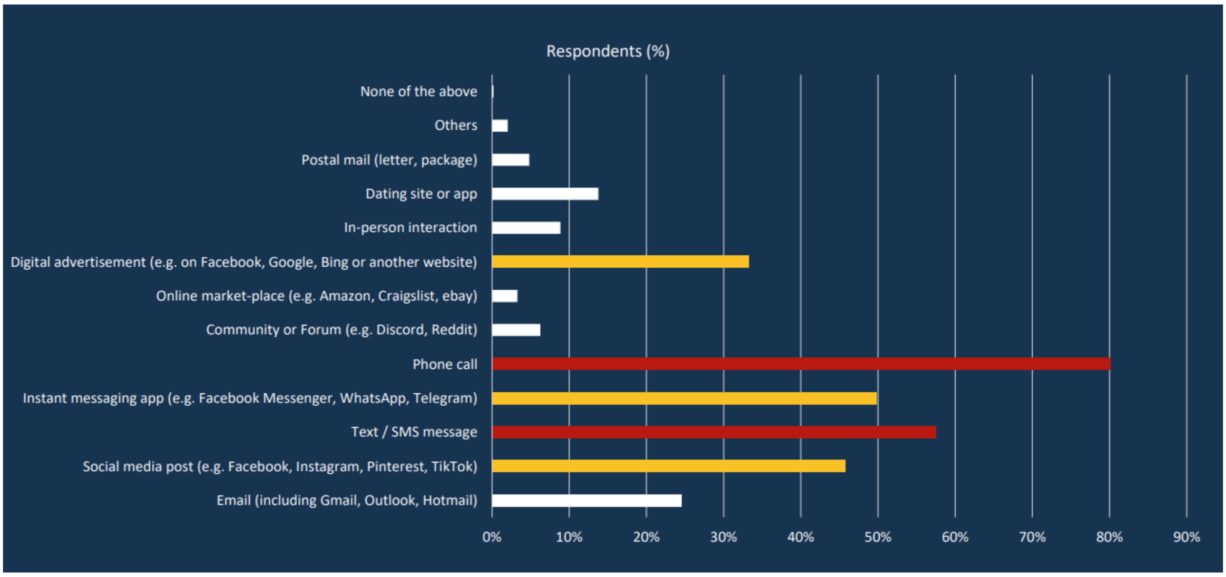


Figure 1. Most Vietnamese receive scam-relate frauds, and different colors mean different levels of respondent rate (Source: Data from the Chongluadao project and its design, which align with the GASA format).

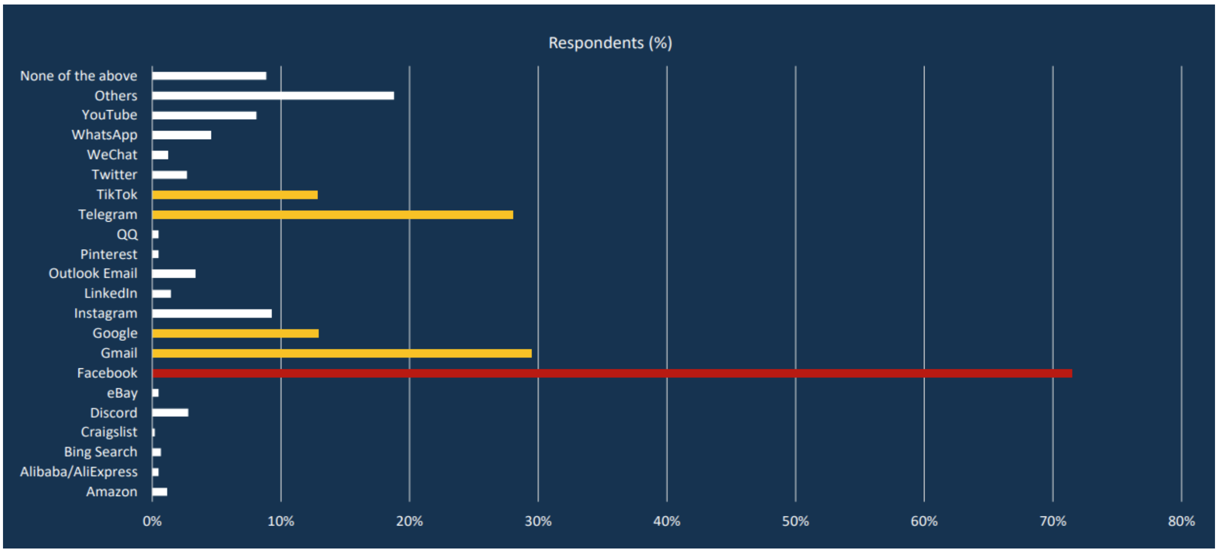


Figure 2. The most used platforms by scammers in Vietnam, different colors mean different levels of respondent rate. (Source: Data from the Chongluadao project and its design, which align with the GASA format).

In the first six months of 2024, there were 60,461 reports related to online scams recorded by the Chongluadao project. The number of reports increased month by month in the first quarter, from only 8667 reports in January to 11,452 reports in March. In particular, March 2024 recorded a sharp increase of 11,452 reports, reflecting a clear escalation in the cybersecurity situation. This can be explained by the need for more vigilance in users after the long break (Lunar New Year) when people are often busy returning to work and daily activities, leading to a decrease in focus and caution in protecting personal information. Among the types of online fraud taking place on social networks, there are up to 24 common types, divided into three main groups including brand counterfeiting, account hijacking, and combined fraud. The target audience of these types includes the elderly, children, students/youth, workers/laborers, and office workers. In the second quarter, the number of reports related to cybersecurity and fraud continued to escalate at an alarming rate. In April, we recorded a total of 10,235 reports, opening the second quarter with a large number of fraud and cyber-attacks. This shows a significant increase compared to the first quarter, possibly due to fraudsters taking advantage of major festivals and holidays to attack users. Although the number of reports decreased (May, with a total of 9523 reports) compared to the previous month, this still does not show a significant decline in the cyber security situation. It also shows that scammers and hackers are very aware of victim's psychology because, after the long holidays on 30 April (known as Reunification Day) and 1 May (known as Labor Day), people's financial conditions will also decrease. June was the month with the highest number of reports in the quarter, with 11,452 reports like March's report, reflecting a clear escalation in cybersecurity and fraud. This increase may be related to the State Bank of Vietnam's Decision No. 2345/QD-NHNN, which came into effect on 1 July 2024, on security solutions such as biometrics for online payments and bank cards. This decision has prompted fraudsters to increase their attacks to exploit weaknesses before new security measures were implemented. Accordingly, scammers can take advantage of this transition period to attack, exploit existing weaknesses, and manipulate victims' psychology. In which, the scammers use malware to take control of the victim's device. After taking control, they collect sensitive data, including images, videos, and eKYC information about the victim. With this information, scammers can access the victim's bank account or e-wallet and steal money by impersonating public service apps such as VNEID (a mobile phone app developed by the National Population Data Center of the Ministry of Public Security) or VSSID (Vietnam Digital Social Security Insurance). Users being lured into installing malware through fake links or applications has become a popular method in the past year, especially targeting users using smartphones, including Android or iOS models. Scammers can remotely control the device and make illegal online money transfers using the victim's biometrics without knowing it.

3. The Profile of Offenders/Victims

This section explains the following: (1) how the victims lured into scam compounds in Cambodia to become scammers work under the Chinese and their accomplices (Cambodians and/or Vietnamese), and (2) how these victims/scammers enter and work under certain conditions at their workplaces. Also, the next section provides brief information regarding the victim's location in Vietnam, gender, and ethnicity.

Our current documents/records reflect the blurred coexistence between former victims and current offenders. They are likely to come from one Vietnamese offender (victim and offender) or through a third person (middleman). For the former, it is clear evidence of an overlapped person who is a Vietnamese victim of a scam operation and returns to the offending role to join the network in Cambodia. They likely still remain in Cambodia to operate in scam compounds or have returned to Vietnam to recruit other potential victims, including their relatives and/or friends. For the latter, the third person includes either a broker/word-of-mouth person or a friend of a friend without identification. They are often at large when investigating and prosecuting and are too difficult for authorities to capture. Regarding their occupation, it is easier to identify their exact place of employment with official records from companies/organizations before joining the scam operation. Our records reflect that either the offender worked in Cambodia in different roles (e.g., translators, master chefs, and/or accountants) or did not work/come to Cambodia (known as unstable jobs) while committing a crime. Those individuals who have experience living and working with Chinese associates in Cambodia's gambling compounds often understand what their demands are directed at new Vietnamese victims and how much commission they can earn from selling these victims. However, in some cases, with personal expectations of gaining benefits, they have actively sought jobs on the Internet and voluntarily joined these illegal gambling groups in Cambodia. Another unique issue for law enforcement agencies is the ability to distinguish between the victim-and-offender overlap and others.

After arriving to Cambodia, victims are recruited to work at establishments that organize fraudulent activities such as online gambling and cryptocurrency trading in cyberspace. During their stay in Cambodia, they were strictly managed, forced to work 12–16 h/day, and not allowed to leave the establishments. When they failed to meet the working frequency, assigned targets, or violated regulations set by the subject side, such as not working enough hours, not attracting enough people to participate in online gambling, or trying to contact the outside, they were tortured, beaten, abused, and overall treated badly. In some situations, there are only two options for them. One option is to call their families and relatives in Vietnam to pay a ransom in order to return home, with an amount ranging from USD 3000 to USD 30,000. The other option is to wait for abusers to quit, and if unlucky, victims die after failing to escape these traps even after the victim's family had paid the amount of money in order to bring the victim's body back to Vietnam.

In terms of geography-based factors, the database reflects a wide range of locations throughout Vietnam that are susceptible to fraudulent activities. Perpetrators and victims can be found in any commune, district, or province across the 63 cities and provinces of Vietnam. This underscores the adaptive and flexible nature of cybercrime, which predominantly operates through various social platforms. While there are no official records from authorities, our reports cover a broad geographical spectrum, encompassing both urban centers and remote communities. These reports span multiple regions across Vietnam, including the north, south, Mekong and Red River Delta provinces, as well as the northern central region and central highlands region.

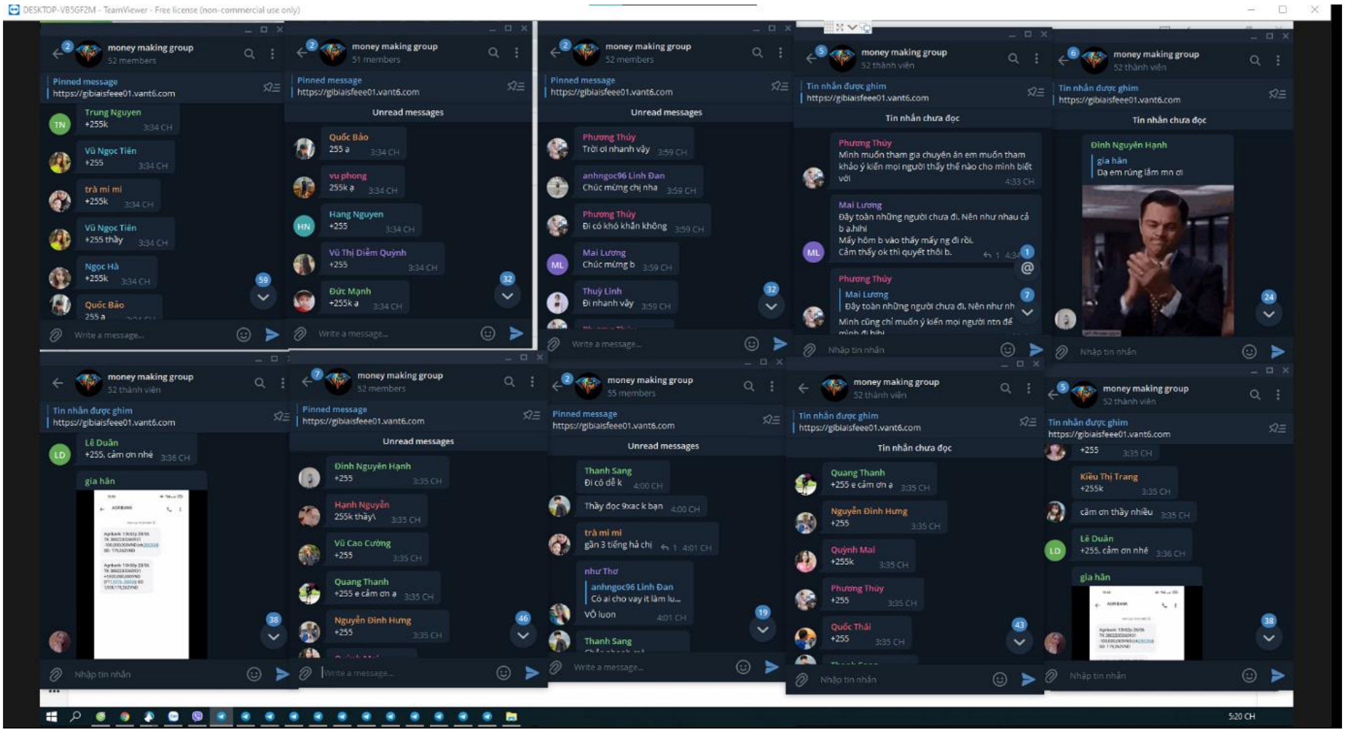
Relating to gender and ethnicity, the mentioned locations encompass both offenders and victims from rural provinces and areas with high ethnic minority populations. Combined with the updated database from the Chongluadao project and our own observations, in Vietnam's context, young males outnumber females as both victims and offenders. Presently, there is insufficient evidence to confirm a focus on ethnicity among offenders in nearly all records. To some extent, we cannot definitively determine the motives of scammers or traffickers in seeking and selling victims. However, our observations and discussions with various participants at conferences and workshops firmly indicate that ethnic minorities are likely to be at a high risk of being scammed or trafficked. This is primarily due to factors such as residing in remote areas with limited access to socio-economic opportunities, inadequate education and related services, limited awareness, a predisposition to trust others easily, and a lack of safety knowledge and skills on social media and online platforms. Additionally, the prevalence of unemployment and unstable employment in rural areas increases the susceptibility of individuals to fall victim to scams and trafficking. Consequently, this elevates the risk of ethnic minorities becoming victims of trafficking and being forced into criminality in the scam-related compounds.

4. Modus Operandi

The current study reiterates that taking advantage of technology and its applications in cyberspace to commit cyber-enabled crimes is an undeniable trend in transnational scam-related fraud (with similar findings from previous research by Cross 2023, 2024; Emami et al. 2019; Franceschini et al. 2023; and Lee 2020, 2021), and Vietnam is no exception. These subjects' methods and tricks often form organized crime rings, carried out in Vietnam and Cambodia with the leading Chinese groups behind the scenes. Social media and its applications have unfortunately become common platforms for criminal groups to carry out scams. Our data show that there are at least eight specific scam categories; they are as follows: (1) high-profit multi-level investment platforms on social platforms (e.g., Zalo, Facebook, Telegram, etc.); (2) giveaways leading to fake job commissions—disguised as popular Vietnamese brands such as Tiki, Shopee, Lazada, or a company name to mislead people into thinking that they are obtaining easy jobs; (3) romance dating; (4) fake/scam online gambling websites; (5) misleading loan apps/websites; (6) impersonations of government companies, authorities, or police officers (e.g., vishing and/or smishing); (7) using malware apps to access and steal personal data; and (8) phishing.

Depending on each scenario, social media and its applications will be designed and applied on a case-by-case basis. Our specific evidence can take the first group—a high-profit investment platform on a social platform—as one typical example (see Figure 3). It is called a 'job advertisement' where using fake information on Facebook/Zalo with a promised salary without special knowledge/skills/degrees is common in all cases. There are two main stages/scripts for conducting this scam category. Firstly, the subjects use social networks (Facebook, Zalo, or Telegram) to post advertisements, recruit workers with the commitment of a "simple job, high salary", or through friends and acquaintances to entice and introduce them to working in Cambodia. In all cases, they were often designed with noticeable slogans and stunning adverts such as 'simple job, high salary' (*viec nhe luong cao* in Vietnamese), 'stable income, no broker, no fee, no experience required' (*Thu nhap on dinh, khong moi gioi, khong mat phi, khong yeu cau kinh nghiem*), 'type words only, light duties' (*chi can danh may, cong viec nhe nhang*), and 'official visa, six months to visit home per time' (*thi thuc chinh ngach, 6 thang ve nha mot lan*). Mostly, all these conversations and exchanges often occurred across Vietnamese territories, either at offender or victim locations and even at third/transit locations. After being trapped and locked in the compounds in Cambodia, the victims become trained to use specific scripts for recruiting new potential victims through social media platforms, online gambling, cryptocurrency investment websites, and other channels. Accordingly, their job here is to entice Vietnamese people to participate in online games, online betting activities, virtual trading floors, or borrow money through applications.

Based on the crime script analysis (Cornish 1994), the script comprises multiple series of scammers with diverse information and relevant activities to achieve the objective at the journey's end. Several detailed scripts are designed and translated into Vietnamese before they spread on specific forums in order to find new victims. This process aims at training these scammers on what and how they will do it through learning with their managers/supervisors. As part of the compulsory stages of the training of trainers (ToT) process, they will cover the duties of setting up and testing scripts, dialogs, conservations, and/or scenarios for scammers to apply in cyberspace. Figure 4, provided by one scammer who was contacted and had a discussion with the second author while handling the case, illustrates detailed scripts with six specific steps (in Vietnamese). In the beginning, after establishing trustworthy relations on social media groups, the victim transferred a small amount of money as a part of the betting task. Taking customer service, the subjects promptly returned the money to their bank account, as promised. This was seen as a way to demonstrate trust and confidence with the customers in the early stages. Then, they will instruct customers to deposit investment money and transfer money to bank account numbers. However, when the victim transferred a larger sum of money and attempted to make a withdrawal, the group of subjects offered various excuses such as system errors, incorrect bank account numbers, or alleged incompleteness of the task to prevent the money from being withdrawn. This script is easily adjusted to become more suitable, depending on the scenario. However, the final purpose of these three steps is to connect and persuade the target to fall for the trap.



DESKTOP-VB5GF2M - TeamViewer - Free license (non-commercial use only)

money making group
52 members
Pinned message
https://gibiaisfeee01.vant6.com

Trung Nguyen
+255k 3:34 CH

Vũ Ngọc Tiến
+255 3:34 CH

trà mi mi
+255k 3:34 CH

Vũ Ngọc Tiến
+255 thầy 3:34 CH

Ngọc Hà
+255k 3:34 CH

Quốc Bảo
255 a

money making group
51 members
Pinned message
https://gibiaisfeee01.vant6.com
Unread messages

Quốc Bảo
255 a 3:34 CH

vu phong
255k ạ 3:34 CH

Hang Nguyen
+255 3:34 CH

Vũ Thị Diễm Quỳnh
+255 3:34 CH

Đức Mạnh
+255k a 3:34 CH

money making group
52 members
Pinned message
https://gibiaisfeee01.vant6.com
Unread messages

Phương Thùy
Trời ơi nhanh vậy 3:59 CH

anhngoc96 Linh Đan
Chúc mừng chị nha 3:59 CH

Phương Thùy
Đi có khó khăn không 3:59 CH

Mai Lương
Chúc mừng b 3:59 CH

Thuỳ Linh
Đi nhanh vậy 3:59 CH

money making group
52 thành viên
Tin nhắn được ghim
https://gibiaisfeee01.vant6.com
Tin nhắn chưa đọc

Phương Thùy
Mình muốn tham gia chuyên án em muốn tham khảo ý kiến mọi người thấy thế nào cho mình biết với 4:33 CH

Mai Lương
Đây toàn những người chưa đi. Nên như nhau cả b a.hihi
Mấy hôm b vào thấy mấy ng đi rồi.
Cảm thấy ok thì quyết thôi b. 4:34

Phương Thùy
Mai Lương
Đây toàn những người chưa đi. Nên như nh
Mình cũng chỉ muốn ý kiến mọi người ntn để mình đi hihi

money making group
52 thành viên
Tin nhắn được ghim
https://gibiaisfeee01.vant6.com
Tin nhắn chưa đọc

Đinh Nguyên Hạnh
gia hân
Dạ em rúng lắm mn ơi

money making group
52 thành viên
Tin nhắn được ghim
https://gibiaisfeee01.vant6.com

Lê Duân
+255, cảm ơn nhé 3:36 CH

gia hân

money making group
52 members
Pinned message
https://gibiaisfeee01.vant6.com
Unread messages

Đinh Nguyên Hạnh
+255 3:35 CH

Hạnh Nguyễn
255k thầy\ 3:35 CH

Vũ Cao Cường
+255 3:35 CH

Quang Thanh
+255 e cảm ơn a 3:35 CH

Nguyễn Đình Hưng
+255 3:35 CH

money making group
55 members
Pinned message
https://gibiaisfeee01.vant6.com
Unread messages

Thanh Sang
Đi có dễ k 4:00 CH

Thầy đọc 9xac k bạn 4:00 CH

trà mi mi
gần 3 tiếng hả chị 4:01 CH

như Thơ
anhngoc96 Linh Đan
Có ai cho vay ít làm lu...
Vô luon 4:01 CH

Thanh Sang

money making group
52 thành viên
Tin nhắn được ghim
https://gibiaisfeee01.vant6.com
Tin nhắn chưa đọc

Quang Thanh
+255 e cảm ơn a 3:35 CH

Nguyễn Đình Hưng
+255 3:35 CH

Quỳnh Mai
+255k 3:35 CH

Phương Thùy
+255 3:35 CH

Quốc Thái
+255 3:35 CH

money making group
52 thành viên
Tin nhắn được ghim
https://gibiaisfeee01.vant6.com

+255 3:35 CH

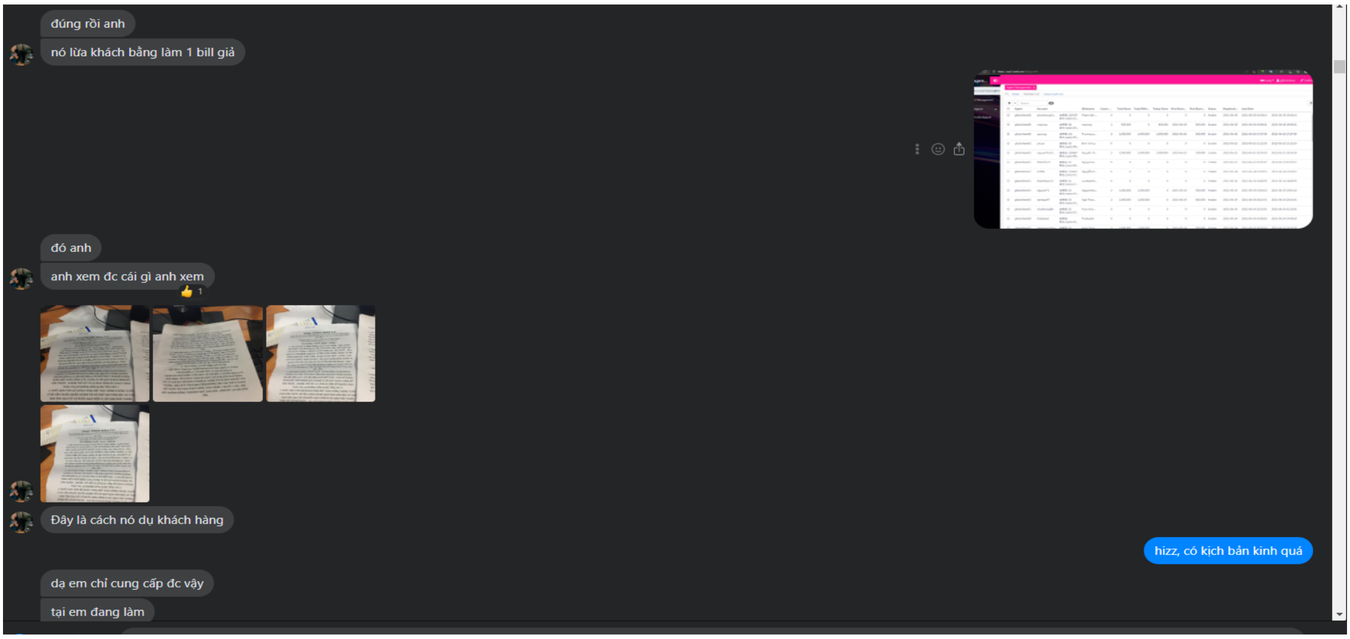
Kiều Thị Trang
+255k 3:35 CH

cảm ơn thầy nhiều 3:35 CH

Lê Duân
+255, cảm ơn nhé 3:36 CH

gia hân

Figure 3. The matrix of the second-by-second conversations among members in the 'money-making group', which is excerpted from the second author's records (Note: All those names are fake names or nicknames of scammers, not victims).



đúng rồi anh

nó lừa khách bằng làm 1 bill giả

đó anh

anh xem đc cái gì anh xem

Đây là cách nó dụ khách hàng

hizz, có kịch bản kinh quá

dạ em chỉ cung cấp đc vậy

tại em đang làm

Figure 4. Part of the Vietnamese detailed scripts used for processing of pig-butchering scams (Sources: The second author's records).

Our records reflect that not all stages appeared together in all selected case studies in this research. However, some stages in each section are likely to occur continuously rather than separately or independently. It will be analyzed in the section below, and it is a scam enterprise structure with its related activities.

5. A Scam Enterprise Structure

We use *Draw.io*, which is a JavaScript and client-side editor for general diagramming/whiteboarding visualization application of information and ideas, to present the detailed structure of a scam-related fraud enterprise. This illustration is based on excerpts from the second author's resources (main drawer) while collecting and analyzing case studies regarding Vietnamese scam-related frauds. It is also combined with the first author's additions from reviewing case-by-case scams in Vietnamese newspapers/online media resources.

Our current data have not officially reflected any Chinese offenders being arrested and prosecuted under the Vietnam criminal code. Although we cannot legally confirm the specific activities of the highest-ranking organizers (level 1—big boss), we can reflect on how they control and manage their networks and operations. In other words, we are confident in drawing this structure based on combining the traceable techniques in cyberspace and reflecting on law enforcement agencies. However, at least three main barriers are impacting accurate evidence regarding the structure of the scam-related fraud enterprise in all cases. Firstly, there is a lack in arrests and prosecutions of the highest players in the whole syndicate/network, comprised mostly of Chinese leaders. Secondly, as part of the 'balloon effect' process, whenever law enforcement agencies disrupt and dismantle the scam operation in one location, they will change and look for another to replace it. Thirdly, there is still limited mutual legal assistance in criminal matters among Southeast Asian countries and/or their counterpart (China) to handle these scams in a timely matter. This caused the slow process of identifying the Chinese roles, and even escaping before law enforcement agencies began their investigation.

Figure 5 shows that four independent teams support bosses. Firstly, the IT team, who are specialists, provide to-do lists for scam centers and the boss. These include the following: (1) an infra-network set-up; (2) app/web distribution; (3) optional selections for crypto wallets for concealing/laundering money; and (4) a phone call system. Secondly, the digital marketing service groups focus on two main duties in the world of Search Engine Optimization (SEO). One is to operate the SEO Backlinks (e.g., Google and CocCoc), which are links on other websites that lead to their website for promoting the votes of credibility. Accordingly, the more high-quality backlinks they have, the higher their website is likely to rank in the search research. The other is to maintain and advertise online ads on social media platforms (e.g., Facebook, Meta, and Google). Thirdly, the data providers cover (1) stolen PII, (2) banking statements, and (3) potential victim lists. Fourthly, money mules provide fraudulent bank accounts and money laundering activities. Among these three groups, the first one will support the boss, while the last two groups will sell their available values to the boss. Currently, our data are insufficient to confirm the exact locations/places of the level 1—boss. In the first scenario, they reside at the scam center's building; if so, they are only confirmed by the arrest of law enforcement agencies. On the other hand, they do not stay there whenever authorities crack down on them and dismantle these centers. While the first one is often not a 'real' big boss, the second one is always at large at the disruption. However, in any situation, they will control and instruct their lower-ranking channels, who are managers (level 2) that live in these scam center blocks.

As our diagram represents, those managers are from various backgrounds with specific skills and come from different countries. The following are some of the main characteristics required for the aforementioned roles: (1) their linguistic capacities (Chinese/Vietnamese/English); (2) direct connection with close flows of information to their boss; (3) their higher commissions in comparison to other group's benefits, which is often based on the monthly money scam; and (4) to be violent in some situations if necessary. Our current database considers that there are specific roles for those managers, which are instructed by their bosses. They create and provide detailed scripts with their related contexts for each scenario and victim. Accordingly, they manage several apps and their related website domains for transferring points to victims' accounts. Those web administrators have the right to intervene and/or edit password information, open bank account numbers, or lock the account. They can even prevent the victim from withdrawing money by creating technical errors. Also, as timekeeping, they will follow up on the timeline and schedule of employees (machines and others) to control all scam key performance indicators (KPI) and money goals, either daily or weekly. Besides that, they also control most fake social media accounts that were created and/or hacked from other resources on the Internet, including Facebook, Telegram, WhatsApp, and/or Zalo. Lastly, they provide cyber slaves (level 3) directly with daily instruction to help them approach their potential victims with smooth procedures and effective measures as practically possible.

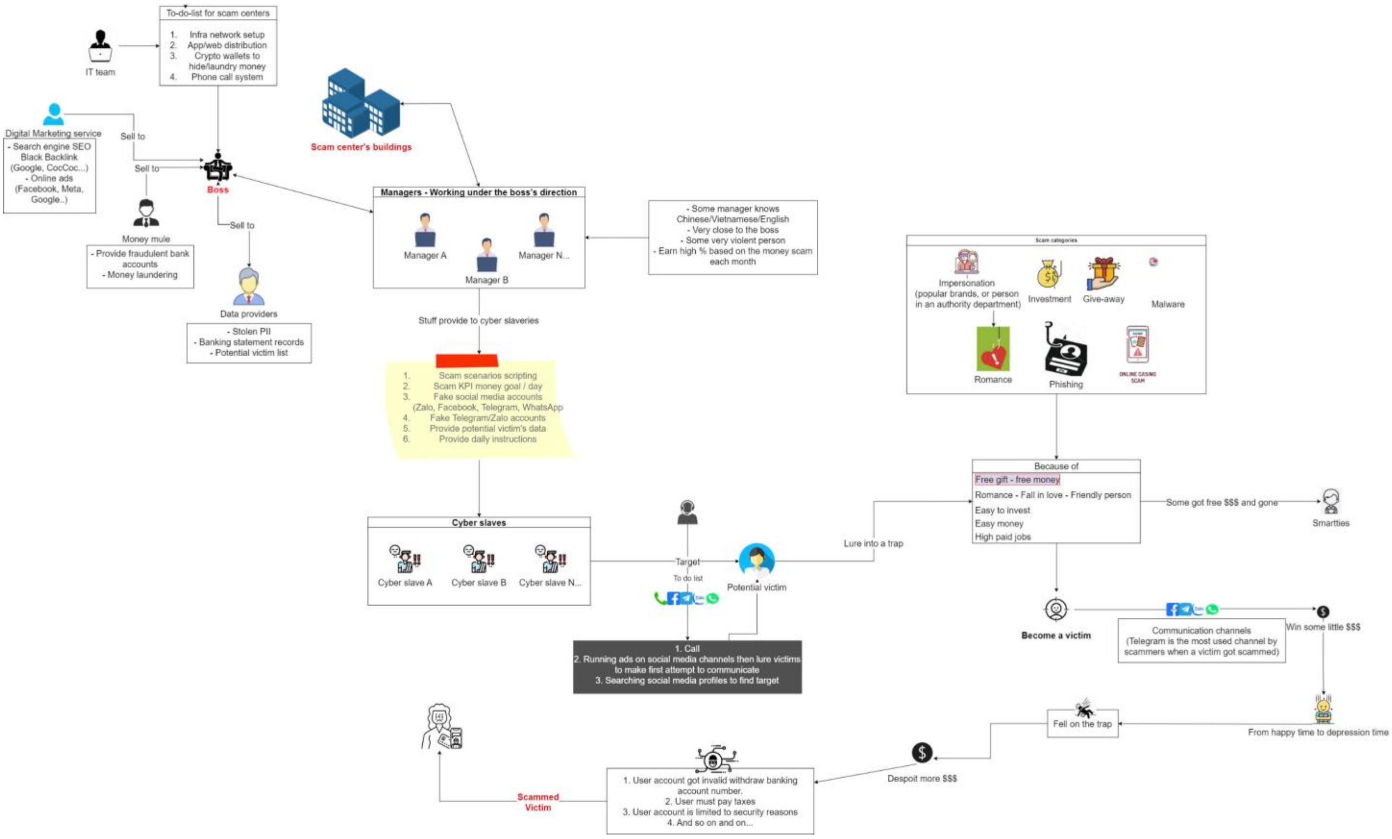

To-do-list for scam centers
1. Infra network setup
2. App/web distribution
3. Crypto wallets to hide/laundry money
4. Phone call system
IT team
Digital Marketing service
- Search engine SEO Black Backlink (Google, CocCoc...)
- Online ads (Facebook, Meta, Google..)
Sell to
Sell to
Boss
Sell to
Money mule
- Provide fraudulent bank accounts
- Money laundering
Data providers
- Stolen PII
- Banking statement records
- Potential victim list
Scam center's buildings
Managers - Working under the boss's direction
Manager A
Manager B
Manager N...
- Some manager knows Chinese/Vietnamese/English
- Very close to the boss
- Some very violent person
- Earn high % based on the money scam each month
Stuff provide to cyber slaveries
1. Scam scenarios scripting
2. Scam KPI money goal / day
3. Fake social media accounts (Zalo, Facebook, Telegram, WhatsApp
4. Fake Telegram/Zalo accounts
5. Provide potential victim's data
6. Provide daily instructions
Cyber slaves
Cyber slave A
Cyber slave B
Cyber slave N...
Target
To do list
Potential victim
1. Call
2. Running ads on social media channels then lure victims to make first attempt to communicate
3. Searching social media profiles to find target
Lure into a trap
Scam categories
Impersonation (popular brands, or person in an authority department)
Investment
Give-away
Malware
Romance
Phishing
ONLINE CASINO SCAM
Because of
Free gift - free money
Romance - Fall in love - Friendly person
Easy to invest
Easy money
High paid jobs
Some got free $$$ and gone
Smarties
Become a victim
Communication channels (Telegram is the most used channel by scammers when a victim got scammed)
Win some little $$$
From happy time to depression time
Fell on the trap
Despoit more $$$
1. User account got invalid withdraw banking account number.
2. User must pay taxes
3. User account is limited to security reasons
4. And so on and on...
Scammed Victim

Figure 5. The original trajectory of the scam-only fraud operation (Source: The authors' own visualizations).

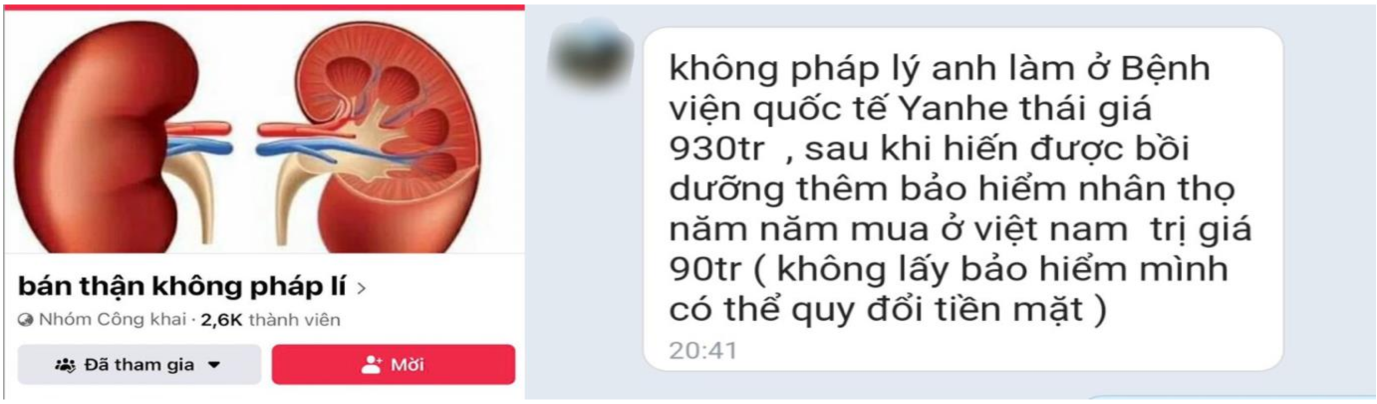
As an illustration in Figure 5, there are spider nets with different layers of cyber-slave staff in each scam compound, which are in Cambodia. There are two main responsibilities of those cyber-enslaved people. First, based on managers' training on committing fraud, such as having employees read documents, "scripts", and fraudulent dialog, they deploy these comprehensive scripts in cyberspace with several online platforms (e.g., Facebook, Telegram, WhatsApp, and/or Zalo). Second, during connections, they had to lure those potential victims with multiple scenarios. These scam scenarios include the following: (1) impersonation (e.g., popular brands or officials from an authorized department such as police, prosecution, court, or bank); (2) investment calls; (3) giving a special gift as a give-away present; (4) using dating apps for romantic purposes; (5) phishing personal accounts; (6) using malware to assess data; and (7) inviting victims to join online casino scams. Almost all potential victims will become 'real' victims with different emotional states, ranging from 'happy' to 'depressed'. Our records show three common reasons to explain why these victims fall into these traps. Accordingly, they often (1) believe scammer advertisements (e.g., 'simple job, high salary'); (2) think it is easy to invest and receive money in return; and (3) fall in love. Based on our systematic reports from the Chongluadao project, Telegram is the most used channel by scammers, among other communicative channels. Whenever they fall into these traps, they are always asked to deposit more money into their account in the system. To maintain those customers engaged (known as victims), scammers often create some specific scripts to respond, including the following: (1) the user account received an invalid withdraw banking account number; (2) the user must pay taxes; and (3) the user account is limited due to security reasons.

6. Nexus Between Cybercrime and Human Trafficking

By examining the recent findings regarding the nexus of pig-butchering and trafficking of persons in the Southeast Asian region (OHCHR 2023; UNODC 2024a, 2024b; USIP 2024), our study also investigates and gauges this new concern in Vietnam. The scheme often begins with a casual conversation initiated by a stranger, who may falsely claim to have obtained the victim's contact information from a mutual acquaintance. Ultimately, this results in two groups of victims: the laborers subjected to forced work, debt servitude, and severe physical abuse, and the victims of the online financial scams, which the trafficked individuals are coercing. Both of these victims' scenarios involve working with either traffickers or scammers in their vicious cycle. On the one hand, they will be targeted by traffickers who play an important role in looking for them in various locations across the different countries in the region. On the other hand, scammers manipulate them with enticing promises of high returns, supported by fake images and deceptive portfolios, before trafficking to another country, often Cambodia territories and, to a lesser extent, Laos.

Our current data identify three specific factors explaining why the link between human trafficking and scam-induced criminal activity occurs in Vietnam. Primarily, we recognize that the COVID-19 pandemic and its associated issues have exerted a significant influence on this trend. Among the various negative impacts of the pandemic, high unemployment and limited job opportunities are the primary factors affecting the economic conditions faced by local people in Vietnam. Consequently, individuals are compelled to seek out opportunities to secure employment and maintain their standard of living while the state grapples with the challenge of rebuilding society. In other words, most laborers often need more financial stability to apply for official migration through registered recruitment agencies, which is time-consuming and expensive. Secondly, amid the pandemic and restricted movements, individuals increasingly turn to social media for job vacancies instead of relying on official reports from state authorities. This is considered one of the main issues leading to the proliferation of 'simple job, high salary' advertisements everywhere in cyberspace and on social media platforms. Furthermore, Vietnam lacks educational campaigns and professional skills to better understand the risks of exploitation associated with labor migration, which largely stems from insufficient information dissemination by migration agencies and local authorities during recruitment. Under these disadvantageous circumstances, both scammers and traffickers often exploit them to identify and target potential victims.

Recently, the tricks and promises of finding 'simple job, high salary' jobs that have been widely propagated by law enforcement agencies and local authorities are no longer effective. Scammers and traffickers are now using the trick of buying kidneys at high prices to trick people who want to sell their kidneys illegally across the border and become victims of human trafficking crimes. Through social networking sites such as Facebook, Zalo, and Telegram, they promise to buy kidneys for hundreds of millions of VND. They lure victims in by promising a simple procedure, and financial bonuses with optional benefits combined with lifetime services (see Figure 6). With this trick, they have deceived many people who are in difficult economic situations and trust them to accept the offer. Then, they guide the victims to the Mien Dong Bus Station in Ho Chi Minh City, before sending a car to pick them up and take them to the Moc Bai International Border Gate, Tay Ninh. In almost all cases, those traffickers often take the victims illegally across the border to Cambodia and sell them to online gambling compounds. Our current records show that first-hand connectors can confirm that they were primarily employed by casinos, virtual enterprises, and online gaming compounds for 12–16 h a day, without proper living conditions and with failed work expectations. The individuals were trafficked under false pretenses and found themselves in challenging unescapable situations, where they were controlled under 24/7 security surveillance and bodyguard escorts. Attempting to leave would result in physical abuse, electric shock, or being sold to another employer. Furthermore, those seeking to return to their hometowns were forced to pay a ransom.



bán thận không pháp lí ›

Nhóm Công khai · 2,6K thành viên

không pháp lý anh làm ở Bệnh viện quốc tế Yanhe thái giá 930tr , sau khi hiến được bồi dưỡng thêm bảo hiểm nhân thọ năm năm mua ở việt nam trị giá 90tr (không lấy bảo hiểm mình có thể quy đổi tiền mặt)

20:41

Figure 6. A translated text from Vietnamese to English. Left: Facebook's public group (2.6k members joined)—Sell Kidney without Legal Barriers. Right: @NOLAW: I work at the YANHE International Hospital. The price is VND 930 million (around USD 40,000). After transplanting your kidney, we will offer money (Source: https://congan.kontum.gov.vn/an-ninh-trat-tu/canh-giac-voi-toi-pham-mua-ban-nguoi-qua-thu-doan-mua-than-gia-cao-.html (assessed on 10 August 2024)).

7. Conclusions with Recommendations

In this study, we have yet to examine the hypothesis regarding the symbiotic relationship between the 'political economy' and 'online scam operations.' It has been investigated and demonstrated in Cambodia, Myanmar, and Laos as "part of compound capitalism, a new manifestation of predatory capital" (Franceschini et al. 2023, p. 575). Instead, our primary focus is on identifying trends and patterns in pig-butchering scams in Vietnam and its neighboring countries, particularly Cambodia. This supports Dick Hobbs' (1998) recommendation to explore local organized crime. While many reports indicate a convergence between human trafficking and cyber-enabled crimes at a general or regional level, there is little evidence at the local level. Our findings align with Hobbs' (1998) analysis, which suggests that the current form of 'transnationality' should be reconsidered based on empirical research showing that interlocking networks of locally based serious criminality are typical. This study demonstrates how local Vietnamese criminal groups collaborate with their counterparts in China and Cambodia under Chinese mobster control. Similar suggestions are found in recent studies (Sergi and Lavorgna 2016; Young 2017), which refer to Hobbs' local approach and emphasize the importance of understanding local crime networks to improve international cooperation. Despite some recent reports (OHCHR 2023; UNODC 2024a, 2024b; and USIP 2024), there is a lack of empirical research focusing on individual countries in the region, making it difficult to compare and discuss the characteristics of scam-related frauds in pig-butchering compounds. Therefore, our findings in Vietnam can serve as a valuable resource for promoting bilateral and multilateral cooperation among law enforcement agencies in order combat these operations in Southeast Asia.

Identifying feasible directions with specific initiatives from each country is crucial for expanding regional dialog and building a comprehensive framework against transnational scam-related fraud. Our findings support recent statements (OHCHR 2023; UNODC 2024a, 2024b; and USIP 2024) and highlight the need for a comprehensive strategy at both regional and national levels. To address the proliferation of scam centers in Southeast Asia, particularly in Vietnam, it is essential to develop a comprehensive strategy rather than focusing on individual scenarios. Alternatively, the recommendations below should be synchronized and integrated by the respected government and authorities.

Building a comprehensive policy formulation. The Vietnamese government is developing strategies and policies to tackle these issues, including regulations to combat online scams and human trafficking. They should encourage the use of hardware security tokens (a physical device that generates a unique passcode to authenticate a user's identity and provide an extra layer of security, such as FIDO2 and U2F)[3] like Google Titan and Yubikey to ensure information security and prevent phishing. These technical tools can prevent obtaining account information, which can hamper the data provider, who is one of three independent groups that support the big boss (see Figure 2). For organizations with limited funding, free two-step security tools like Google Authenticator and Microsoft Authy should be promoted. Additionally, early warnings about cybersecurity and information security awareness should be provided through media campaigns. Companies should refer to standards for handling security incidents, cyber security laws, and data security compliance from developed countries such as Australia, Germany, Singapore, and the U.S.A. At the same time, they should pay attention to developing laws for blockchain technology or virtual currencies in order to address these issues.

Raising public awareness through setting up specific propaganda campaigns. Specific propaganda campaigns should be set up to limit fraud and reduce negative factors (Gotelaere and Paoli 2022; Smith and Akman 2008). Local communities should be educated to ensure legitimate job seekers use reliable resources and official job referral centers. Support systems for victims, such as hotlines, counseling services, and legal aid, should be established. Authorities should also encourage the use of virtual private networks (VPNs) in public places to enhance cybersecurity. For companies and organizations, information security awareness should be raised, and infrastructure systems should be strengthened through penetration testing and immediate patching of vulnerabilities. To do this, they need to invest in their capabilities according to the Security Operations Center (SOC) model. They should strengthen the organization with intrusion detection systems (IDS) and intrusion prevention systems (IPS) combined with Security Information and Event Management (SIEM). Additionally, it is necessary to organize training sessions to raise information security awareness for employees and officers on a quarterly and annual bases. Moreover, they need to identify which data are important for the organization, so they can implement the best protection measures.

Enhancing the collaboration between law enforcement and others. Law enforcement should closely monitor fraudulent activities on platforms like Facebook, Telegram, and the Darkweb/Darknet (Luong 2023). It is also worth mentioning that criminals buy, sell, and use personal data, such as credit cards and bank accounts, on domestic and foreign hacker forums. In Vietnam, cybercriminals primarily operate on Telegram and Raidforums. They should also collaborate with organizations focused on anti-fraud, phishing, and scams to exchange data and solutions. In Vietnam, key organizations include NCSC Viet Nam, CocCoc, Chongluadao, and ScamVN. Coordination with international entities like Interpol, Kaspersky, Google, and Microsoft, and those that operate strongly in the field of scams and phishing, such as Scamadviser, Phishstats, and FishTank, is also crucial.

Supporting the evidence-based approach, our findings show that concerns related to pig-butchering scams not only occur in individual countries like Vietnam, but also require shared support from common communities in the region. Regional and national authorities should call for further consideration. It is not just from their policymakers and practitioners but they also invite non-governmental organizations (NGOs), civil society organizations (CSOs), and academics to provide comprehensive reports and analyses of the situation, particularly regarding technology-related issues. These insights are invaluable for understanding the scale of the problem and planning initiatives to combat human trafficking. Based on this scientific evidence, governments can partner with tech companies

[3] Literally, these terms could be understood as follows: (1) FIDO2 (Fast Identity Online 2) is an open standard for user authentication that aims to strengthen the way people sign in to online services to increase overall trust and (2) U2F (Universal 2nd Factor) is an open standard that strengthens and simplifies two-factor authentication (2FA) using a specialized Universal Serial Bus (USB) to protect and unlock supported accounts.

to identify and dismantle scam operations. This could involve developing AI tools for detecting scam activities or tracing cryptocurrency transactions.

These are just a few potential strategies, and the exact approach would depend on each country's specific circumstances, either legal frameworks or technological capabilities. Again, we recognize that pig-butchering operations involving scam-related frauds are complex problems requiring a well-rounded and coordinated response. We also look forward to further collaboration with other authors in order to improve strategies and solutions for addressing these concerns.

Author Contributions: Conceptualization, methodology, formal analysis, writing—original draft preparation, and supervision, H.T.L.; software and visualization, H.M.N.; writing—review and editing, H.T.L. and H.M.N. 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.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article. The original contributions presented in the study are included in the article.

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

References

Brewer, Russell, Vel-Palumbo Melissa, Hutchings Alice, Holt Thomas, Goldsmith Andrew, and Maimon David. 2019. *Cybercrime Prevention: Theory and Applications*. London: Palgrave Macmillan.

Chang, Lennon. 2017. Cybercrime and Cyber Security in ASEAN. In *Comparative Criminology in Asia*. Edited by Jianhong Liu, Max Travers and Lennon Chang. Cham: Springer, pp. 135–48.

Choi, Kwan, Ju-Lak Lee, and Yong-Tae Chun. 2017. Voice phishing fraud and its modus operandi. *Security Journal* 30: 454–66. [CrossRef]

Choi, Kyung-Shick. 2008. Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology* 2: 308–33.

Choo, Kim-Kwang, and Russell Smith. 2008. Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology* 3: 37–59. [CrossRef]

Cornish, Derek. 1994. The Procedural Analysis of Offending and Its Relevance for Situational Prevention. In *Crime Prevention Studies*. Edited by Ronald Clarke. New York: Criminal Justice Press, vol. 3, pp. 151–96.

Cross, Cassandra. 2023. 'I Knew It Was a Scam': Understanding the Triggers for Recognizing Romance Fraud. *Criminology and Public Policy* 22: 613–37. [CrossRef]

Cross, Cassandra. 2024. Romance Baiting, Cryptorom and 'Pig Butchering': An Evolutionary Step in Romance Fraud. *Current Issues in Criminal Justice* 36: 334–46. [CrossRef]

Emami, Catherine, Russell Smith, and Penny Jorna. 2019. *Online Fraud Victimisation in Australia: Risks and Protective Factors*; Research Report. Canberra: Australian Institute of Criminology (AIC). Available online: https://www.aic.gov.au/sites/default/files/2020-05/rr16_online_fraud_victimisation_in_australia-v3.pdf (accessed on 10 November 2022).

Franceschini, Ivan, Ling Li, and Mark Bo. 2023. Compound Capitalism: A Political Economy of Southeast Asia's Online Scam Operations. *Critical Asian Studies* 55: 575–603. [CrossRef]

GASA. 2024. *The Global State of Scams—2023*. The Hague: Global Anti-Scam Alliance (GASA). Available online: https://www.gasa.org/_files/ugd/7bdaac_b0d2ac61904941aeb4cbf0217aa355d2.pdf (accessed on 15 July 2024).

Gotelaere, Sofie, and Letizia Paoli. 2022. Prevention and Control of Financial Fraud: A Scoping Review. *European Journal on Criminal Policy and Research*, 1–22. [CrossRef]

Grabosky, Peter. 2001. Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies* 10: 243–49.

Grabosky, Peter, and Russell Smith. 2017. Cybercrime. In *Crime and Justice: A Guide to Criminology*, 5th ed. Edited by Darren Palmer, Willem de Lint and Derek Dalton. Sydney: Thomson Reuters (Professional) Australian Limited, pp. 243–77.

Hobbs, Dick. 1998. Going Down the Glocal: The Local Context of Organised Crime. *The Howard Journal of Criminal Justice* 37: 407–22. [CrossRef]

Holt, Thomas, and Jin Lee. 2022. A Crime Script Analysis of Counterfeit Identity Document Procurement Online. *Deviant Behavior* 43: 285–302. [CrossRef]

Hutchings, Alice, and Thomas Holt. 2018. Interviewing Cybercrime Offenders. *Journal of Qualitative Criminal Justice & Criminology* 7: 1–23.

Lee, Claire. 2020. A crime script analysis of transnational identity fraud: Migrant offenders' use of technology in South Korea. *Crime, Law and Social Change* 74: 201–18. [CrossRef]

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 Thomas Holt, eds. 2020. *The Human Factor of Cybercrime*. New York: Routledge.

Luong, Hai Thanh. 2023. Foundations and Trends in the Darknet-Related Criminals in the Last 10 Years: A Systematic Literature Review and Bibliometric Analysis. *Security Journal* 37: 535–74. [CrossRef]

Luong, Hai Thanh, Phan Duc Huy, and Chu Van Dung. 2019a. Cybercrime in Legislative Perspectives: A Comparative Analysis Between the Budapest Convention and Vietnam Regulations. *International Journal of Advanced Research in Computer Science* 10: 1–12. [CrossRef]

Luong, Hai Thanh, Phan Duc Huy, Chu Van Dung, Nguyen Quoc Viet, Le Quang Toan, and Hoang Trong Luc. 2019b. Understanding Cybercrimes in Vietnam: From Leading-Point Provisions to Legislative System and Law Enforcement. *International Journal of Cyber Criminology* 13: 290–308.

Lusthaus, Jonathan. 2020a. *Cybercrime in Southeast Asia: Combating a Global Threat Locally*. Policy Brief. Available online: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-05/Cybercrime%20in%20Southeast%20Asia.pdf?naTsKQp2jtSPYsWpSo4YmE1sVBNv_exJ (accessed on 11 December 2021).

Lusthaus, Jonathan. 2020b. Modelling Cybercrime Development: The Case of Vietnam. In *The Human Factor of Cybercrime*. Edited by Rutger Leukfeldt and Thomas Holt. New York: Routledge, pp. 240–57.

Lusthaus, Jonathan, and Federico Varese. 2021. Offline and Local: The Hidden Face of Cybercrime. *Policing: A Journal of Policy and Practice* 15: 4–14. [CrossRef]

Nguyen, Minh Ngoc. 2024a. GMV of the Internet Economy in Vietnam 2015–2025. Available online: https://www.statista.com/statistics/1193113/vietnam-gmv-internet-economy/#:~:text=In%202023,%20the%20annual%20gross,billion%20U.S.%20dollars%20in%202025 (accessed on 18 July 2024).

Nguyen, Minh Ngoc. 2024b. Internet Usage in Vietnam—Statistics & Facts. Available online: https://www.statista.com/topics/6231/internet-usage-in-vietnam/#topicOverview (accessed on 18 July 2024).

Nguyen, Trong Van. 2021. The Modus Operandi of Transnational Computer Fraud: A Crime Script Analysis in Vietnam. *Trends in Organized Crime*, 1–22. [CrossRef]

Nguyen, Trong Van, and Hai Thanh Luong. 2021. The Structure of Cybercrime Networks: Transnational Computer Fraud in Vietnam. *Journal of Crime and Justice* 44: 419–40. [CrossRef]

OHCHR. 2023. *Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response*. Geneva: Office of the United Nations High Commissioner for Human Rights (OHCHR). Available online: https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf (accessed on 10 December 2023).

Sergi, Aanna, and Aanita Lavorgna. 2016. *Ndrangheta: The Glocal Dimensions of the Most Powerful Italian Mafia*. London: Palgrave Macmillan.

Smith, Russell, and Tabor Akman. 2008. Raising Public Awareness of Consumer Fraud in Australia. *Trends & Issues in Crime and Criminal Justice* 349: 1–6.

UNODC. 2024a. *Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia*. Vienna: United Nations Office on Drugs and Crime (UNODC). Available online: https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf (accessed on 19 July 2024).

UNODC. 2024b. *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 27 October 2024).

USIP. 2024. *Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security*. Washington, DC: United States Institute of Peace (USIP). Available online: https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf (accessed on 28 September 2024).

Wall, David. 2001. Cybercrimes and the Internet. In *Crime and the Internet: Cybercrimes and Cyberfears*. Edited by David Wall. New York: Routledge, pp. 1–17.

Wang, Peng, Mei Su, and Jingyi Wang. 2021. Organized Crime in Cyberspace: How Traditional Organized Criminal Groups Exploit the Online Peer-to-Peer Lending Market in China. *British Journal of Criminology* 61: 303–24. [CrossRef]

Young, Mary. 2017. "Going Down the Glocal": Wildlife Crime in Vietnam. *The European Review of Organized Crime* 4: 54–83.

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.