Safer Internet Lab
Led by CSIS in partnership with Google

Centre for Strategic and International Studies

Google

Research report

Online Fraud and Scams in Vietnam

Safer Internet Lab

Online Fraud and Scams in Vietnam

Thao Phuong Nong[1]

INTRODUCTION

In recent years, Vietnam has witnessed rapid digital transformation, driven by the expansion of e-commerce, digital banking, and widespread internet penetration. As the country embraces new technologies, the risks associated with cyber threats have also intensified, with online scams emerging as a significant concern. Among these, the rise of generative artificial intelligence (AI) has introduced a new dimension to cyber fraud, enabling scammers to create highly sophisticated and convincing schemes that exploit unsuspecting individuals and businesses. AI-powered tools allow cybercriminals to automate large-scale phishing attacks, develop deepfake videos for identity theft, and produce fraudulent websites that closely mimic legitimate ones. The evolving landscape of online scams threatens not only financial security but also public trust in Vietnam's digital ecosystem, posing challenges for the government, businesses, and individuals alike.

Vietnam's dynamic economic growth, coupled with its strategic position in the ASEAN region, makes it an attractive target for cybercriminals operating across borders. As one of the fastest-growing digital economies in Southeast Asia, the country has experienced a surge in cross-border online fraud incidents, where scammers leverage AI to exploit regulatory loopholes and jurisdictional challenges. The increasing reliance on digital platforms for financial transactions and communication further exacerbates the situation, making it imperative for Vietnam to adopt a proactive approach in addressing the threats posed by AI-driven scams. The regulatory and law enforcement mechanisms currently in place are often reactive rather than preventive, highlighting the need for a comprehensive strategy that integrates technological solutions with policy interventions.

Vietnam's government, in collaboration with international partners, has launched various initiatives to enhance cybersecurity awareness and strengthen its digital infrastructure. However, public awareness campaigns have not kept pace with the sophistication of AI-driven scams, leaving many citizens and small businesses vulnerable to cyber threats. The private sector, including banks and e-commerce platforms, has also taken steps to implement fraud detection systems powered by AI; however, the lack of collaboration and information-sharing between stakeholders remains a significant barrier to comprehensive fraud prevention efforts.

This study aims to provide an in-depth analysis of the current patterns and trends of AI-enabled online scams in Vietnam, offering insights into the evolving tactics used by cybercriminals and the vulnerabilities that exist within the country's digital infrastructure. It will assess the effectiveness of existing national and regional policies designed to combat online fraud, identifying gaps and areas for

[1] Central Institute for Economic Management (CEM)

improvement. The research also seeks to evaluate the social and economic impact of such scams on businesses and individuals, with a particular focus on vulnerable populations, such as small and medium enterprises (SMEs) and individuals with limited digital literacy.

The scope of this study encompasses both domestic and cross-border aspects of online scams, recognizing that the problem is not confined within national borders. Vietnam's participation in regional frameworks, such as the ASEAN Cybersecurity Cooperation Strategy, underscores the importance of collaborative efforts in tackling cyber threats. The study will explore the roles of key stakeholders, including government agencies, the financial sector, e-commerce platforms, telecom companies, and civil society organizations, in developing and implementing effective countermeasures. Understanding the challenges faced by these actors is crucial for formulating targeted policy recommendations that enhance Vietnam's resilience against AI-powered cyber fraud.

Addressing the threats posed by AI-driven online scams is critical for ensuring Vietnam's continued digital growth and economic development. The country’s ambition to become a regional digital hub necessitates robust cybersecurity measures that not only deter cybercriminals but also foster public confidence in digital platforms. This study will offer strategic recommendations aimed at strengthening Vietnam’s regulatory frameworks, improving cross-border collaboration, and enhancing public awareness initiatives. By leveraging both domestic and international best practices, Vietnam can build a more secure and trustworthy digital environment, protecting its citizens and businesses from the ever-evolving threats of AI-enabled online fraud.

FINDINGS AND ANALYSIS

Patterns and Trends

Types of Scams

Online scams in Vietnam are an issue that has been and continues to receive significant attention from society. Malicious actors are taking advantage of the rapid explosion of information technology, including advancements in artificial intelligence (AI), to carry out numerous online fraud schemes, seizing high-value assets. The rise of generative AI and sophisticated AI tools has enabled scammers to automate and scale their operations, making scams more convincing and harder to detect.

There are three main types of online scams in Vietnam such as brand impersonation, account takeover, and various hybrid methods—with 24 specific scam tactics currently occurring in Vietnam's cyberspace. Scammers increasingly leverage AI-driven techniques, such as deepfake technology, AI-generated phishing emails, and voice cloning, to impersonate trusted individuals or organizations with an unprecedented level of realism. This has resulted in a growing number of victims falling prey to fraudulent schemes that exploit AI-generated content to bypass traditional security measures.

Table 1: Summary of 24 specific scam tactics in Vietnam

No	Scam type	Description	AI Technology/ Traditional
1.	Deepfake, Deepvoice video call scam	Scams using AI-generated voices and videos to impersonate individuals.	AI Technology
2.	Cheap travel package scam	Fraudulent offers of low-cost travel packages.	Traditional
3.	SIM card lock scam	Claiming a SIM card will be locked due to incomplete subscriber verification.	Traditional
4.	Fake successful money transfer receipt	Scammers forge receipts to show false transactions.	Traditional
5.	Impersonating teachers/medical staff	Scammers claim a relative is in an emergency to extort money.	Traditional
6.	Child model recruitment scam	Fraudsters lure victims with fake model job offers.	Traditional
7.	Financial institution impersonation	Scammers pose as banks or financial companies.	Traditional
8.	Gambling, betting, and loan app scams	Fraudulent apps and links promoting illegal gambling and loans.	Traditional
9.	Fake websites of institutions and businesses	Impersonation of official websites (e.g., social insurance, banks).	Traditional
10.	SMS brandname scam	Distribution of fraudulent SMS messages.	Traditional
11.	Stock, cryptocurrency, and Ponzi scheme scams	Fake investment opportunities promising high returns.	Traditional
12.	Online collaborator recruitment scam	False job offers for online work.	Traditional
13.	Social media account hacking	Stealing accounts to send scam messages.	Traditional

14.	Law enforcement impersonation scam	Fraudsters posing as police, prosecutors, or courts.	Traditional
15.	Selling counterfeit goods on e-commerce platforms	Fake products sold online.	Traditional
16.	Identity theft for credit loans	Using stolen ID cards to take out loans.	Traditional
17.	Accidental bank transfer scam	Scammers claim accidental transfers to demand refunds.	Traditional
18.	Fraudulent recovery services	Scams claiming to recover lost money.	Traditional
19.	Telegram OTP theft	Stealing Telegram OTP codes to gain access.	Traditional
20.	Fake money loss call scams like FlashAI	Spreading false news about losing money through calls.	AI Technology
21.	Facebook recovery service scam	Scams claiming to recover lost Facebook accounts.	Traditional
22.	Romance and financial investment scams	Luring victims with love, fake investments, parcel deliveries, or lottery winnings.	Traditional
23.	Phishing links and fake ads on Facebook	Fraudulent links and deceptive advertisements.	AI Technology
24.	Lottery number scam	Providing fake lottery number predictions.	Traditional

Source: MIC and author's compilation

AI-powered scams, such as deepfake and deepvoice video call scams, represent a new frontier in online fraud. These technologies allow scammers to convincingly impersonate individuals, exploiting trust-based relationships to deceive victims. For instance, using deepfake videos and voice cloning, criminals can impersonate a family member or colleague in real-time video calls, making their fraudulent requests seem authentic. Similarly, phishing links and deceptive advertisements on platforms like Facebook are increasingly powered by AI algorithms that analyze user behavior to target victims more effectively. These scams demonstrate the transformative power of AI in amplifying the scale and sophistication of cybercrime in Vietnam. Another noteworthy example is the "FlashAI" scam, which leverages AI-generated fake calls or messages to manipulate victims into believing they are losing money. The psychological pressure created by such real-time and personalized interactions significantly increases the success rate of these scams. These methods highlight the evolving nature of fraud, where AI enables precise targeting and realistic simulations that traditional methods cannot achieve.

Despite the rise of AI-driven fraud, traditional scams remain a significant concern in Vietnam. These include tactics like impersonating financial institutions, forging money transfer receipts, and creating fake job opportunities. Such scams often exploit low digital literacy, trust in official institutions, and lack of robust verification mechanisms. For example, scams involving fake SIM card lock warnings or counterfeit e-commerce platforms capitalize on users' unfamiliarity with digital safety practices. While these methods lack the technological sophistication of AI-driven scams, they are still effective due to their simplicity and adaptability to various contexts.

Targeted Victims

Scammers today employ a wide array of increasingly sophisticated techniques, leveraging both traditional and AI-driven methods to target two key categories: individuals and organizations/businesses. This segmentation allows scammers to tailor their methods based on the vulnerabilities, behaviors, and digital footprints of their targets.

a. Individual Targets

With AI-powered data analysis and social engineering tactics, scammers can personalize their attacks based on an individual's online behavior, preferences, and vulnerabilities. For each age group, scammers use different AI-driven tactics to lure their victims, such as chatbot-based fraud schemes or AI-generated fake news to manipulate trust. The common goal remains to gain trust, steal personal information, and ultimately misappropriate assets.

Table 2. The target groups and the types of scams associated with each group

Target group	Types of scams	AI Technology or Traditional
Elderly	1. Travel package scams with "cheap combos."	Traditional
	2. Scams involving Deepfake video calls.	AI Technology
	3. "SIM lock" scams due to incomplete registration of phone numbers.	Traditional
	4. Impersonation for successful money transfers.	Traditional
	5. Fake messages impersonating government, enterprises, or organizations (e.g., social insurance, banks).	Traditional

	6. Fake brand name promotional messages.	Traditional
	7. Impersonation of police, investigators, courts, via fraudulent phone calls.	Traditional
	8. Scams involving low-quality goods on e-commerce platforms.	Traditional
	9. Stealing personal information from ID cards for fraudulent activities.	Traditional
	10. Fake accidental transfers to bank accounts.	Traditional
	11. Service scams targeting Facebook account recovery.	Traditional
	12. Emotional manipulation, investments, or fraudulent packages.	Traditional
	13. Phishing links via fake advertisements on Facebook.	Traditional
	14. Scams involving betting or gambling.	Traditional
	15. Spreading fake news about losing money.	Traditional
Children (under age 18)	1. Scams involving Deepfake video calls.	AI Technology
	2. Scams with emotional manipulation or sharing sensitive images.	Traditional
	3. Facebook account recovery service scams.	Traditional
Students/Youth	1. Travel package scams with "cheap combos."	Traditional
	2. Scams involving Deepfake video calls.	AI Technology
	3. "SIM lock" scams due to incomplete registration of phone numbers.	Traditional
	4. Fraudulent gambling apps, betting, or black-market links.	Traditional
	5. Fake brand name promotional messages.	Traditional
	6. Financial fraud or fake investment scams.	Traditional
	7. Fake online collaborator recruitment.	Traditional
	8. Impersonation of police, investigators, courts, via fraudulent phone calls.	Traditional
	9. Scams involving low-quality goods on e-commerce platforms.	Traditional

	10. Stealing personal information from ID cards for fraudulent activities.	Traditional
	11. Fake accidental transfers to bank accounts.	Traditional
	12. Service scams targeting Facebook account recovery.	Traditional
	13. Emotional manipulation, investments, or fraudulent packages.	Traditional

Source: MIC and author's compilation

The table highlights a mix of traditional fraud methods and emerging AI-driven scams, shedding light on the evolving cyber threat landscape in the country. The presence of both types emphasizes the urgent need for multi-faceted responses to protect vulnerable populations from exploitation.

AI-driven scams, such as those involving Deepfake video calls, demonstrate how malicious actors leverage advanced technologies to enhance the believability of their schemes. Deepfake technology enables scammers to mimic voices and appearances, making impersonation highly realistic. This is particularly concerning in a country like Vietnam, where digital transformation is progressing rapidly, yet digital literacy remains uneven across different demographic groups. For instance, elderly victims may lack awareness about how sophisticated AI technology can make fake calls appear genuine, making them prime targets for such scams. Traditional scams, such as fake brand promotions, phishing, and fraudulent online transactions, still dominate the landscape. These scams often exploit trust in familiar institutions, such as government agencies or e-commerce platforms. Their prevalence highlights gaps in public awareness and digital security practices, particularly among the elderly and youth. While these scams do not rely on AI, their continued success underscores the importance of education campaigns to raise awareness and build resilience against basic fraud tactics. The table also illustrates how scammers tailor their tactics to specific demographic vulnerabilities. The elderly, for example, are targeted with scams impersonating government or financial institutions, leveraging their perceived trust in authority. Meanwhile, youth and students are more likely to face recruitment scams and fraudulent apps that exploit their familiarity with digital tools but limited experience with cyber threats. The use of AI-driven Deepfake calls in both groups shows the versatility of AI in enabling scams to penetrate diverse segments of the population.

Scammers exploit the financial insecurity of low-income workers and the limited cybersecurity awareness in rural communities by leveraging AI tools like chatbots, personalized phishing emails, and AI-generated content to create false legitimacy. For low-income workers, schemes such as Ponzi scams and fraudulent investment platforms use fake reviews and user-generated content to promise quick financial gains. Similarly, rural communities, often reliant on mobile devices and lacking access to cybersecurity education, are targeted with AI-generated fake job offers and fraudulent online lending platforms tailored to their financial aspirations.

b. Organizational/Business targets

Small and medium-sized enterprises (SMEs), are also a major focus for scammers. SMEs are particularly vulnerable due to their limited cybersecurity resources and reliance on digital communications. AI-powered phishing attacks and Business Email Compromise (BEC) scams are among the most common tactics used. These involve highly personalized emails that mimic business partners or clients, often containing convincing details like invoice numbers or account specifics. Such scams deceive SME owners or employees into transferring funds or sharing sensitive information.

Another prevalent scam targeting SMEs involves fake invoices and fraudulent transactions. Scammers use AI to generate realistic fake invoices, exploiting SMEs' reliance on electronic payment systems. This can lead to significant financial losses for businesses operating on tight margins. In export-driven sectors like textiles and seafood, supply chain fraud is another major concern. Scammers use AI to impersonate suppliers or buyers, often creating fake websites or automating negotiations to deceive employees and disrupt business operations.

The private sector, particularly financial institutions and e-commerce platforms, faces mounting challenges in combating AI-powered fraud. Banks such as TPBank and Techcombank report a surge in cases where scammers use AI-driven deepfake technology and voice cloning to bypass biometric authentication systems. Fraudsters have manipulated eKYC (electronic Know Your Customer) verification processes, allowing them to create fraudulent bank accounts under stolen identities. The telecommunications sector has also noted an increase in AI-enhanced SMS phishing ("smishing") attacks, where scammers deploy fake base transceiver stations (BTS) to send fraudulent messages impersonating government agencies or financial institutions.

A notable case involved a Techcombank customer who lost 14.6 billion VND after scammers posed as law enforcement officers and used AI-generated voice calls to coerce the victim into transferring funds. Such incidents highlight the growing sophistication of AI-powered social engineering attacks, making traditional fraud detection methods obsolete. While some e-commerce platforms like TIKI.vn have not been directly exploited, they remain vigilant against the risk of brand impersonation by scammers who create fake online stores mimicking legitimate businesses.

Despite efforts to improve fraud detection through AI-driven transaction monitoring, Vietnam's financial institutions face a major challenge in coordinating responses to emerging scam threats. The lack of standardized fraud reporting mechanisms has hindered cross-industry collaboration, preventing real-time intelligence sharing between banks, telecom providers, and government authorities. Additionally, cross-border fraud remains a significant concern, as cybercriminals increasingly leverage international payment gateways and offshore accounts to launder stolen funds beyond Vietnam's jurisdiction.

Emerging Trends – AI-driven Scams

Several key trends highlight the increasing scale and impact of AI-driven scams, including widespread data leaks, AI-powered identity theft, deepfake impersonations, and automated scam operations. These trends pose severe risks to individuals, businesses, and national security, necessitating urgent regulatory and technological interventions.

a. AI-driven data leaks and personal information exploitation

One of the most alarming trends in online fraud in Vietnam is the escalation of personal data leaks, which serve as the foundation for increasingly sophisticated AI-driven scams. According to the National Cyber Security Center (NCSC) under the Ministry of Public Security (2024), cybercriminals primarily acquire personal information from underground marketplaces, where data is bought and sold via chatbots and paid for with cryptocurrency, making transactions difficult to trace. the number of individual accounts compromised in 2024 reached 121,482,341, marking a 15.8% increase compared to 2023 (104,917,940 accounts). The sectors most affected include:

- Public services - 5,271,054 compromised accounts
- Social networks - 5,905,760 accounts (Facebook: 4,947,312 and Twitter: 958,448)
- Banking and online payments - 1,161,713 accounts (PayPal: 750,414, Payoneer :70,863 and Visa: 34,811)
- Healthcare and education platforms – 335,314 accounts (education: 186,092 and the healthcare: 149,222)

The root causes of these data leaks are multifaceted. NCSC also indicates that 73.99% of users attribute leaks to providing information during online shopping, while 62.13% believe the cause stems from sharing data on social media. Additionally, 67% of users reported data leaks from essential services such as restaurants, hotels, and supermarkets, where information security measures are often weak. These breaches enable scammers to create highly personalized scams using AI-powered analytics, increasing the likelihood of victims falling for fraud attempts.

b. Escalation of AI-enhanced phishing and social engineering scams

With access to vast amounts of stolen personal data, cybercriminals are using AI to craft hyper-personalized phishing campaigns. Traditional phishing emails were often generic and riddled with grammatical errors, making them easier to detect. However, modern scams leverage AI-powered natural language processing (NLP) algorithms to generate flawless, contextually relevant phishing messages. These scams frequently mimic official communications from banks, government agencies, and e-commerce platforms, tricking victims into revealing sensitive information or making financial transfers. According to NCSC, an increasing 66.24% of users in Vietnam report that their personal information has been used illegally, demonstrating the effectiveness of AI-driven scams. Furthermore, 1 in every 220 smartphone users in Vietnam falls victim to fraud, with financial investment scams, impersonation fraud, and fake lottery winnings among the most prevalent. Alarmingly, despite the large number of victims, only 45.69% report scams to authorities, making law enforcement efforts even more challenging. According to the Vietnam Scam Report 2023:

- 70% of Vietnamese internet users encounter scam attempts at least once a month
- 49% reported an increase in scam attempts over the past 12 months
- Only 1% of victims successfully recovered their stolen money.

According to the Vietnam Scam Report 2023, AI-powered phishing attacks are becoming harder to detect due to their linguistic accuracy and personalized nature. Cybercriminals leverage AI-driven chatbots and automated email generators to create hyper-realistic messages that mimic banks, law enforcement agencies, or e-commerce platforms. These messages often include deepfake voice recordings or AI-generated images to further deceive victims. Among the most exploited communication platforms:

- Facebook and Gmail (71%) are the most frequently used by scammers
- Telegram (28%), Google (13%), and TikTok (13%) are also growing targets
- Phone calls and SMS remain the primary scam outreach channels.

c. Automated scam call networks and chatbot-assisted fraud

The use of AI-generated deepfakes and synthetic voices is reshaping impersonation scams in Vietnam. Fraudsters are now able to clone voices and faces of family members, government officials, or bank representatives, making phone scams almost indistinguishable from legitimate calls.

- 62.08% of Vietnamese users reported receiving scam calls impersonating police, tax agencies, and banks, urging them to install software or transfer money under false legal threats.

- 60.01% received fake prize notifications, often accompanied by AI-generated promotional videos.

These AI-powered deepfakes are being used to gain victims' trust quickly, persuading them to divulge sensitive information or approve unauthorized transactions. The nTrust system, an anti-fraud initiative, has recorded 134,000 reports of scam phone numbers in just six months, forcing authorities to continuously update a list of fraudulent numbers, which reached 296,000 in 2024.

AI-driven chatbots are also being deployed on social media and e-commerce platforms to engage victims in real-time. These bots can simulate human conversations, answer queries, and build trust, leading victims to share financial details or make fraudulent transactions. Given Vietnam's high social media penetration, these scams have been particularly effective in targeting younger demographics who frequently engage in online commerce.

d. Rise of AI-enhanced malware and ransomware attacks

The increasing reliance on digital platforms for work, finance, and social interactions has exposed Vietnamese users to sophisticated AI-enhanced malware attacks. According to a survey by the National Cyber Security Association:

- 23.4% of users reported being attacked by malware at least once a year.
- 9.65% suffered from ransomware attacks, leading to severe financial and data losses.
- 31.36% admitted to downloading software from unverified links, often disguised as “free” or “cracked” software.

These malware variants can steal login credentials, hijack financial accounts, or lock users out of their own devices. The risk is amplified by the widespread use of personal devices for both work and leisure, creating new vulnerabilities for corporate data breaches.

e. Financial losses and economic consequences of ai-powered fraud

The financial impact of online fraud in Vietnam has more than doubled in just one year. In 2023, online fraud caused losses of 8,000 billion VND, but by 2024, this figure surged to 18,900 billion VND, a 2.36x increase. The economic burden is not just limited to direct monetary losses; businesses also suffer from brand damage, loss of consumer trust, and the costs associated with fraud prevention. The banking sector, e-commerce platforms, and telecommunications companies bear the brunt of these attacks, often having to refund stolen funds or implement expensive security upgrades to protect their customers.

According to NCSC (2024), when falling victim to a scam, 88.98% of users stated that they immediately warned and discussed the incident with their relatives and friends. However, only 45.69% of respondents reported the case to the authorities, which remains relatively low.

Additionally, 70.72% of users reported receiving invitations to invest in financial exchanges of unknown origin, which promised no risks and high returns. Meanwhile, 62.08% encountered fraudulent calls impersonating various agencies and organizations (such as the police, court, tax authorities, and banks), coercing them into installing software or threatening them to transfer money as proof of innocence in alleged legal violations. Furthermore, 60.01% of respondents reported receiving notifications of winning prizes or being offered high-value promotions, but the information provided was often vague and suspicious.

One of the biggest challenges in combating AI-driven scams in Vietnam is the lack of effective reporting mechanisms and low public trust in law enforcement efforts. According to the Vietnam Scam Report 2023:

- 66% of scam victims did not report fraud incidents due to complicated reporting processes or lack of confidence in resolution.
- Only 23% reported scams to law enforcement, highlighting a significant enforcement gap.
- 29% of respondents expressed dissatisfaction with the government's response to online scams.

Many victims feel that law enforcement agencies are slow to act or lack the technical expertise to track AI-enhanced fraud operations. This highlights an urgent need to strengthen digital crime units, invest in AI-based fraud detection systems, and streamline scam reporting processes.

Socio-Economic Implications of Scams

Economic Impacts

Online scams in Vietnam have resulted in substantial economic losses, affecting individuals, businesses, and financial institutions. The rapid proliferation of generative AI has enabled fraudsters to execute sophisticated scams that are increasingly difficult to detect, leading to financial damages that cost Vietnamese citizens millions of dollars annually. E-commerce platforms, a critical driver of Vietnam's digital economy, have been heavily targeted by fraudulent activities such as fake online stores and counterfeit payment gateways, leading to declining consumer trust and reduced transaction volumes. Furthermore, financial institutions face increased operational costs associated with implementing fraud detection systems, managing customer disputes, and complying with regulatory requirements to combat cyber fraud. SMEs, which form the backbone of Vietnam’s economy, are particularly vulnerable to financial fraud due to their limited cybersecurity measures and lack of resources to recover from financial losses caused by scams. In addition, foreign investors are increasingly concerned about the potential risks associated with Vietnam's growing cybercrime landscape, potentially affecting the country’s attractiveness as a business destination.

Social Consequences

Beyond the economic ramifications, AI-driven online scams have significant social implications for Vietnamese society. A rising number of scam victims experience emotional and psychological distress, including anxiety, depression, and a loss of confidence in digital interactions. Scammers often exploit vulnerable populations such as elderly citizens and individuals with low digital literacy, leaving them feeling isolated and distrustful of technology. The proliferation of online scams also erodes public trust in digital platforms, slowing down Vietnam's digital transformation goals by discouraging users from engaging in e-commerce, online banking, and other digital services. Families of scam victims may experience strained relationships due to financial losses and social stigma associated with falling victim to fraud. In addition, the widespread fear of online fraud has led to a growing demand for government intervention and stricter regulations, increasing pressure on policymakers to implement robust cybersecurity measures while balancing economic growth and digital innovation.

Vulnerable Groups

Certain demographic groups in Vietnam are disproportionately affected by online scams, exacerbating existing social and economic inequalities. Elderly individuals, who may have limited experience with digital platforms, are particularly susceptible to AI-driven fraud schemes such as phishing emails, fraudulent investment opportunities, and impersonation scams. Similarly, rural populations with lower access to digital literacy programs are at high risk of falling victim to scams, as they often lack awareness of cyber threats and preventive measures. Additionally, low-income individuals who seek online financial opportunities or loans are frequently targeted by scammers offering fake job opportunities or financial assistance, further entrenching them in financial distress. The impact of these scams on vulnerable groups not only results in personal financial hardship but also deepens the digital divide, limiting the potential benefits of Vietnam's push toward a digital economy.

Challenges for law enforcement and cybersecurity

Vietnam's law enforcement agencies face significant challenges in tackling the growing threat of AI-driven online scams. The transnational nature of these crimes complicates efforts to track and apprehend perpetrators, who often operate from abroad and exploit jurisdictional loopholes. Local authorities are also hindered by a lack of advanced technological capabilities and specialized training in dealing with sophisticated AI-driven fraud tactics. While Vietnam has enacted the Cybersecurity Law to address cybercrime, the enforcement of these regulations remains challenging due to resource constraints and the rapid evolution of scam tactics. Additionally, the absence of comprehensive data-sharing mechanisms between financial institutions, telecommunications providers, and law enforcement agencies further hampers efforts to identify and mitigate fraudulent activities effectively.

Broader economic and technological implications

The persistent threat of online scams has broader implications for Vietnam's economic development and technological advancement. As the country aspires to become a regional hub for digital innovation and e-commerce, continued incidents of fraud pose a significant risk to Vietnam’s reputation in the global market. Businesses and investors may hesitate to expand their operations in Vietnam if they perceive the digital environment as unsafe or unregulated. Moreover, the growing sophistication of AI-driven scams presents a challenge for Vietnam's workforce, necessitating greater investment in cybersecurity skills development and digital literacy initiatives to equip citizens with the knowledge and tools to protect themselves against evolving threats. Without decisive action to curb online scams, Vietnam risks undermining public confidence in its digital economy, slowing down its progress toward Industry 4.0 and broader economic integration.

Stakeholder Roles

Several organizations, such as government, private sectors and CSOs play an important role in addressing the challenges derived from the scams. The table below shows some of the challenges and initiatives that have been taken in Vietnam.

Type of Institutions	Institutions/Organizations	Initiatives and Challenges
Government	The Ministry of Public Security (MPS)	Leads law enforcement efforts by investigating fraud cases, cracking down on cybercrime, and enhancing international cooperation
	The Ministry of Planning and Investment (MPI)	Strengthens business registration regulations to prevent fraudulent companies from operating
	Ministry of Finance (MOF)	Oversees financial markets, ensuring transparency and preventing fraudulent investment schemes
	The State Bank of Vietnam (SBV)	Regulates digital payments, preventing financial fraud, and coordinating with law enforcement to block suspicious transactions
	Ministry of Industry and Trade (MOIT)	Monitors e-commerce activities, cracking down on fake online stores and illegal multi-level marketing (MLM) schemes

	The Ministry of Information and Communications (MIC)	Enhances cybersecurity regulations, collaborates with tech companies to remove fraudulent content, and promotes digital literacy among consumers
	the Supreme People's Court and Supreme People's Procuracy	Ensure strict judicial enforcement, prosecuting offenders and securing asset recovery for victims
Private Sector	Banks and financial institutions	TPBank, for instance, has recorded cases where AI-driven fraudsters impersonated customer service representatives to manipulate victims into increasing their credit card limits or making unauthorized withdrawals Implemented biometric security measures, AI-powered fraud detection, and multi-factor authentication (MFA) to strengthen customer verification processes Integrated bio-authentication, NFC scanning for chip-embedded IDs, and transaction monitoring via Big Data analytics
	Telco	Increase in the use of fake base transceiver stations (BTS) by scammers, allowing them to impersonate mobile network operators and send fake messages urging victims to click on malicious links, which lead to the theft of personal data, OTP codes, and unauthorized access to banking accounts. Enhanced spam filtering systems, implemented real-time monitoring of network anomalies, and worked

		closely with law enforcement to detect fraudulent SIM card activations
	E-commerce platforms	Challenges in preventing online scams, including fake seller accounts, counterfeit product listings, and fraudulent transactions The industry requires a more coordinated approach, including regulatory support for AI-powered scam detection, stricter seller verification processes, and real-time scam reporting channels
Civil society organizations (CSOs)		Organized digital literacy campaigns, published scam alerts, and provided legal consultation services for scam victims. Researching AI-driven scams, identifying vulnerabilities in cybersecurity frameworks, and developing fraud detection technologies

Policy overview

National Policies

Vietnam has made significant strides in developing legal frameworks to address cybersecurity and online fraud; however, the current regulations fall short in tackling the emerging challenges posed by generative AI in online scams, including:

- **Law on Cyber Security (2018) and Decree 53/2022/ND-CP detailing a number of articles of the 2018 Cybersecurity Law**: Regulations on activities to protect national security and ensure social order and safety in cyberspace; responsibilities of relevant agencies, organizations, and individuals. It provides a legal framework for managing and protecting cyberspace, preventing cybercrime, including transnational online fraud.
- **Criminal Law (2015, amended in 2017):** Article 174 stipulates the crime of fraud and appropriation of property.

- **Law on Electronic Transactions (2005):** Protects consumer rights in the digital environment, including international transactions.
- **Law on Information Technology (2006):** applies to Vietnamese and foreign organizations and individuals engaged in information technology application and development activities in Vietnam
- **Law on Protection of Consumer Rights (2023):** provides for principles and policies for protecting consumers' rights; rights and obligations of consumers; traders' responsibility to consumers; consumer right protection activities by agencies and organizations; settlement of disputes between consumers and traders; state management of protection of consumers' rights.
- **The Directive No. 21/CT-TTg, issued on May 25, 2020:** underscores the Vietnamese government's commitment to strengthening the prevention and handling of fraudulent activities related to asset appropriation
- **Decree No. 13/2023/ND-CP on personal data protection, Decree No. 116/2013/ND-CP of October 4, 2013, detailing a number of articles of the Anti-Money Laundering Law and Decision No. 2345/QD-NHNN dated December 18, 2023 on application of safety and security measures to online payment and card payment**: Regulates to meet data protection requirements, the management, provision, and use of Internet services, including measures to prevent online fraud.
- **Decision 1811/QD-BTTTT dated 2024: Approves the "Plan to strengthen management and minimize abuse of domain names to violate the law", issued by the Minister of Information and Communications**: Implement comprehensive measures to prevent and address domain name abuse, particularly for international and cross-border domains, while raising public and business awareness about safe and reliable websites through the promotion of the national domain ".vn."
- Hotline of the Department of Cyber Security and High-Tech Crime Prevention: 069.219.4053 - Criminal Police Department;
- Address https://canhbao.ncsc.gov.vn./#!/ of the Vietnam Information Security Warning Page.

In response to the growing threat, the Vietnamese government has launched several initiatives to enhance cybersecurity capabilities, such as:

- **Established The National Cyber Security Center (NCSC):** responsible for monitoring and ensuring cybersecurity across Vietnam's cyberspace, serving as the central technical hub for cybersecurity supervision, support, and coordination. It oversees national cybersecurity by establishing monitoring networks, directing telecommunications and Internet service providers, collecting and analyzing cyber threats, and issuing early warnings. NCSC also facilitates information sharing between domestic and international organizations and manages national cybersecurity data systems to support regulatory enforcement and policy implementation.

- Citizens and businesses can report cybersecurity incidents or seek assistance through the **Hotline of the Department of Cyber Security and High-Tech Crime Prevention at 069.219.4053, managed by the Criminal Police Department**.
- Access real-time alerts and resources via the **Vietnam Information Security Warning Page at https://canhbao.ncsc.gov.vn**, which provides updates, guidance, and preventive measures to enhance cybersecurity awareness and response.

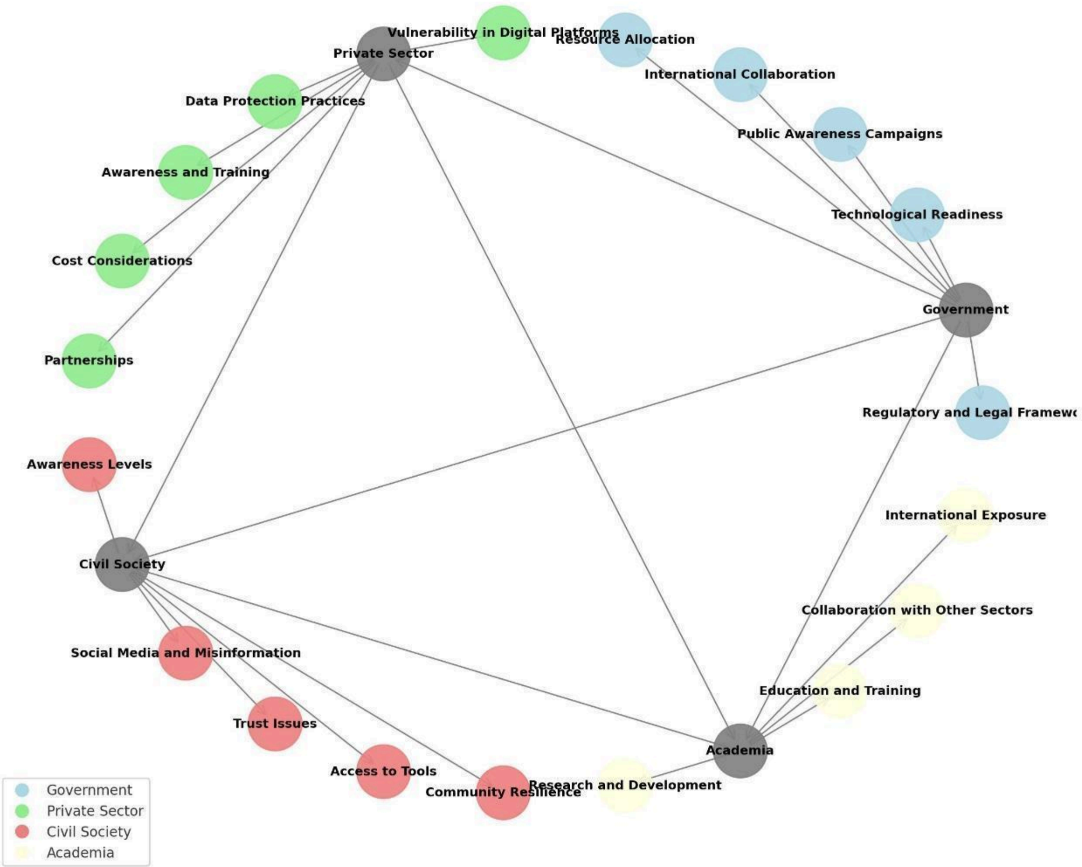
Vietnam has established a comprehensive legal framework to address cybersecurity and online fraud through various laws and regulations. These legal instruments provide a solid foundation for managing and protecting cyberspace, ensuring social order, and prosecuting cybercriminals, including those involved in transnational fraud. However, the current legal framework primarily focuses on traditional cyber threats and lacks specific provisions to tackle the emerging risks posed by generative AI technologies. Advanced threats such as AI-generated phishing, deepfake fraud, and automated identity theft remain unaddressed, leaving gaps in the regulatory landscape. As AI-driven scams become increasingly sophisticated, Vietnam's existing policies must evolve to include targeted measures that can effectively counter these challenges.

Despite the launch of several cybersecurity initiatives aimed at enhancing national cyber resilience, they fall short in addressing the unique risks associated with generative AI. Current initiatives focus on general cybersecurity threats but lack specific strategies for detecting and mitigating AI-powered fraud. There is an urgent need to incorporate AI-specific risk assessments and develop advanced detection systems capable of identifying AI-generated threats in real time. A proactive and forward-thinking approach is required, including AI-focused regulatory guidelines, robust oversight mechanisms, and collaboration with the private sector to build a resilient cybersecurity ecosystem. Without such targeted measures, Vietnam may struggle to effectively counter the growing wave of AI-enabled cyber fraud.

Moreover, Vietnam’s cybersecurity policies do not adequately address the cross-border nature of AI-driven fraud. Generative AI technologies transcend national boundaries, making it essential for Vietnam to strengthen its international cooperation efforts. Aligning domestic policies with global best practices and participating in international cybersecurity frameworks will be crucial to tackling AI-related cyber threats. Collaborative efforts with international cybersecurity organizations, regulatory harmonization, and the exchange of intelligence will enhance Vietnam's ability to combat transnational AI-driven fraud and bolster its cybersecurity capabilities on a global scale.

In Vietnam, the emergence of AI-driven online scams has become a growing concern, impacting individuals, businesses, and institutions. These scams leverage sophisticated AI technologies, making them harder to detect and combat. The complexity of this issue demands a multi-stakeholder approach involving the government, private sector, civil society, and academia. Each group plays a unique role in addressing the risks associated with AI-enabled scams. Governments must strengthen legal and regulatory frameworks while investing in advanced detection systems. The private sector, particularly industries like e-commerce and fintech, needs to enhance data protection and deploy robust cybersecurity measures. Civil society is a critical force in building awareness and resilience among citizens, while academia contributes through research, innovation, and workforce training.

Figure 1. Factors driving the interaction of AI-driven online scams in Vietnam



Source: author's compilation

Cross-border Measures

The rapid advancement of generative AI has significantly escalated the sophistication and scale of cross-border online scams targeting Vietnamese citizens and businesses. Fraudsters are increasingly leveraging AI-generated deepfake videos, voice cloning, and automated phishing techniques to deceive victims. These technologies enable cybercriminals to impersonate Vietnamese law enforcement officials, financial institutions, and even corporate executives with high accuracy. According to the survey, fraudsters are exploiting cryptocurrency transactions and anonymous payment channels, contributing to an estimated $37 billion stolen in Southeast Asia in 2023, with Vietnam accounting for a significant portion. One of the most alarming cases in recent years involved a Cambodia-based fraud ring that used deepfake technology to mimic Vietnamese police officers and tax officials, coercing victims into transferring funds under false pretenses. This operation defrauded over 13,000 individuals, causing financial losses estimated at 1,000 billion VND[2].

Vietnam's fight against AI-driven cross-border scams is particularly challenging due to the international nature of these criminal networks. Investigations have revealed that most large-scale scams affecting Vietnam are operated by companies headquartered in Cambodia, led by foreign nationals, and using offshore bank accounts to obscure their financial trails. Law enforcement efforts are further hindered by the fact that many of these scams operate outside Vietnam's jurisdiction, making it extremely difficult to arrest key perpetrators or recover stolen funds.

Despite Vietnam's engagement in regional cybersecurity initiatives, including cooperation with ASEAN and INTERPOL, gaps remain in enforcement capabilities. Existing legal frameworks in Southeast Asia are not fully harmonized, creating loopholes that cybercriminals exploit. The lack of standardized AI governance policies across ASEAN countries further complicates efforts to track and dismantle AI-driven fraud networks. Even when suspects are arrested, the use of offshore accounts and decentralized cryptocurrency transactions makes financial recovery nearly impossible.

Recognizing these threats, Vietnamese authorities have ramped up efforts to dismantle AI-enhanced fraud networks. A recent joint operation between multiple provincial police departments and national agencies successfully disrupted a Cambodia-based deepfake scam operation, leading to the arrest of 60 individuals. However, these enforcement actions remain reactive rather than preventive, highlighting the need for stronger intelligence-sharing mechanisms, AI-driven fraud detection systems, and cross-border policy alignment.

Policy Gaps in Effectively Addressing Scams

Despite Vietnam's ongoing efforts to strengthen cybersecurity and combat online scams, several critical gaps remain in addressing the growing threat posed by AI-driven fraud. These gaps span across regulatory frameworks, enforcement capabilities, inter-agency coordination, public awareness, and cross-border cooperation. The rapid evolution of generative AI has outpaced the country's current policies and detection mechanisms, making it increasingly difficult for authorities and private entities to effectively combat these sophisticated scams.

a. Narrow Coverage of the Existing Cyber Law

The emergence of deepfakes and AI-driven scams poses a significant challenge for governments in tackling these evolving threats. Although existing laws such as the Cybersecurity Law (2018) and the Personal Data Protection Decree (2023) provide a foundation for regulating online fraud, it does not yet encompass the complexities of AI-powered cyber

[2] https://vietnamnet.vn/triet-pha-duong-day-goi-dien-lua-dao-xuyen-bien-gioi-chiem-doat-1-000-ty-dong-2366553.html

threats. These laws are primarily designed to address conventional cybercrimes such as hacking and identity theft. Nevertheless, a cautious and measured approach is needed when dealing with AI-based threats. Introducing overly specific regulations may inadvertently hinder the ethical development of AI, which is an important tools in early fraud detection mechanism. As such, it would be more effective to first revisit and revise the current Cybersecurity Law (2018), expanding its scope to redefine fraud and scams, and explicitly include deepfakes within its provisions.

b. Enforcement limitations and technical capacity constraints

Even when online scams are identified, Vietnamese law enforcement agencies face significant challenges in investigating and dismantling these operations. A major obstacle is the limited technical expertise and insufficient resources available to combat AI-driven fraud effectively. Cybercriminals frequently operate from foreign jurisdictions, using encrypted communications, offshore accounts, and decentralized payment systems, making it nearly impossible for domestic agencies to track, identify, and arrest perpetrators.

The Ministry of Public Security (MPS), which oversees cybercrime investigations, often lacks the advanced AI-powered forensic tools needed to analyze deepfake content, detect AI-generated phishing attacks, or trace funds linked to fraudulent activities. Additionally, there is a shortage of trained personnel specializing in AI-related cybersecurity threats, which weakens Vietnam's ability to stay ahead of cybercriminal tactics. Compared to leading cybersecurity agencies in countries like Singapore or South Korea, Vietnam's law enforcement lacks real-time threat detection capabilities and AI-driven fraud monitoring systems, leaving them in a reactive position rather than proactively preventing scams.

c. Fragmented coordination among regulatory bodies

Vietnam's cybersecurity efforts are hampered by fragmented coordination between government agencies, financial institutions, and digital service providers. The Ministry of Information and Communications (MIC), the Ministry of Public Security (MPS), and the State Bank of Vietnam (SBV) all play roles in cybersecurity governance and fraud prevention, yet they operate under separate mandates without a unified approach. This lack of inter-agency collaboration results in delays in responding to scams, inefficient information sharing, and inconsistent enforcement actions.

For example, financial institutions and e-commerce platforms frequently detect fraudulent activities but struggle to coordinate with law enforcement agencies due to unclear reporting protocols. Many private sector entities lack direct communication channels with the government, forcing them to handle scams internally rather than escalating them for investigation. Additionally, there is no centralized AI fraud monitoring system where financial institutions, telecom companies, and government bodies can share real-time scam alerts and intelligence.

To effectively combat AI-driven scams, Vietnam needs to establish an integrated fraud response framework that facilitates information sharing between government agencies, financial institutions, e-commerce platforms, and telecom providers. This would allow for faster detection, improved collaboration, and more coordinated enforcement efforts.

d. Low public awareness and digital literacy

Another major gap in Vietnam's fight against AI-driven online scams is the lack of widespread public awareness and low levels of digital literacy, especially among vulnerable populations. Many Vietnamese citizens, particularly the elderly, rural communities, and small business owners, are unaware of how AI is being used in online fraud. Scammers frequently exploit low cybersecurity awareness, using AI-generated voice calls, fake government notifications, and deepfake videos to impersonate trusted authorities or financial institutions.

Although some public awareness campaigns have been launched by government agencies and financial institutions, they have not kept pace with the sophistication of AI-enhanced scams. Many victims remain unaware of how to verify digital identities, detect AI-generated fraud, or report scams to the appropriate authorities. A recent survey found that only 45.69% of scam victims reported their cases to law enforcement, demonstrating a lack of trust in the system and insufficient knowledge of reporting mechanisms.

To address this, Vietnam needs to implement nationwide digital literacy programs, particularly in rural areas and among high-risk groups. Public awareness campaigns should focus on educating users about AI-generated phishing, deepfake fraud, and common scam tactics, while financial institutions and telecom providers should integrate fraud prevention alerts into their customer communication strategies.

e. Challenges in Cross-border Collaboration

Vietnam's struggle with cross-border AI-driven scams is further exacerbated by inconsistent international cooperation and legal limitations in tracking cybercriminal networks operating beyond its borders. Many large-scale scams affecting Vietnam originate from Cambodia, China, and other Southeast Asian countries, where fraud syndicates operate call centers and AI-powered scam factories targeting Vietnamese citizens. These operations use foreign bank accounts, cryptocurrency transactions, and fake identities, making it nearly impossible for Vietnamese law enforcement to recover stolen funds.

While Vietnam has participated in ASEAN cybersecurity initiatives and collaborated with INTERPOL, these partnerships have not translated into effective cross-border enforcement mechanisms. Jurisdictional barriers, differences in legal frameworks, and the lack of formal extradition agreements make it difficult for Vietnamese authorities to prosecute foreign-based scammers. Additionally, regional law enforcement agencies lack AI-specific expertise, further limiting their ability to investigate AI-driven cybercrime effectively.

To improve cross-border enforcement, Vietnam should push for greater legal harmonization across ASEAN, advocate for bilateral agreements with key regional partners, and work with international cybersecurity organizations to establish a dedicated AI fraud intelligence-sharing network. Strengthening cross-border financial tracking mechanisms and enhancing collaboration with global tech companies would also help in identifying scam operators and shutting down fraudulent operations.

RECOMMENDATIONS

Policy recommendations

Areas of action by government

The Vietnamese government plays a central role in developing and enforcing policies to mitigate the risks posed by AI-driven scams. As AI fraud techniques continue to evolve, Vietnam's legal framework and enforcement capabilities must adapt swiftly to protect individuals and businesses from cybercrime. The government must focus on strengthening regulations, enhancing enforcement mechanisms, fostering regional cooperation, and increasing public awareness.

a. Strengthening legal and regulatory frameworks

Vietnam’s current cybersecurity and fraud prevention laws are outdated when it comes to addressing AI-driven scams. The Cybersecurity Law (2018), which governs Vietnam’s online security framework, does not explicitly cover AI-generated deepfake fraud, voice phishing scams, or synthetic identity fraud. Without precise legal definitions, law enforcement agencies face challenges in tracking and prosecuting cybercriminals who exploit AI tools.

To address this issue, the government must review the existing laws, and incorporate AI-powered scams into the legal definitions of fraud and scams. The Penal Code (2015, amended 2017) should be expanded to include harsh penalties for individuals and organizations using AI technologies for fraudulent activities. Additionally, mandatory reporting mechanisms should be enforced for financial institutions, telecom providers, and digital platforms, requiring them to report suspected AI-driven scams to law enforcement agencies in real time.

A National AI Governance Framework should be introduced, outlining ethical AI usage, responsible AI development, and enforcement measures against misuse. This framework should align with international AI security standards, such as the OECD AI Principles and the EU AI Act, ensuring that Vietnam's AI governance is in line with global best practices.

b. Institutional capacity building and enforcement enhancement

Law enforcement agencies, including the Ministry of Public Security (MPS) and the Cybersecurity and High-Tech Crime Prevention Department (A05), are currently ill-equipped to handle AI-driven scams due to a lack of specialized training and advanced forensic tools. The government must establish a specialized AI Fraud Detection Unit, equipped with cutting-edge AI forensic tools that can analyze fraudulent transactions, detect deepfake scams, and track AI-generated phishing campaigns.

To build expertise, comprehensive training programs must be implemented for law enforcement officers, prosecutors, and judges, focusing on AI-powered cybercrime investigation, digital forensics, and international cybersecurity standards. These efforts will enable authorities to track, investigate, and prosecute AI-enhanced fraud more effectively.

Additionally, the deployment of AI-powered surveillance systems is crucial for real-time fraud detection. Government agencies should partner with AI firms and cybersecurity organizations to integrate machine learning algorithms that can identify fraudulent activities across social media, financial transactions, and telecom networks.

c. Public awareness and consumer protection

AI-driven scams thrive on public ignorance and low digital literacy. Many victims fall prey to deepfake impersonation scams, AI-generated phishing emails, and fake investment schemes due to a lack of awareness.

To combat this, the government should launch a nationwide Digital Scam Awareness Program, targeting individuals, small businesses, and vulnerable groups such as elderly citizens and rural communities. This program should include mass media campaigns, online tutorials, and school-based cybersecurity education programs.

Government agencies should also collaborate with banks, telecom providers, and social media platforms to create fraud alerts and scam detection tools that warn users about AI-generated fraud attempts in real time.

d. Strengthening cross-border collaboration

Since many AI-driven scams in Vietnam originate from international cybercrime networks, Vietnam must prioritize cross-border cybersecurity collaboration. The lack of regional cooperation has allowed cybercriminals to exploit legal loopholes between ASEAN nations, making it difficult to track and prosecute foreign-based scam operators.

Vietnam should advocate for an ASEAN-wide AI Scam Prevention Task Force, which would facilitate real-time intelligence sharing, coordinated law enforcement operations, and policy harmonization among ASEAN countries. Vietnam should also expand its cooperation with INTERPOL, APEC, and global cybersecurity alliances, enabling faster extradition agreements and joint cybercrime investigations.

A critical challenge in tackling cross-border AI fraud is the use of offshore bank accounts and cryptocurrency transactions to launder stolen funds. The Vietnamese government must work with regional financial regulators to establish cross-border financial fraud monitoring mechanisms that detect suspicious transactions linked to AI-driven scams.

Areas of action by private sector

The private sector, including financial institutions, e-commerce platforms, telecommunications companies, and technology firms, is at the frontline of detecting and preventing AI-driven online scams. As fraudsters increasingly exploit generative AI for phishing, deepfake impersonation, and automated scams, businesses must strengthen fraud detection systems, data security, consumer awareness, and industry collaboration to mitigate risks.

a. Adoption of advanced fraud detection technologies

One of the most critical steps in combating AI-driven online scams is investing in advanced AI security solutions. Financial institutions and e-commerce platforms should integrate AI-driven fraud detection tools capable of identifying deepfake-assisted scams, synthetic identity fraud, and phishing attacks. Banks should enhance biometric authentication, voice recognition, and behavioral analytics to detect fraudulent transactions in real time. Additionally, telecommunications firms must deploy AI-based call and SMS filtering systems to block voice-cloned scam calls and smishing attacks before they reach users.

Another essential measure is implementing real-time monitoring and risk scoring systems. Banks like TPBank and Techcombank have already introduced risk-based authentication and transaction monitoring tools that assess customer behaviors to flag unusual activities. This approach should be expanded across industries to include e-commerce and fintech sectors. Companies should also adopt automated scam detection algorithms capable of identifying fraudulent activities across digital platforms, banking systems, and payment gateways to prevent scams before they occur.

b. Enhancing cross-industry and public-private collaboration

A major challenge in combating AI-driven scams is the lack of real-time fraud intelligence sharing among financial institutions, telecom providers, and digital platforms. To address this, the private sector should work toward developing a National AI-Driven Fraud Intelligence

Network, allowing businesses to share data on fraudulent accounts, suspicious transactions, and scam-related content. A private sector consortium focused on fraud prevention could facilitate this exchange and improve collective defense mechanisms.

In addition, stronger public-private partnerships on cybersecurity are essential. The Ministry of Public Security (MPS), State Bank of Vietnam (SBV), and Ministry of Information and Communications (MIC) should collaborate with private companies to develop a centralized fraud detection platform. AI security firms, financial institutions, and digital platforms should participate in government-led cybersecurity exercises to test fraud prevention measures and refine AI-based scam detection models.

c. Consumer awareness and support

Consumer education is key to preventing AI-driven scams. Banks, e-commerce platforms, and telecom providers should launch fraud awareness campaigns via SMS alerts, emails, and mobile app notifications, warning users about AI-generated scams.

Businesses should integrate AI-driven chatbots to assist customers in identifying fraudulent messages and transactions. Hosting online workshops and training sessions can further help users recognize deepfake impersonations and phishing attempts, especially targeting elderly individuals and rural communities, who are more vulnerable to scams.

To improve fraud reporting, companies must establish dedicated hotlines, online portals, and in-app reporting tools for users to quickly report suspicious activities, ensuring faster response and mitigation.

d. Strengthening user protection measures

To enhance security for users, financial institutions and e-commerce platforms must improve customer authentication and data security mechanisms. Banks should strengthen e-KYC (Electronic Know Your Customer) processes by integrating chip-embedded ID verification, biometric authentication, and AI-driven identity validation. Multi-factor authentication (MFA) should become mandatory for high-value transactions, particularly in cross-border payments, to reduce fraud risks. Additionally, e-commerce platforms should enforce stricter seller verification processes to prevent fraudulent listings and scams.

Alongside improved security measures, consumer education on AI-driven scams is crucial. Banks, e-commerce platforms, and telecom companies should organize nationwide digital literacy campaigns to help users recognize deepfake scams, phishing websites, and fraudulent job postings. Raising awareness about AI-generated fraudulent investment schemes and impersonation scams will empower consumers to identify potential risks and avoid falling victim to scams.

e. Addressing cross-border AI-driven fraud challenges

As AI-driven fraud often operates across national borders, stronger regional cybersecurity agreements are necessary to address these threats. Vietnamese financial institutions and telecom providers should support the development of regional AI-driven fraud monitoring systems in partnership with ASEAN countries. International cooperation between law enforcement, financial regulators, and technology firms is crucial to tracking and blocking cross-border scam transactions.

At the same time, AI regulation and policy compliance must be strengthened to ensure that fraud prevention measures align with data protection laws. Companies must actively engage in shaping AI governance regulations to ensure that fraud detection frameworks are both effective and compliant with privacy regulations. Banks, in particular, should follow Vietnam's Personal Data Protection Decree (Decree 13) while ensuring that AI-driven fraud detection tools are used transparently and responsibly.

f. Improving corporate incident response and crisis management

The private sector should also focus on establishing AI-powered scam incident response teams to detect and respond to AI-generated fraud cases swiftly. Financial institutions and digital platforms should have dedicated cybersecurity response units that can implement automated fraud alerts, emergency account freezes, and scam dispute resolution mechanisms. These teams would play a key role in minimizing financial losses and preventing further victimization.

Additionally, regular security audits and AI model testing must become a standard practice for private sector organizations. Banks, fintech firms, and e-commerce companies should conduct regular assessments of their AI-driven fraud detection models to ensure they remain effective. AI-based scam detection systems should undergo continuous testing against evolving fraud tactics to prevent fraudsters from adapting and circumventing security measures.

Areas of action by civil society and academia

As AI-driven scams continue to evolve in complexity, civil society organizations (CSOs) and academic institutions play a crucial role in shaping policies, raising awareness, and conducting research to mitigate the risks associated with these cyber threats. Their involvement ensures a balanced approach that complements government regulations and private sector initiatives by focusing on public education, victim support, policy advocacy, and cybersecurity research. By strengthening collaboration between policymakers, businesses, and communities, CSOs and academia can help Vietnam build resilience against AI-enabled fraud.

a. Promoting research and policy advocacy

Vietnamese universities and think tanks must prioritize research on AI-driven scams to assess their economic, technological, and social implications. Given the rapid advancements in generative AI, academic institutions should focus on understanding how AI is exploited for fraudulent activities, identifying vulnerabilities in cybersecurity policies, and developing predictive models to detect emerging fraud trends. Establishing AI and Cybersecurity Research Centers within universities can provide a dedicated platform for studying AI-related threats and collaborating with law enforcement agencies and financial institutions to strengthen fraud detection strategies.

In addition to research, academia should play a proactive role in policy advocacy by publishing policy briefs, white papers, and scam trend reports that offer data-driven insights for the government and private sector. These reports should highlight case studies of AI-driven scams in Vietnam, assess regulatory gaps, and propose concrete legal frameworks for tackling AI-enhanced fraud. Collaboration with international organizations such as ASEAN, APEC, and OECD would further enhance Vietnam's AI governance capabilities, allowing policymakers to align local regulations with global cybersecurity standards.

b. Expanding digital literacy and cybersecurity training

One of the most effective ways to reduce vulnerability to AI-driven scams is by improving digital literacy across all demographics. Many individuals, particularly elderly citizens, rural communities, and small business owners, fall victim to scams due to a lack of awareness about AI-enhanced fraud tactics. Universities, CSOs, and technology firms should collaborate to develop nationwide digital literacy programs that equip individuals with the knowledge to identify and prevent AI-generated phishing attacks, deepfake scams, and impersonation fraud.

Integrating cybersecurity education into school and university curricula is an essential step toward long-term prevention. Schools should introduce basic cybersecurity modules that teach students how AI-generated scams operate, how to protect personal data online, and how to recognize fraudulent digital content. At the university level, AI ethics and fraud detection courses should be incorporated into computer science, business, and law programs to train the next generation of cybersecurity professionals and policymakers.

In addition to formal education, community-based cybersecurity workshops should be conducted in local libraries, community centers, and workplaces to raise awareness among non-tech-savvy populations. These programs should focus on teaching individuals how to spot AI-generated scam emails, recognize voice phishing attempts, and use multi-factor authentication (MFA) to protect their financial assets. Civil society organizations should also collaborate with telecom providers, e-commerce platforms, and financial institutions to distribute educational materials on scam prevention through TV campaigns, social media, and SMS alerts.

c. Victim support services and public engagement

Victims of AI-driven scams often face financial ruin, psychological distress, and legal uncertainties in attempting to recover lost funds. Civil society organizations must establish dedicated victim support services that provide legal aid, psychological counseling, and financial recovery assistance. A national AI scam victim support hotline should be set up to allow individuals to report fraudulent activities, seek advice, and receive guidance on navigating the legal system.

Legal assistance programs should be expanded to help victims recover stolen funds, file legal complaints, and understand their rights under consumer protection laws. CSOs should partner with legal advocacy groups, cybersecurity law firms, and financial institutions to ensure that scam victims receive professional guidance on reclaiming lost assets. Additionally, psychological support services should be provided to help victims cope with stress, trauma, and social stigma associated with online fraud.

Public engagement is also critical in influencing consumer protection policies and pressuring financial institutions and tech companies to adopt more rigorous anti-fraud measures. Civil society organizations should organize public forums, online petitions, and advocacy campaigns that push for greater accountability from corporations and stronger legal protections for scam victims. Encouraging victims to share their stories through media platforms can help raise awareness about new scam tactics and prevent others from falling prey to similar fraud schemes.

d. Multi-stakeholder collaboration for cybercrime prevention

The fight against AI-driven scams requires coordinated efforts from government agencies, private companies, academic institutions, and civil society groups. Universities and CSOs should act as facilitators of dialogue between these stakeholders, ensuring that cybersecurity policies are informed by both research insights and real-world experiences.

Hosting national and regional cybersecurity summits would provide a platform for knowledge exchange, where experts from law enforcement, the financial sector, AI research, and consumer advocacy groups can discuss emerging fraud threats and best practices. Universities and research institutes should also lead multi-stakeholder working groups that develop policy recommendations for AI governance, scam prevention, and cross-border cybercrime collaboration.

Public-private partnerships should be strengthened to enhance fraud detection capabilities. CSOs and universities can collaborate with banks, telecom providers, and social media companies to establish real-time scam monitoring systems that share fraud intelligence across industries. Additionally, the creation of a National Cyber Threat Intelligence Hub would enable law enforcement agencies and private companies to exchange real-time fraud detection data, helping them respond quickly to new AI-driven scam techniques.

Universities should also establish AI Ethics and Cybersecurity Advisory Committees, which provide guidance on responsible AI development, ethical AI governance, and risk mitigation strategies. These committees can advise lawmakers, businesses, and consumer protection organizations on balancing technological innovation with fraud prevention.

e. Monitoring and evaluation of anti-scam efforts

CSOs and academic institutions should take the lead in assessing the effectiveness of government policies and private sector initiatives in combating AI-driven scams. Regular independent evaluations of cybersecurity policies should be conducted to identify gaps, assess enforcement challenges, and propose regulatory improvements.

Publishing annual scam reports is another important initiative that can help policymakers track financial losses, emerging fraud techniques, and evolving scam tactics. These reports should include detailed case studies, statistical analyses, and policy recommendations, guiding future cybersecurity strategies and public awareness campaigns.

Furthermore, civil society organizations should facilitate community feedback mechanisms such as online surveys, town hall meetings, and consumer complaint hotlines to understand how individuals and businesses experience AI-driven fraud. This data should be used to inform government responses, refine cybersecurity education programs, and advocate for stronger consumer protections.

ANNEXES

List of consulted stakeholders

A detailed list of organizations and experts consulted during the research process to provide transparency and credibility.

Government Agencies:

+ Ministry of Planning and Investment (MPI)

+ Ministry of Industry and Trade (MOIT)

Private Sector:

- Tiki.vn - a top retail e-commerce platform in Vietnam
- Vietnam Technological and Commercial Joint Stock Bank (Techcombank)
- Lien Viet Post Bank (LPBank)
- Tien Phong Commercial Joint Stock Bank (TPBank)
- Viettel Telecom - the largest telecommunications company in Vietnam

Academia and Civil Society:

- Greenfield - an Inter-Level Private School
- Central Institute for Economic Management – CIEM
- National Institute for Finance – NIF
- Viet Nam Institute of Industrial and Trade Policy and Strategy - VIOIT

References and citations

Vietnam Ministry of Information and Communications. (2022). *Cybersecurity Report 2022.*

National Cyber Security Center (NCSC). (2023). *Cybersecurity report 2023*

ASEAN. (2021). *ASEAN Digital Economy Framework Agreement.*

World Economic Forum. (2023). *Global Cybersecurity Outlook 2023.*

Global Anti-Scam Alliance (GASA) and Chongluadao.vn. (2023). *The State of Scams In Vietnam. 2023.* Available at: https://thesaigontimes.vn/wp-content/uploads/2024/01/State-of-Scam-Report-2023-Vietnam.pdf

GASA and Gogolook (2023). *Asia Scam report 2023.* Available at : https://hpt.vn/Uploads/File/2023/Bao-cao-lua-dao-Chau-A-2023.pdf

Website: Anti-Scams: https://chongluadao.vn/thong-ke?type=blacklist

Safer Internet Lab

saferinternetlab.org

Jl. Tanah Abang III no 23-27
Gambir, Jakarta Pusat. 10160

Find Us On

CSIS Indonesia | Safer Internet Lab