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 SCAM IN VIETNAM

A Research Report by Safer Internet Lab

The views expressed here are solely those of the author(s) and do not represent an official position of SAIL, CSIS, Google, or any other organization. Please contact the author(s) directly with any comments or questions.

Online Fraud and Scams in Vietnam

Nong Phuong Thao[24]

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 report 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 improvement. The scope of the policy assessment encompasses both domestic and cross-border aspects of online scams, recognizing that the problem is not confined within national borders. 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. Furthermore, 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.

[24] Researcher, Central Institute for Economic Management (CEM)

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 (see Annex A). 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.

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 online platforms 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 (see Annex B). The common goal remains to gain trust, steal personal information, and ultimately misappropriate assets.

AI-driven scams, such as those involving Deepfake video calls, demonstrate how malicious actors leverage advanced technologies to enhance the believability of their schemes. In Vietnam, where digital transformation is progressing rapidly, yet digital literacy remains uneven across demographic groups, the elderly are particularly vulnerable, as they often lack awareness of how AI technologies can make fraudulent calls appear convincingly authentic.

Meanwhile 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 addition, financial institutions, telco industry, 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. 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. 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.

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 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 table below shows some of the sectors with most affected accounts:

Table 11.1 Number of Affected Accounts Based on Sectors

Sectors	Number of affected accounts
Public services	5,271,054
Social media	5,905,760
Banking and digital payment	1,161,713
Healthcare and education	335,314

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 due to 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 (70% of Vietnamese encounter scam attempts at least once a month), only 45.69% report scams to authorities, making law enforcement efforts even more challenging. In addition, the fact that only 1% of victims have successfully recovered their stolen money shows the urgent need for stronger frameworks to address scams.

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. Although phone calls and SMS remain the primary scam outreach channels, social media platform and email are also growing targets.

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. For instance, 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. While 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 Trust 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 and 9.65% suffered financial and data losses. 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.

Socio-Economic Implications of Scams

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. 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.

Economic impacts

Online scams in Vietnam have resulted in substantial economic losses, affecting individuals, businesses, and financial institutions. 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 2.36 times 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. 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.

STRATEGY IN ADDRESSING ONLINE FRAUD AND SCAMS

The Role of Stakeholders in Addressing Online Fraud and Scams

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 has been taken in Vietnam.

Table 11.2 Initiatives From Key Institutions to Address Scams

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	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	Enhanced spam filtering systems, implemented real-time monitoring of network anomalies, and worked closely with law enforcement to detect fraudulent SIM card activations.
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:

Table 11.3 Vietnam National Policies to Address Scams

Type of policies	Name of Regulations/Initiatives	Description
Regulations	Law on Cyber Security (2018) and Decree 53/2022/ND-CP	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)	Engagement in information technology application and development activities in Vietnam

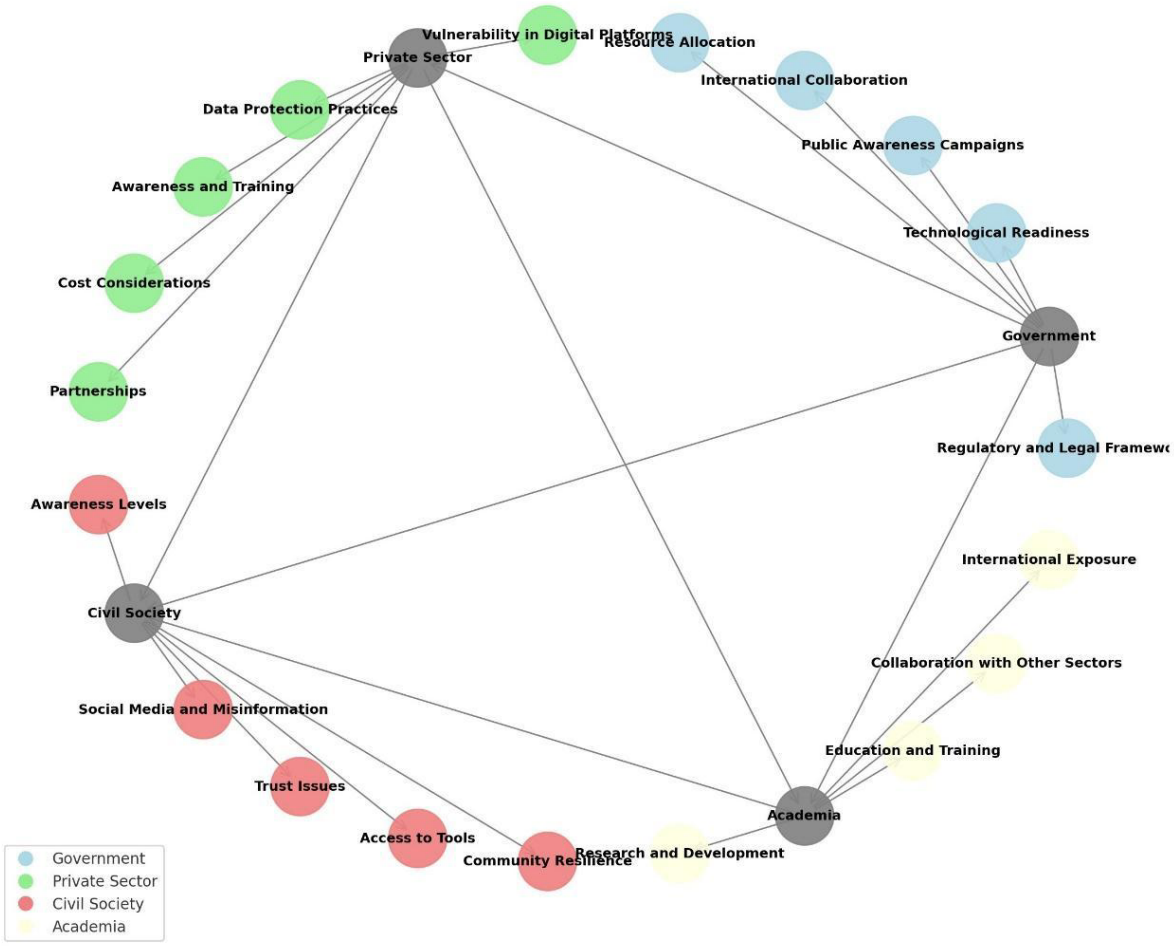
	Law on Protection of Consumer Rights (2023)	principles and policies for protecting consumers' rights
	The Directive No. 21/CT-TTg (2020)	government's commitment to strengthening the prevention and handling of fraudulent activities related to asset appropriation
	• Decree No. 13/2023/ND-CP on personal data protection. • Decree No. 116/2013/ND-CP on Anti-Money Laundering. • Decision No. 2345/QD-NHNN on 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 on the plan strengthen management and minimize abuse of domain names to violate the law	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."
Initiatives	The National Cyber Security Center (NCSC)	Responsible for monitoring and ensuring cybersecurity across Vietnam's cyberspace, directing telecommunications and Internet service providers, collecting and analyzing cyber threats, and issuing early warnings, and facilitates information sharing between domestic and international organizations to support regulatory enforcement.
	Hotline of the Department of Cyber Security and High-Tech Crime Prevention at 069.219.4053	Hotline for citizens and businesses can report cybersecurity incidents or seek assistance, managed by the Criminal Police Department
	Vietnam Information Security Warning Page at https://canhbao.ncsc.gov.vn	Access real-time alerts and resources 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. 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. In addition, the complexity of this issue demands a multi-stakeholder approach involving the government, private sector, civil society, and academia.

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.

Figure 11.1 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. 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 (Vietnamnet, 2025).

Vietnam's fight against AI-driven cross-border scams is particularly challenging due to the international nature of these criminal networks. 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. Investigations have revealed that most large-scale scams affecting Vietnam are operated in Cambodia, led by foreign nationals, and using offshore bank accounts to obscure their financial trails.

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.

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 threats. These laws are primarily designed to address conventional cybercrimes such as hacking and identity theft. Thus, revisit and revise the current Cybersecurity Law (2018), expanding its scope to redefine fraud and scams, and explicitly include deepfakes within its provisions is needed to address fraud and AI-driven scams.

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.

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. 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.

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.

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.

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.

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 reviews the existing laws, and incorporating 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.

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 in the need for advancing capacity in AI-driven scams including strengthen specialized training and advanced forensic tools. The government is recommended to 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.

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.

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.

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.

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.

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.

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.

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.

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. CSOs should play a more role in (i) promoting research in understanding the AI for fraudulent activities, (ii) collaborating with other stakeholders in developing digital literacy and cybersecurity programs for all groups, (iii) creating support services platforms for scam's victim, (iv) forming multistakeholder dialogue to bridge the research and policies, and (v) monitoring and evaluating anti-scams efforts.

ANNEXES

Annex A. 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 brand name 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

Annex B. Target Groups and 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

REFERENCES

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

Chongluadao. (2025). *Available at:* https://chongluadao.vn/thong-ke?type=blacklist

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

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

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

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

Vietnamnet. (2025). Dismantling a cross border scam phone call ring, appropriating nearly 1000 billion VND. Available at: https://vietnamnet.vn/triet-pha-duong-day-goi-dien-lua-dao-xuyen-bien-gioi-chiem-doat-1-000-ty-dong-2366553.html

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

Safer Internet Lab

saferinternetlab.org

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

Find Us On

CSIS Indonesia | Safer Internet Lab