IRIS
Information Resilience
& Integrity Symposium

RESEARCH PAPER

Regulatory and Institutional Responses to Online Scams in the Generative AI Era: Insights from Multi-Stakeholder Perspectives in Vietnam

PANEL 1 | Deepfakes for Financial Fraud

Safer Internet Lab
Led by CSIS in partnership with Google

Centre for Strategic and International Studies

Google

Universitas Gadjah Mada
Fakultas Ilmu Sosial dan Ilmu Politik

Center for Digital Society

Thao P. Nong

Thao P. Nong is a researcher at the Institute for Policy and Strategic Studies, under the Centrer Commission for Policy and Strategy, Vietnam. She holds a Master's degree from the University of Leicester, UK, and has extensive experience in digital economy policy, international trade, and the development of new economic models. Her recent research focuses on regulatory and institutional responses to emerging challenges in the digital era, particularly those associated with generative AI and online fraud.

Tran Luu Ly

Tran Luu Ly is currently pursuing a doctoral degree at the University of Languages and International Studies (ULIS), Vietnam National University (VNU). As a dedicated university lecturer specializing in interpreting and translation at both ULIS and Thuyloi University, Tran combines academic expertise with a practical understanding of business management. Holding a Master of TESOL from Victoria University and an MBA from Vietnam Japan University, Tran's educational background is further enhanced by prestigious scholarships from the Japanese Government and JICA, as well as a full scholarship from the Southeast Asian Ministers of Education Organization. With a passion for both language education and management, Tran is committed to advancing research and contributing to the development of these fields.

This paper is circulated for discussion and feedback. The views expressed are solely those of the author(s) and do not represent an official position of SAIL, CSIS, Google, CfDS, Faculty of Social and Political Sciences UGM or any other organization. The author(s) welcome comments on this version and invite you to contact them directly with any feedback or questions.

Regulatory and Institutional Responses to Online Scams in the Generative AI Era: Insights from Multi-Stakeholder Perspectives in Vietnam

Thao P. Nong, Tran Luu Ly

The rapid advancement of generative artificial intelligence (GAI) has introduced both opportunities and challenges for digital ecosystems, particularly in the realm of online fraud. In Vietnam, where digital transformation is accelerating, online scams have grown in scale and sophistication, increasingly leveraging synthetic content and impersonation techniques enabled by GAI. This study examines how regulatory institutions, private sector entities, and civil society organizations in Vietnam are responding to the evolving threat of AI-enabled scams. Drawing on semi-structured interviews and survey data collected from 11 organizations across government, industry, and academia, the research explores institutional awareness, response capabilities, and perceived gaps in the legal framework. Findings reveal that while stakeholders recognize the risks posed by GAI, current regulatory responses remain fragmented, reactive, and limited by unclear legal definitions and weak inter-agency coordination. Private sector actors highlight the lack of secure mechanisms for information-sharing, while civil society representatives emphasize underreporting, limited victim support, and uneven digital literacy. The paper argues for a more adaptive and integrated governance mode, combining regulatory reform, cross-sectoral collaboration, and technical capacity-building, to effectively safeguard Vietnam's digital landscape in the GAI era.

Keywords: generative artificial intelligence, online scams, stakeholder insights, cybersecurity, regulatory frameworks, institutional responses, Vietnam.

Introduction

The emergence of GAI has reshaped digital interactions, bringing new opportunities for communication, commerce, and service provision. At the same time, it has enabled more complex and difficult-to-detect forms of online fraud. These developments pose pressing challenges for policymakers and institutions, particularly in countries like Vietnam, where digital transformation is occurring rapidly. In this context, it is crucial to examine how existing regulatory and institutional frameworks are responding to scams that leverage GAI technologies.

This study forms part of a broader policy and stakeholder review, combining literature analysis with empirical findings. It aims to provide a nuanced overview of how Vietnam is addressing the risks posed by AI-driven fraud. Special attention is given to the financial services sector, where the potential of GAI has already led to increased adoption of measures such as stronger authentication systems, ongoing risk monitoring, and greater information exchange across institutions (Nikhil, 2025). The study highlights governance approaches that are adaptive, cooperative, and sensitive to local contexts.

GAI describes systems capable of producing synthetic content, including text, images, audio, and video, based on patterns learned from large datasets. Unlike earlier AI tools, which were limited to classification or prediction tasks, GAI creates original outputs that can be misused for malicious purposes. In online scams, this includes impersonation using manipulated media or highly tailored phishing messages. The flexibility of these tools means they can be used both to detect fraud and to perpetrate it (Bociga & Nicholas, 2025). For Vietnam, where online commerce, mobile payments, and social networking are expanding rapidly, such risks require action from a range of actors: regulators, technology developers, financial institutions, and the public.

The central question guiding this research is: What regulatory approaches, institutional arrangements, and collaborative strategies are most effective in tackling GAI-enabled online scams in Vietnam? While there is growing international literature on AI regulation and cybercrime prevention, few studies address the specific conditions of Vietnam, including its institutional capacities, legal frameworks, and public awareness. Bridging this gap calls for a detailed understanding of stakeholder roles, policy coordination mechanisms, and the socio-economic context (Iga et al., 2024).

This study considers how GAI-related threats intersect with Vietnam's ongoing regulatory reforms and brings together insights from multiple stakeholders. The study also evaluates current policy tools, such as laws on data protection, cybersecurity, and electronic transactions, and examines whether they remain fit for purpose as scams grow more technologically complex. Emphasis is placed on the need for flexible, cross-sector governance models that can incorporate international experience while remaining responsive to Vietnam's specific regulatory environment (Bikash, 2025).

A key contribution of this study is its attention to the differing perspectives of stakeholders: from law enforcement agencies seeking investigative support, to fintech firms prioritizing system resilience, and citizens concerned about personal data and trust. By identifying these dynamics, the paper outlines a layered regulatory approach that balances innovation with safeguards for rights and transparency.

Ultimately, this research aims to inform the development of a more responsive and coordinated policy environment, one capable of meeting the challenges posed by GAI-enabled scams in Vietnam. Through the integration of policy analysis and field-based insights, it seeks to support efforts to protect the integrity of the digital economy in a time of rapidly changing threats.

Literature Review

The emergence and rapid proliferation of GAI technologies are reshaping digital ecosystems by transforming how content is created, distributed, and consumed globally (Araz, 2025). These technologies enable the automatic generation of hyper-realistic media, including text, audio, and visuals, thereby heightening the risk of misinformation and deceptive practices (Jaidka et al., 2024); (Ng & Taeihagh, 2021). The personalized and autonomous nature of GAI-powered tools also facilitates the scalable production and dissemination of malicious content, increasing the sophistication of digital fraud and potentially weakening public trust and social cohesion. Tackling these threats requires more than technical interventions; it demands collaborative governance and cross-sectoral engagement to strengthen societal resilience against digital manipulation.

Traditional online fraud research has shown that many scams rely less on technological breaches and more on manipulating human psychology. Fraudsters often exploit trust through interaction, rather than through hacking systems. As Rusch (1999) observed, even in secure digital environments, users must remain cautious when dealing with unknown entities. Historically, scam tactics involved static rule-based scripts, spam campaigns, and website replication. In Vietnam, growing digital literacy has improved public awareness of online scams, but knowledge remains uneven. A recent survey of 205 Vietnamese internet users found that while educational campaigns were not broadly recognized, users demonstrated above-average ability to detect fraud, especially those with prior victimization experience or technical occupations (Kha et al., 2024).

The evolution of GAI marks a turning point in cybercrime strategies. Contemporary fraud methods increasingly involve impersonation, AI-generated synthetic content, and deepfake technology. These tools allow scammers to convincingly mimic voices, faces, and text styles, thereby complicating the distinction between legitimate and fabricated communication (Nguyen et al., 2024). George (2023) warns that deepfakes are now being deployed to influence political discourse, defame individuals, and commit large-scale fraud. While imperfections in these synthetic media, such as visual glitches or unnatural movement, remain detectable, technological advancements are narrowing this window of detectability.

In the Southeast Asian context, and particularly in Vietnam, research has begun to capture how GAI intersects with pre-existing digital vulnerabilities. According to the 2023 Vietnam Scam Report by the Global Anti-Scam Alliance (GASA) and Chongluadao.vn, over 70% of users experience scam attempts monthly, yet only 1% successfully recover losses, highlighting a systemic weakness in response and remediation mechanisms. The National Cyber Security Center (NCSC, 2024) identifies key barriers, including inefficient reporting channels and public skepticism toward law enforcement. Specifically, 66% of scam victims chose not to report incidents, citing either cumbersome procedures or a lack of trust in resolution mechanisms. Of those who did report, only 23% reached out to authorities, and 29% expressed dissatisfaction with official responses. This suggests that law enforcement agencies often lack the agility and expertise required to counter AI-enabled fraud effectively.

On the regulatory front, Vietnam has laid groundwork with laws governing cybersecurity, digital transactions, and consumer protection. Instruments such as the Cybersecurity Law (2018), Criminal Code (2017), Law on Electronic Transactions (2023), and Law on Consumer Protection (2023) are gradually being supplemented by newer policies focused on data governance and digital technology. However, these frameworks do not yet comprehensively address the challenges posed by GAI. While the ongoing Data Law (2024) and Law on Digital Technology Industry propose ethical principles and risk-classification schemes for AI applications, they lack enforceable mechanisms and clear definitions for key terms like “serious harm” or “trustworthy AI”. No binding rules are attached to violations, and there is limited oversight or accountability for high-risk use cases. Similarly, while mandatory labeling of AI-generated content is a promising step, it remains unclear how enforcement will be ensured across platforms, especially in cross-border digital environments.

Vietnam’s national strategy for AI development, articulated in Decision No. 127/QD-TTg (2021) and further elaborated in Decision No. 1290/QD-BKHCN (2024), envisions AI as a cornerstone of economic modernization. However, these strategic documents largely focus on innovation and capacity building, with insufficient attention to risk mitigation or misuse prevention. The 2024 technical guidance (Document No. 2619/BTTTT-CĐSQG) for evaluating large language models offers recommendations but remains voluntary and lacks any binding regulatory power. There is currently no dedicated agency responsible for certifying or monitoring AI systems after deployment, nor is there a national standard for assessing the impact of AI-generated content. Vietnam’s approach to incorporating AI governance into existing legal frameworks, while adaptive, risks overlooking the unique threats posed by generative systems and diluting institutional accountability.

These legal and institutional gaps form the foundation of this study’s inquiry. As Vietnam advances its digital economy, it must simultaneously confront the new challenges introduced by GAI–powered fraud. This research contributes to the literature by integrating perspectives from multiple stakeholder groups to explore how regulatory, institutional, and societal actors are responding to these evolving risks.

Moving forward, effective governance of GAI in Vietnam will require a multifaceted strategy that aligns regulatory reform with technological oversight and civic trust-building. Lessons from broader digital governance literature stress the importance of agile legal instruments, coordinated multi-stakeholder action, and investment in resilient infrastructure (Tuan, 2025). Applying these insights to the generative AI era will be critical for Vietnam to not only safeguard its citizens but also to lead in ethical AI governance in the region

Methods

Design

The study adopts a purposeful sampling strategy to identify and engage a cross-section of Vietnamese stakeholders with direct exposure to or responsibility for addressing online scams. A total of 11 organizations across three categories participated in the study: (1) government ministries and agencies, (2) private sector entities in finance, telecom, and e-commerce, and (3) civil society and academic institutions. Interviews were tailored to each group, covering topics such as AI applications in scams, response mechanisms, and policy gaps. Interviews were conducted in person or online via zoom.

Data collection was conducted through semi-structured interviews and secure online survey forms between January and February 2025. Questionnaires were customized for three main stakeholder groups: government agencies, private sector entities, and academic institutions, to reflect their operational roles, exposure to online scams, and areas of expertise. This design allowed for targeted insights while ensuring comparability across sectors.

Each questionnaire covered six thematic areas. Respondents were asked about the current landscape of online scams, common types of fraudulent activity, and the frequency of incidents. The private sector was also invited to share whether their platforms or services had been misused for fraudulent purposes. Participants discussed the cross-border nature of scams and the responsibilities of different institutions, including how coordination occurs across sectors and jurisdictions. They also assessed both financial and reputational consequences, as well as broader impacts on public trust and institutional resilience.

Further questions focused on how organizations are responding to these challenges, including the tools, strategies, and procedures they have adopted. Government and business representatives described internal monitoring practices and how effectiveness is measured, while all stakeholders identified legal and policy gaps that hinder enforcement or protection.

The final section of the questionnaire gathered perspectives on potential reforms and collaborative approaches to strengthen the institutional response to online scams in the digital age.

Participants Recruitment

To ensure the credibility and relevance of the study, participants were purposefully selected based on their institutional roles, practical experience, and involvement in addressing issues related to online scams and the digital regulatory landscape in Vietnam. The selection process aimed to capture diverse and informed perspectives from three key stakeholder groups: government agencies, the private sector, and academia/civil society. All interviewees held mid- to senior-level positions and were actively engaged in regulatory, operational, or research work concerning digital governance, e-commerce oversight, financial services, or consumer protection. A detailed overview of participating institutions is provided below.

Table 3. General description of interviewees

Groups	Number of interviewees	Background
Government agencies	02	01 Deputy Head and 01 Senior officer from Ministries. These individuals have played key roles in shaping and executing national strategies on digital economy governance, e-commerce regulation, and consumer protection in response to emerging online scam challenges.
Private sector	05	01 Senior Director, 01 Senior Manager, 01 Team Leader, 01 Senior Specialist, 01 Senior engineer from banks, telecommunication and ecommerce

		firm. Interviewees offered diverse insights into institutional and technical responses to online scams, including infrastructure-level controls, seller verification, transaction monitoring, user protection, and fraud risk management within financial, telecommunications, and e-commerce platforms.
Academia and civil society	04	02 Deputy Head, 01 Researcher from Institutes and 01 lecturer from university. Interviewees from state research institutes and academic organizations actively engaged in policy analysis, regulatory research, and public education. They provided insights into institutional responses to online scams, digital literacy efforts, and regulatory challenges arising from rapid technological developments in the generative AI era.

Results

Government Ministries and Agencies

Representatives expressed a shared concern over the growing complexity of online scams in Vietnam. Both institutions acknowledged that fraudulent activities are becoming increasingly difficult to detect, particularly due to the emergence of new forms of impersonation that appear highly realistic. Cases involving fake phone calls or video messages impersonating government officials have become more common, and are often convincing enough to coerce victims into transferring money or revealing personal information. Officials cited several incidents where individuals were deceived into complying with fabricated legal threats, suggesting that the psychological tactics employed by scammers have evolved to become more targeted and persuasive.

Despite this awareness, ministry representatives also pointed to a number of institutional shortcomings. At present, there is no legal framework specifically designed to address new forms of deception that rely on manipulated media. While existing laws penalize fraud and unauthorized access to digital networks, they do not clearly define or prohibit the use of altered images, voices, or videos for the purpose of impersonation. This has made it difficult for authorities to pursue charges in cases where the deception does not fall neatly into the categories currently outlined in the criminal code.

Officials also emphasized the fragmented nature of the national response. Each ministry or enforcement body tends to act within its own jurisdiction, with little coordination between agencies. There is no central database that tracks scam cases, no standardized process for reporting or sharing information, and no regular mechanism for joint investigations. While warnings are occasionally issued in response to large-scale incidents, there is no long-term strategy or unified campaign to educate the public or prepare frontline institutions for these threats.

One issue repeatedly highlighted was the limited capacity for technical analysis. Investigation teams often lack the necessary tools to detect whether a digital message, image, or voice recording has been altered. Training on how to assess these new forms of deception remains inadequate, and current practices still rely heavily on manual inspection or citizen reports. This technological gap significantly slows down the response to new scams and limits the ability to gather evidence that would stand in court.

On the question of legal reform, they advocated for a cautious, yet proactive approach. Rather than drafting a completely new law dedicated to artificial intelligence or emerging technologies, officials recommended strengthening existing legal instruments, such as the Law on Cybersecurity and the Law on Information Technology, by incorporating new definitions and penalties relevant to today's threats. This horizontal integration, they argued, would help avoid legal overlap and reduce the risk of discouraging private-sector innovation.

At the same time, both institutions acknowledged that more ambitious reforms may be needed in the near future. For example, one proposed the creation of a controlled testing environment where enforcement agencies could simulate scam scenarios and trial new forms of detection. Such a lab could also support collaboration with banks, telecom providers, and other critical infrastructure sectors. The long-term goal, as described by officials, is to develop a more agile and integrated response system that combines legal clarity, technical capacity, and inter-agency coordination.

Private Sector Entities in Finance, Telecom, and E-Commerce

Interviews with representatives from major financial institutions, telecom operators, and e-commerce platforms revealed a shared recognition of the growing threat posed by online scams that increasingly exploit advanced digital tools. Many noted a marked shift from conventional fraud methods toward more deceptive schemes that mimic official communications, falsify identities, or exploit trust in public institutions. For example, one financial institution reported that fraudsters had successfully forged digital identities during remote account verification procedures, resulting in unauthorized access and substantial financial losses for affected customers.

Despite these risks, most companies acknowledged that their current fraud prevention measures remain largely reactive. Some have implemented enhanced identity verification protocols and transaction monitoring systems, but these are often deployed in response to incidents rather than as part of a comprehensive strategy. A few banks have adopted more proactive tools to flag suspicious behavior patterns or abnormal transaction activity, yet these efforts are limited by concerns over compliance with data protection laws, which restrict the types of customer data that can be stored, analyzed, or shared internally.

Companies also highlighted the challenges of maintaining security standards in a fast-evolving digital environment. One telecom provider described frequent attempts to exploit weaknesses in messaging systems, such as impersonating SMS messages from financial institutions using spoofed signals. E-commerce platforms, while less directly targeted by scams, noted that their systems are routinely probed for vulnerabilities. Across the sector, there was a consensus that while threat awareness is growing, the capacity to anticipate and prevent these schemes remains uneven.

In terms of regulation, private firms expressed frustration with the lack of specific legal guidance regarding new forms of digital deception. Many felt that the current legal framework does not adequately distinguish between fraud carried out using conventional methods and those made possible through modern synthetic content or automated scripts. This ambiguity has left companies uncertain about their responsibilities and the limits of acceptable intervention, especially when customer privacy, cybersecurity regulations, and service quality standards intersect.

A recurring concern was the absence of formal mechanisms for collaboration and information exchange. Firms described a siloed landscape where incidents of fraud are handled internally and often not reported unless absolutely necessary. The reluctance to disclose scam-related data stems from fears of reputational damage and the lack of a protected, standardized channel through which such information could be shared with regulators or peers. Several respondents suggested that the development of a shared fraud monitoring platform, where patterns, red flags, and prevention techniques could be exchanged securely, would significantly improve sector-wide preparedness.

Finally, there was a strong perception that regulatory enforcement has not kept pace with the technological sophistication of scams. Some companies noted that when incidents are reported to authorities, responses are delayed, and technical expertise to investigate digital fraud is often lacking. Others mentioned that while they are open to collaborating with regulators, the absence of binding standards and clear guidelines creates uncertainty, particularly when balancing fraud prevention with compliance requirements. Overall, while private sector actors are aware of the scale of the problem and are experimenting with various internal controls, they remain constrained by fragmented coordination, regulatory ambiguity, and an enforcement ecosystem that is struggling to adapt to the current threat environment.

Civil Society and Academic Institutions

Interviews with representatives from academic and civil society organizations revealed growing concern over the state's ability to respond effectively to the evolving nature of online scams, particularly those enabled by recent technological developments. These stakeholders emphasized that the manipulation of audio-visual content to mimic trusted individuals, such as family members, law enforcement, or financial institutions, has become increasingly difficult to detect. Techniques that simulate live interactions, rather than static impersonation, are now being used to deceive victims with alarming precision. Academic experts stressed that these methods exploit trust-based relationships in ways that existing legal frameworks were not designed to anticipate.

There was consensus among respondents that the legal system has not kept pace with the sophistication of current fraud techniques. Although a number of laws cover general cybercrime and consumer protection, none provide a clear legal basis for addressing deception involving fabricated digital identities or synthetic communications. The absence of precise definitions for manipulated media has made it difficult to establish liability or build legal cases against perpetrators. Respondents noted that, under current statutes, it is often unclear who should be held responsible when an individual is deceived through content that was generated without a direct human author.

In addition to legislative limitations, civil society actors expressed concern over the institutional response to fraud. Most notably, victims often receive little to no follow-up support after reporting an incident. Several interviewees mentioned that many cases go unreported, not due to lack of awareness, but because the reporting process is perceived as overly complicated and unlikely to produce results. Moreover, there are no standard procedures in place to guide victims through recovery or redress. This lack of victim-centered infrastructure not only undermines public trust but also contributes to systemic underreporting, further limiting the ability of authorities to understand the full scope of the problem.

The uneven distribution of digital literacy across demographic groups was also raised as a critical vulnerability. Respondents observed that older adults, rural populations, and individuals with limited education are particularly susceptible to online fraud. Many of these individuals are unfamiliar with the tactics now being used and are unable to verify the authenticity of digital interactions. However, it was also noted that even those who are more digitally fluent can fall prey to these schemes, especially when emotional pressure or urgent messaging is involved. This underscores the point that technological familiarity does not necessarily equate to fraud resistance.

Respondents consistently called for stronger engagement between state institutions and non-governmental actors. They advocated for regular consultation between policymakers, educators, and researchers to co-develop public education materials, design early warning systems, and contribute to the development of legal standards. One suggestion that emerged repeatedly was the creation of a central database cataloguing known fraud methods, particularly those involving digital manipulation, which could be used for both public awareness and policy development.

In their final reflections, several participants urged policymakers to move beyond reactive enforcement and consider long-term preventive strategies. This includes integrating digital safety into school curricula, investing in community-based education initiatives, and establishing clearer lines of accountability for platforms that host or facilitate deceptive content. While technology will undoubtedly continue to evolve, respondents emphasized that institutions must develop a more adaptive and collaborative approach if they are to remain effective in safeguarding the public.

Discussion Phần này em định thêm một chút:

As GAI continues to reshape the digital threat landscape, Vietnam faces both an opportunity and an imperative: to modernize its regulatory and institutional architecture in ways that reflect the complex, cross-cutting nature of AI-enabled online scams. This study has highlighted that while awareness of GAI-related risks is rising across government, private, and civil society sectors, current responses remain fragmented, reactive, and constrained by outdated legal frameworks and limited technical capacity.

The findings emphasize the need for a holistic governance approach, one that integrates legal reform, technological innovation, institutional coordination, and public engagement. Regulatory clarity must be strengthened through updated definitions of AI-assisted fraud, while inter-agency collaboration should be institutionalized to overcome jurisdictional silos. At the same time, private sector actors require clearer guidelines and protected channels for information exchange to ensure that fraud prevention does not conflict with data protection obligations.

Equally critical is the investment in digital literacy and victim support infrastructure, especially as GAI enables scams that are psychologically manipulative and difficult to detect even for experienced users. By engaging academic and civil society organizations in public education and early-warning design, Vietnam can enhance its collective resilience against emerging digital harms.

Vietnam's evolving response to AI-driven fraud offers lessons not only for domestic policy but also for other nations navigating similar digital transformations. Building a proactive, inclusive, and adaptive governance system, rooted in cross-sector trust and technological foresight, will be essential to protecting the integrity of Vietnam's digital economy and fostering public confidence in the generative AI era.

Conclusion

This study examined Vietnam's readiness to address the emerging threat of generative AI–enabled scams through the perspectives of government agencies, private sector actors, and civil society organizations. While stakeholders recognize the growing sophistication and prevalence of AI-assisted fraud, their responses remain constrained by fragmented coordination, outdated legal definitions, and uneven technical capacity.

The findings highlight an urgent need for a more integrated and adaptive governance approach—one that combines regulatory clarity, institutional coordination, and public engagement. International experience demonstrates that targeted, risk-based regulation can address the unique challenges of AI-generated deception without stifling beneficial innovation. For Vietnam, this means updating legal frameworks to clearly define synthetic content and AI-assisted fraud, enabling cross-sector intelligence sharing, and embedding scam resilience into both public education and platform design.

Beyond national policy, Vietnam's experience has broader relevance for other rapidly digitizing economies facing similar governance dilemmas. The tension between enabling AI-driven growth and mitigating emergent harms will persist as technologies evolve. By institutionalizing adaptive, trust-based governance, Vietnam can not only reduce the risks of AI-enabled scams but also strengthen public trust in digital transformation—turning a reactive posture into a proactive model for responsible innovation.

References

Araz Taeihagh. 2025. "Governance of Generative AI." *Policy and Society* 44 (1): 1–22. https://doi.org/10.1093/polsoc/puaf001.

Bikash Saha, Nanda Rani, and S. K. Shukla. 2025. "Generative AI in Financial Institution: A Global Survey of Opportunities, Threats, and Regulation." *ArXiv* abs/2504.21574. https://doi.org/10.48550/arXiv.2504.21574.

Bociga, Diana, and Nicholas Lord. 2025. "Artificial Intelligence and the Organisation and Control of Fraud." *CrimRxiv*, 10–16.

Chongluadao.vn. n.d. *Anti-Scam Blacklist Statistics*. https://chongluadao.vn/thong-ke?type=blacklist.

Divya, V., and Agha Urfi Mirza. 2024. "Transforming Content Creation: The Influence of Generative AI on a New Frontier." *Exploring the Frontiers of Artificial Intelligence and Machine Learning Technologies* 143. https://doi.org/10.59646/efaimltC8/133.

Dunford, Helen. 2015. "Digital Literacy and Digital Inclusion: Information Policy and the Public Library." *The Australian Library Journal* 64 (2): 148–49. https://doi.org/10.1080/00049670.2015.1033054.

GASA, and Gogolook. 2023. *Asia Scam Report 2023*. https://hpt.vn/Uploads/File/2023/Bao-cao-lua-dao-Chau-A-2023.pdf.

George, A. Shaji, and AS Hovan George. 2023. "Deepfakes: The Evolution of Hyper Realistic Media Manipulation." *Partners Universal Innovative Research Publication* 1 (2): 58–74.

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

Iga Daniel Ssetimba, Jimmy Kato, Eria Othieno Pinyi, Evans Twineamatsiko, Harriet Norah Nakayenga, and Eudis Muhangi. 2024. "Advancing Electronic Communication Compliance and Fraud Detection Through Machine Learning, NLP and Generative AI:

A Pathway to Enhanced Cybersecurity and Regulatory Adherence." *World Journal of Advanced Research and Reviews*. https://doi.org/10.30574/wjarr.2024.23.2.2364.

Jaidka, K., T. Chen, S. Chesterman, W. Hsu, M. Y. Kan, M. Kankanhalli, M. L. Lee, G. Seres, T. Sim, A. Taeihagh, A. Tung, X. Xiao, and A. Yue. 2024. "Misinformation, Disinformation, and Generative AI: Implications for Perception and Policy." *Digital Government: Research and Practice*. Association for Computing Machinery.

Kha-Luan Pham, Tien-Dat Le, Anh-Duy Tran, Minh-Triet Tran, and Duc-Tien Dang-Nguyen. 2024. "Vietnamese User Awareness Against Scams in Cyberspace: An Empirical Survey." In *Proceedings of the 1st Workshop on Security-Centric Strategies for Combating Information Disorder*. https://doi.org/10.1145/3660512.3665525.

Kulkarni, Prasanna, Pankaj Pathak, Samaya Pillai, and Vishal Tigga. 2025. "Role of Generative AI for Fraud Detection and Prevention." In *Generative Artificial Intelligence in Finance: Large Language Models, Interfaces, and Industry Use Cases to Transform Accounting and Finance Processes*, 175–198.

Lai Nam Tuan. 2025. "The Synergistic Impact of AI, IoT, Blockchain, 5G, and Cloud Computing on Supply Chain Resilience in Vietnam." *International Journal of Scientific Research in Science and Technology*. https://doi.org/10.32628/ijsrst25121216.

Lodge, M., and K. Wegrich. 2012. *Managing Regulation: Regulatory Analysis, Politics and Policy*. Palgrave Macmillan, 27–73. https://doi.org/10.1007/978-1-137-26552-4.

National Cyber Security Center. 2023. *Cybersecurity Report 2023*. https://antoanthongtin.gov.vn/tin/lua-dao-truc-tuyen-trong-nam-2024-gay-thiet-hai-len-den-18900-ty.

Ng, L. H. X., and Araz Taeihagh. 2021. "How Does Fake News Spread? Understanding Pathways of Disinformation Spread Through APIs." *Policy and Internet* 13 (560): 585. https://doi.org/10.1002/poi3.268.

Nguyen, Huy H., Siyun Liang, Junichi Yamagishi, and Isao Echizen. 2024. "Navigating Real and Fake in the Era of Advanced Generative AI." *APSIPA Transactions on Signal and Information Processing* 14 (3).

Nikhil Gupta. 2025. "Security Risks of Generative AI in Financial Systems: A Comprehensive Review." *World Journal of Information Systems*. https://doi.org/10.17013/wjis.v1i3.16.

Reid, Julie. 2024. "Risks of Generative Artificial Intelligence (GAI)-Assisted Scams on Online Sharing-Economy Platforms." *The African Journal of Information and Communication (AJIC)*, no. 33 (August): 1–21. https://doi.org/10.23962/ajic.i33.18162.

Rusch, Jonathan J. 1999. "The 'Social Engineering' of Internet Fraud." In *Internet Society Annual Conference*. http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm.

Vietnam National Cyber Security Technology Joint Stock Company. 2024. *Vietnam Cybersecurity Report 2024*. https://ncsgroup.vn/wp-content/uploads/2025/01/NCS-Bao-cao-an-ninh-mang-2024.pdf.

Viettel Threat Intelligence. 2024. *Vietnam Cyber Security Report 2024*. https://blog.viettelcybersecurity.com/bao-cao-tinh-hinh-nguy-co-attt-tai-viet-nam-nam-2024/.

World Economic Forum. 2023. *Global Cybersecurity Outlook 2023*. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

INFORMATION RESILIENCE & INTEGRITY SYMPOSIUM

Generative AI and Information Resilience in the Asia-Pacific: Actions and Adaptations

↘ Faculty of Social and Political Sciences
Universitas Gadjah Mada

↘ 21 August 2025

saferinternetlab.org/iris
@saferinetlab
@cfds_ugm
iris@saferinternetlab.org