Safer Internet Lab
Led by CSIS in partnership with Google

Centre for Strategic and International Studies

Google

Research report

Online Fraud and Scams in the Philippines

Safer Internet Lab

Online Fraud and Scams in the Philippines

Jose Carlos Alexis Bairan[1], Queen Cel Oren[2]

INTRODUCTION

As with most countries globally, the Philippines experienced an accelerated shift towards digitalization in the past years due to the advancements in technology and the COVID-19 pandemic, transforming many aspects of how Filipinos lived and worked. The digital shift provided an opportunity for people to work, study, and do most activities remotely, while it enabled organizations to continue operating amidst the mobility challenges posed by the COVID-19 pandemic. These two factors encouraged the growth and widespread adoption of various online tools such as digital wallets (e-wallets), digital banking, online payment systems, online shopping, and remote meeting platforms.

However, the promised convenience, connectivity, efficiency, and transparency of digitalization came with increased susceptibility of Filipinos to fraudulent schemes over the internet. In 2024 alone, it was reported by the Central Bank of the Philippines or *Bangko Sentral ng Pilipinas* (BSP) that around 59.4 percent of internet users have encountered or have fallen victim to online fraud. Perpetrators trick their victims through various methods, including identity theft, fake websites and profiles, digitally-tampered documents, and spammed text messages, among many others. These types of scams are also quickly becoming more problematic with the rise of artificial intelligence, which enabled online scammers to craft and execute more sophisticated scams.

A study on internet use by Meltwater and We Are Social reported that 91.3 percent of Filipino internet users aged 16 years old and higher use banking, investment, or insurance websites or applications every month. Accordingly, data from the BSP reveal that the number of e-money accounts in the Philippines significantly expanded from 257.5 million in 2022 to 393.6 million accounts in 2023. The value of digital transactions in the country totaled to about PHP 110.5 billion, making up 55.3 percent of the total retail transactions value in 2023 (BSP, 2024). The sheer volume of digital payments, internet users, e-money accounts, and internet users in the country makes it a very attractive target of artificial intelligence (AI)-powered online scams.

The growing number and sophistication of scams amidst the pervasive use of digital tools, especially those that involve personal information and financial transactions, underscore that cybersecurity has become an imperative for individuals and organizations. Against this background, this paper aims to provide an

[1] Research Associate, Ateneo Center for Research and Innovation

[2] Research Specialist, Philippine Institute for Development Studies

overview of the patterns and trends in online scams in the Philippines, the country's regulatory and policy environment, current initiatives and challenges, and recommendations to enhance the country's defenses against various kinds of online scams.

PATTERNS AND TRENDS IN ONLINE SCAMS IN THE PHILIPPINES

Online scams in the country continue to evolve, with scammers leveraging AI for phishing, voice cloning, ransomware, and deep-fake videos to deceive individuals into revealing personal information or making financial transactions. AI-generated content is also used to craft highly personalized messages targeting specific individuals or demographics, making fraudulent communications more difficult to detect. However, identifying whether a scam is AI-enabled remains a challenge.

Online scams occur frequently, with some being cross-border. Some private industries measure both financial and non-financial impacts but usually keep such information confidential. AI-enabled tools are used for scam detection, though specific details are not shared publicly. A significant number of scams take place on social media platforms, and organizations emphasize data privacy and customer security. While public awareness of online scams is high, trust in government protective measures remains relatively low.

Phishing occurs across various platforms, including calls, SMS, emails, phishing links, fraudulent social media pages, e-commerce apps, and lost or stolen phones. Incidents of hacking emails and social media accounts are also common. Pyramid schemes use deceptive tactics, such as incorporating tasks like CAPTCHA encoding, to appear legitimate while relying on recruitment rather than sustainable product sales.

Scammers also exploit social media and messaging apps for romance scams, where they build trust with victims before defrauding them. Package scams deceive individuals into paying fees for non-existent deliveries, often using platforms like Facebook Messenger. As scams continue to adapt and spread, heightened vigilance, stronger cybersecurity measures, and proactive fraud detection remain essential in combating these threats.

SOCIO-ECONOMIC IMPLICATIONS OF SCAMS

Online scams result in substantial financial losses for individuals, businesses, and financial institutions, disrupting economic stability and personal financial security. Fraudsters continuously exploit weaknesses in digital systems, employing deceptive tactics such as phishing, business email compromise, hacking, and romance scams to manipulate victims into divulging sensitive information or transferring funds. These scams evolve with technological advancements, making them increasingly difficult to detect and prevent.

Certain groups are particularly vulnerable to online scams, with senior citizens and low-income individuals facing a heightened risk due to limited digital literacy and a lack of awareness about cybersecurity threats. Many elderly victims fall prey to scams disguised as urgent financial requests or fraudulent investment opportunities. At the same time, low-income individuals may be enticed by fake job offers or loan scams promising quick financial relief. These deceptive practices not only deplete personal savings but also contribute to emotional distress and economic hardship, further widening social inequalities.

Businesses, too, are severely impacted by online scams, experiencing both direct financial losses and secondary consequences that affect long-term stability. Cybercriminals often target companies through sophisticated social engineering schemes, compromising business operations and eroding customer trust. Beyond immediate financial setbacks, organizations suffer reputational damage that may result in lost clientele, decreased investor confidence, and increased regulatory scrutiny. Resources allocated to mitigating cyber fraud—such as enhanced security measures, legal fees, and fraud investigations—divert funds away from business expansion, innovation, and job creation, stifling overall economic progress.

The repercussions of online scams extend far beyond financial losses, influencing public confidence in digital financial services. Widespread cybersecurity concerns deter individuals from fully participating in digital transactions, limiting the adoption of online banking, digital payments, and other fintech solutions. Victims who experience financial fraud often reduce discretionary spending due to diminished trust in online platforms, leading to lower consumer engagement and weaker investment activity. This hesitancy directly affects government-led financial inclusion initiatives aimed at expanding access to credit, insurance, and investment opportunities for Filipinos. A lack of trust in digital financial systems hampers the country's transition toward a more digitally connected economy, slowing economic growth and innovation.

Compounding this issue is the increasing misuse of AI in executing scams, allowing fraudsters to refine their tactics with greater sophistication. AI-driven phishing attacks, deepfake scams, and automated fraud schemes make it more difficult to differentiate between legitimate and fraudulent transactions as scammers continue to leverage AI to enhance deception, traditional detection methods become less effective, necessitating continuous advancements in cybersecurity defenses.

The persistent rise in online fraud highlights the need for ongoing research into emerging scam trends and the effectiveness of awareness initiatives. Understanding how scams evolve, assessing the effectiveness of current preventive measures, and enhancing public preparedness are crucial in mitigating financial crimes. Without proactive intervention, the economic and social consequences of cyber fraud will continue to escalate, reinforcing skepticism toward digital financial services and hindering the country's progress in building a secure and inclusive digital economy.

STAKEHOLDER IDENTIFICATION/INSTITUTIONAL SETUP

There are several Philippine government offices and law enforcement agencies with various functions and responsibilities that are relevant to ensuring that Filipinos are safe and secure from online scams. The frontline of the country's financial system, the BSP, formulates, implements and monitors compliance to policies and regulations that govern BSFIs, which are the prime targets of online scammers.

The Department of Information and Communications Technology (DICT) is the primary government entity involved in policy making, planning, coordinating, implementing, and administering the development of the national information and communications technology (ICT) sector. The DICT leads the crafting and implementation of the NCSP to set standards that aim to enhance cybersecurity across government agencies and critical infrastructures. It also oversees the National Computer Emergency Response Team (NCERT), which handles cybersecurity incident responses. Other offices attached to the DICT with cybersecurity-related mandates are as follows:

- **Cybercrime Investigation and Coordinating Center (CICC)** - responsible for developing and employing coordinating mechanisms that allow law enforcement agencies, telecommunications industry, and other key stakeholders to work together in cybercrime prevention, investigation, and enforcement.

- **National Privacy Commission (NPC)** - Ensures the compliance of individuals and organizations to the Data Privacy Act and monitors possible data privacy violations in the collection, storage, processing, and use of personal data, which is usually linked to online scams.

- **National Telecommunications Services (NTC)** - regulates all telecommunications services and provides reporting mechanisms for telecommunications service providers and users to report incidents related to online scams.

There are also several law enforcement agencies involved in ensuring that online scam incidents in the country are appropriately addressed. The Office of Cybercrime under the Department of Justice (DOJ) acts as the focal government office for investigating and prosecuting cybercrime cases, including online scams, under the Cybercrime Prevention Act. Meanwhile, the Philippine National Police's Anti-Cybercrime Group enforces laws against cybercrimes, receives reports on online scams and enforces entrapment operations, while the National Bureau of Investigation's Cybercrime Division conducts investigations, gathers evidence, and runs forensic analyses on cybercrime cases.

To keep up with the expansion of the digital economy, particularly e-commerce, the E-Commerce Bureau under the Department of Trade and Industry (DTI) was also established through the passage of the Internet

Transactions Act in 2023. With the Bureau's mandate to formulate and oversee the policies for e-commerce, the Philippine government is expected to better regulate online transactions, enhance consumer protection, and foster a high-trust environment between consumers and businesses.

Table 1. Summary Matrix of Philippine Government Offices with Cybersecurity-Related Roles

Authority	Role in Online Scams and Fraud
Policy Formulation and Oversight	
Department of Information and Communications Technology (DICT) *Includes the following offices:* 1. Cybercrime Investigation and Coordinating Center (CICC) 2. National Telecommunications Commission (NTC) 3. National Privacy Commission (NPC)	• Oversees policies and programs related to the development of the national ICT sector, data privacy, security, and confidentiality. • Formulates cybersecurity policies that aim to prevent, address, and minimize cyber threats and attacks. • Provides countermeasures to address domestic and transnational cyber incidents. • Monitors cybercrime cases handled by law enforcement agencies.
Bangko Sentral ng Pilipinas (BSP)	• Formulates, implements, and monitors policies and regulations to guide BSFIs in cybersecurity-related concerns. • Assists in mediating complaints between BSFIs and consumers.
Department of Trade and Industry (DTI)	• Formulates policies and monitors and oversees e-commerce transactions. • Handles consumer complaints about unfair trade practices.
Department of Justice – Office of Cybercrime (DOJ-OOC)	• Handles the prosecution of cybercrime cases, including online scams, that violate the provisions of the Cybercrime Prevention Act. • Responsible for international cooperation on legal assistance and extradition, which may involve

	resolving issues related to cross-border fraudulent transactions.
Anti-Money Laundering Council (AMLC)	• Although it has no mandate to prevent online scams, it provides initiatives to create infographics for public awareness.
Law Enforcement Agencies	
Philippine National Police – Anti-Cybercrime Group	• Enforces laws, conducts cybercrime investigations, including online scams, and raises public awareness against online fraud.
National Bureau of Investigation - Cybercrime Division	• Investigates investment scams, cybercrime, and other types of online scams.

SIGNIFICANT POLICY DEVELOPMENTS

To combat the growing volume and sophistication of online scams, the Philippine government has several laws, regulations, and plans in place that build a strong cybersecurity system that aim to protect businesses and consumers from these crimes. Over the past decade, the Philippines has made significant progress in tightening measures not only to enhance the resilience of digital transactions against online scams, but also to protect consumers' data.

For instance, in 2012, the Philippines was ahead of other Southeast Asian countries in introducing legislation on data privacy and cybercrime. The Cybercrime Prevention Act (RA 10175) criminalizes fraudulent activities facilitated online such as hacking, identity theft, and online fraud, including scams that utilize AI technologies. On the other hand, the Data Privacy Act (RA 10173) regulates the storage, processing, and use of personal information. It mandates organizations to comply with the set security measures to protect personal sensitive data from unauthorized access, disclosure, or loss to reduce the risk of data breaches that can be used maliciously for scams and other cybercrimes.

Anti-Money Laundering Act (AMLA) (RA 9160) or the also serves as key legislative tools in combating online scams, AI-driven fraud, and cross-border cybercrimes. The AMLA establishes the legal framework for monitoring financial transactions, detecting suspicious activities, and working with international organizations to address financial crimes linked to scams. These legal frameworks provide a foundation for a coordinated response to evolving cyber threats.

More recently, new legislation on consumer protection and cybersecurity such as the "Financial Products and Services Consumer Protection Act" (FCPA) (RA 11765) and the "Anti-Financial Account Scamming Act (AFASA)" (RA 12010) to fortify the consumers and financial industry's line of defense against online scams. FCPA empowered the BSP, along with other financial regulators, to implement rules and mechanisms to address consumer complaints. It also encourages financial institutions to establish accessible and reporting mechanisms for consumers to report anomalies. Meanwhile, the AFASA compels all BSP-supervised financial institutions (BSFIs)[3] to adopt more rigorous measures to protect consumers. It reinforces the responsibility of BSFIs to employ proper fraud management systems, infrastructure and security monitoring, multi-factor authentication, and user enrollment and verification processes. The legislation also sought to enhance coordination between financial institutions and law enforcement agencies by giving the BSP power to investigate suspicious transactions and share the results with relevant law enforcement agencies.

These laws are complemented by the recent launch of the Financial Services Cyber Resilience Plan (FSCRP), which will serve as the country's roadmap and framework to strengthen the financial system's defenses against cyberthreats and cybercrimes in the next 5 years. The FSCRP highlights the need for stronger information sharing and collaboration between BSFIs, government agencies, and other stakeholders through cyber threat and incident reporting, inventory, and mapping.

Moreover, the BSP issued key circulars to reinforce financial security. It issued BSP Circular No. 808, s. 2013, establishing IT risk management guidelines, requiring financial institutions to implement stringent security controls; BSP Circular No. 982, s. 2017, strengthening information security to prevent fraud; and BSP Circular No. 1019, s. 2018, mandating all BSFIs to report cyber-related incidents.

Other relevant policies and regulations help combat online scams by strengthening cybersecurity and consumer protection. Internet Transactions Act of 2023 (RA 11967) aims to enhance protection in online transactions and improve consumer trust by regulating businesses and consumers engaged in online transactions. This involves creating an e-commerce bureau in charge of maintaining a database of online businesses, ensuring dispute resolution mechanisms, and creating a code of conduct for both businesses and consumers. The adoption of the National Cybersecurity Plan 2023-2028 aligns with the Philippine Development Plan (PDP) to enhance cybersecurity, build a more skilled workforce, and strengthen policy frameworks for a safer digital environment. The bill on the Cybersecurity Act, which seeks to enable the government to keep up with major advancements in technology and cybersecurity such as AI, critical information infrastructures, and digital assets, is still pending in the 19th Congress.

[3] Includes banks, quasi-banks, pawnshops, foreign exchange dealers, money changers, remittance agents, electronic money issuers or e-wallets, and non-stock savings and loan associations.

CHALLENGES TO COMBAT ONLINE SCAMS

Cybercriminals continue to develop more sophisticated methods, making it essential for businesses and other entities handling financial transactions to remain vigilant in protecting both themselves and their clients. Some government agencies provide infographics on their websites to inform the public about current and emerging threats.

Campaigns to increase public awareness play a key role in helping individuals recognize and report scams. The effectiveness of scam awareness efforts can be gauged through surveys and feedback, which help determine people's understanding of scam tactics, their ability to recognize red flags, and their reactions to potentially fraudulent situations. As digital financial transactions grow, improving data protection measures, enhancing information-sharing systems, and implementing timely interventions are necessary to strengthen anti-fraud efforts.

Institutions are adopting various IT solutions, including AI-driven tools to prevent, detect, and mitigate cyber threats. Regular cybersecurity advisories and awareness campaigns are disseminated among staff to minimize risks and safeguard IT infrastructure. Additionally, security awareness infographics are shared to educate personnel about emerging scams. Advanced perimeter cybersecurity tools are also deployed to monitor and counter malicious emails and traffic, addressing both conventional and AI-enabled threats.

Evaluating the effectiveness of these anti-scam initiatives requires assessing awareness programs, tracking scam prevalence, and analyzing regulatory measures. AI-driven fraud detection is gaining traction, enhancing transaction monitoring by identifying suspicious patterns and anomalies in real-time. While AI adoption remains limited, its potential to improve detection accuracy, incident response times, and regulatory compliance underscores the need for stronger implementation strategies. However, the lack of AI-related governance policies and skilled professionals, particularly in regional agencies, remains a challenge. Strengthening enforcement and investing in AI-driven security measures are essential to mitigating the growing risks of digital fraud in the Philippines.

A significant challenge in combating online scams is the validation of social media accounts and the spread of misinformation. The Philippines has limited mechanisms to hold major platforms such as Meta, X, and TikTok accountable for the proliferation of fraudulent accounts and false information. Additionally, there are resource limitations in providing public information to combat online scams and other fraudulent activities.

Cross-border online scams remain a growing concern despite ongoing international cooperation, including the use of mutual legal assistance treaties (MLATs). However, the increasing sophistication and global nature of these scams require more streamlined and efficient collaboration between authorities.

Strengthening real-time information-sharing mechanisms is necessary to address the rapidly evolving tactics used by cybercriminals.

CONCLUSION AND RECOMMENDATIONS

In the face of more sophisticated cyber threats, particularly the escalating prevalence of emerging fraudulent scams, the Philippines must adopt various approaches to enhance its cybersecurity defenses. Elevating public awareness is of paramount importance. Comprehensive public awareness campaigns are essential to instill a culture of vigilance against online scams. Although detecting online fraud through observation alone is difficult, timely reporting and informing potential victims *through social media platforms* can prevent further harm. These campaigns should go beyond mere warnings, providing practical, actionable tips for identity protection and scam detection, empowering citizens to safeguard their personal information. Fostering collaborative action is also crucial. A robust cybersecurity ecosystem necessitates a strong partnership between government agencies, private sector businesses, and civil society organizations. This collaborative approach facilitates the seamless sharing of threat intelligence, the development of effective countermeasures, and the encouragement of timely reporting of cybercrimes and suspected fraudulent activities. This synergy ensures a unified front against cyber threats.

Empowering Small and Medium-sized Enterprises (SMEs) is vital, as they are often the most vulnerable to cyberattacks. Targeted support and resources must be provided to enhance their cybersecurity capabilities. This includes guidance on prevention strategies, mitigation tactics utilizing artificial intelligence, and access to affordable, yet effective, cybersecurity solutions. The rapid advancement of AI necessitates the urgent development of a comprehensive AI governance framework. This framework must strike a delicate balance between fostering innovation and ensuring responsible deployment. It should address critical ethical considerations, safeguard data privacy, and mitigate potential security risks, ensuring that AI benefits society without compromising its safety. Strengthening regulatory enforcement is crucial. Existing cybersecurity laws, such as the Cybercrime Prevention Act of 2012 (RA 10175) and the Data Privacy Act of 2012 (RA 10173), must be rigorously enforced. This requires a substantial investment in cutting-edge technology, recruiting and training highly skilled personnel, and streamlining enforcement processes.

Empowering the Local Government Units (LGUs) is also critical for a universally secure cyberspace. Cybersecurity efforts must extend beyond Metro Manila, reaching all corners of the country. Investing in LGUs' cybersecurity capabilities ensures effective response and prevention efforts are implemented nationwide. A significant increase in resource allocation is necessary. The government must allocate sufficient funds to acquire state-of-the-art technological tools and to develop a highly skilled workforce capable of effectively combating cybercrime. This investment is essential to building a resilient and secure

digital environment for the Philippines. Furthermore, it is essential to encourage further studies that continuously monitor and evaluate emerging trends in AI-driven scams to enhance prevention and mitigation strategies.

REFERENCES

Bangko Sentral ng Pilipinas. 2024. *Financial services resilience plan 2024-2029: Fortifying cyber frontier for BSP-supervised financial institutions.* Bangko Sentral ng Pilipinas, Technology Risk and Innovation Supervision Department.

Bangko Sentral ng Pilipinas. 2024. *Traversing new heights: The future is digital: 2023 status of digital payments in the Philippines*. Bangko Sentral ng Pilipinas.

Financial Inclusion Steering Committee. 2024. *2023 annual report: National strategy for financial inclusion*. Bangko Sentral ng Pilipinas.

Meltwater & We Are Social. 2024. *Digital 2025 Global overview report: The essential guide to the world's connected behaviours.* https://www.meltwater.com/en/global-digital-trends

Safer Internet Lab

saferinternetlab.org

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

Find Us On

CSIS Indonesia | Safer Internet Lab