Safer Internet Lab
Led by CSIS in partnership with Google

Centre for Strategic and International Studies

Google

Research report

Online Fraud and Scams in Indonesia

Safer Internet Lab

ONLINE FRAUD AND SCAMS IN INDONESIA

Safer Internet Lab

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 Indonesia

Adinova Fauri[12], Futy Ichiradinda[13], Rojwa Rachmiadi[14]

INTRODUCTION

Over the past decade, the internet penetration rate in Indonesia has more than doubled from 88,1 million users in 2014 to nearly 221.6 million users or 79,5 percent of the population in 2024 (Shofa & Muslim, 2024). The increasing trend of internet penetration has opened new economic opportunities, such as digital payment systems, remote working, e-commerce, cross-border transactions, and Artificial Intelligence (AI) tools.

However, the rise in internet penetration and digital platform adoption also presents significant challenges, as it increases the risk of scams spreading among the public. New technology such as AI are also being exploited for scams, such as replicating an individual's facial and audio features to deceive victims and illegally acquire financial gains. This crime, combined with existing online scams such as ransomware, phishing, and bogus schemes, poses an emerging threat, especially among vulnerable communities with lower levels of digital and financial literacy. In response to these threats, the Indonesian government has introduced several initiatives to combat scams, including the establishment of the Indonesia Anti-Scam Center. The Indonesian government has also launched its "National Strategy for Artificial Intelligence", providing a guideline to develop AI from 2020 to 2045. Despite existing laws on data protection, electronic information and transactions, and anti-scam strategies, there is room to strengthen policies and interventions to protect the public against online scams.

PATTERNS AND TRENDS

Types of Scams

Indonesia has historically been a victim of financial fraud cases, especially since the early 2000s due to the growing usage of mobile phones and the internet. The types of scams observed from 2008 to 2012 include distraction principle scams (advance fee/lottery scams, romance/relationship scams, job scams), time principle scams (intimidation scams via voice-and-text-based communication scams), kindness principle scams (charity scams via emails, websites, and forums), social compliance scams (business scams via SMS, email, forums), and unnoticeable scams (hacking, fake ATMs, phishing) (A.H. Kusomo, et al., 2017).

Unlike traditional scams that may rely on a single method, modern fraudsters frequently use a variety of channels, such as a combination of phone calls, emails, and text messages to boost their success rate. Moreover, creating a sense of urgency while impersonating law enforcement officers, bank officials, or family members is a key strategy in luring victims, as people tend to use less reasoning when making decisions under time pressure (A.H. Kusomo, et al., 2017).

Based on a 2013 State of The Internet report, Indonesia ranks second in the world for cybercrime cases, with romance scams being one of the most common, particularly among women. Typically, love scammers are foreign nationals working in groups with Indonesian accomplices to pretend as wealthy military officials, doctors, engineers, or businessmen. Fraudsters target individuals through social media,

[12] Researcher, Department of Economics, CSIS Indonesia
[13] Project Research Assistant, Safer Internet Lab, CSIS Indonesia
[14] Project Research Assistant, Safer Internet Lab, CSIS Indonesia

building an emotional relationship with them over a long time before manipulating them into sending money under the deception that they are helping a significant other. Victims tend to disregard warnings about the risks of being scammed because they are convinced that the relationship is real (Juditha, 2015).

In COVID-19, online scam cases have surged in tandem with the development and popularity of online platforms. Fraudsters offer victims illegal loans through SMS or WhatsApp from an unknown number. When they fail to pay on an agreed schedule, they can be charged a 10 percent interest daily, making the repayment of loans nearly impossible. Victims may fail to recognize they were being scammed, and are reluctant to report due to the fear of damaging their reputation. These fraudsters also threaten family members, using their personal data for their benefit, causing severe psychological consequences that may lead to suicide (Magfirah & Husna, 2022).

In 2021, the growth of online shopping platforms and digital payment systems has also opened new opportunities for e-commerce scams, where fraudsters act as fake sellers, fabricating the image of a trusted shop and luring victims to pay for goods that were never shipped (Saleh, 2022). In 2023, online gambling became a growing concern; they are frequently advertised through WhatsApp, offering promising bonuses to lure victims. Furthermore, perpetrators were found to quickly change their sites and mechanisms to avoid getting caught by law enforcement (Hasibuan, 2023).

In 2024, Indonesia ranks second in Southeast Asia with 85.908 phishing cases after Thailand, with nearly triple the number (Novianty, 2025). Previous studies show that most respondents were tricked into clicking seemingly credible organizations that promise rewards (33.8 percent) (Abisono, et al., 2022). Moreover, s.id, my.id, and biz.id were among the most used domains used by perpetrators to deceive victims, mainly targeting social networking sites (e.g., Facebook, Meta, Instagram), financial (e.g., Dana, BRI), and gaming platforms (e.g., Garena) (IDADX, 2024).

Moreover, scams are 3,5 times more likely to occur in piracy sites compared to mainstream sites, as most users are unaware of seemingly benign digital behaviors, such as watching sports streams on illicit websites. Out of the 90 advertisements identified through repeated page views, 52,22 percent of them were classified as high-risk entry points for online scams. Fake streaming platforms collect users' sensitive information by requiring them to create an account, and a user would likely encounter up to 20 cyber threats for every 100-page visit to these sites. For instance, links disguised as Adobe Flash installations were confirmed to have malicious capabilities, including potential attacks of malware, ransomware, credential theft, data exfiltration, and destructive attacks (Watters, 2024).

Targeted Victims

Individual targets

A study identified that Indonesia exhibits high levels of power distance and collectivism, which in turn contribute to a high level of materialism in the country. This culture drives the susceptibility of people to the temptation of quick financial gain schemes. In many cases (see Annex A), financially literate people are not immune to deceitful messages, as multiple psychological principles were used to lure them (Prabowo, 2024).

Despite that, ample evidence illustrates that fraudsters have been consistently impacting people from low socioeconomic and educational status. In 2022, Indonesia ranks 61st out of 100 countries based on the level of education and internet (Amanta, 2022), and low levels of financial literacy may contribute to the low awareness of loan scams (Magfirah & Husna, 2022). Fraudsters were also found to take advantage of this by offering them small amounts of cash in exchange for self-portraits of them with their national ID to be used for illegal activities (GrabDefence, 2022).

In terms of gender, in 2022, women accounted for 55 percent of online scam victims (BaliNews, 2025). In the following year, a qualitative study on romance scam victims in Indonesia revealed that physical attraction was the main determinant in pursuing the initial attraction online, as woman/s interpersonal success in the country is often associated with having a partner (Niman, et al., 2023). In terms of age group, financial scams appeal to younger and older individuals. Older individuals, especially those who live alone, are targeted due to their loneliness and less familiarity with online platforms (A.H. Kusomo, et al., 2017). Younger individuals, on the other hand, were targeted due to their susceptibility to indulge in addictive and trendy schemes.

The rise of online gambling in Indonesia has affected both the younger and the older generation. In 2024, approximately 4 million Indonesians engage in online gambling sites. Although the majority of players are between 31 and 50 years old (40 percent) and above 50 years old (33 percent), there is a small portion of underage players who are often neglected by their parents. Furthermore, about 80 percent of players come from the middle to lower socioeconomic class. From 2017 to 2022, online gambling transactions totaled up to a turnover value of Rp 190 trillion. Online gambling players in Indonesia are dominated by the West Java region (~535,644 players with transactions of Rp 3,8 trillion), followed by DKI Jakarta (~238,568 players with transactions of Rp 2.3 trillion) and Central Java (~201,963 players and transactions of Rp 1.3 trillion). Increased financial losses have led to massive debts, triggering them to commit criminal acts such as theft, fraud, and violence to earn money (Junaedi, 2024).

With having a simpler verification steps in registering digital financial services, the Indonesian Financial Transaction Reports and Analysis Centre (PPATK) found that more than 24.000 children aged 10 to 18 years were victims of financial scams, with transaction values of more than Rp 127 billion. Security features in digital wallets are becoming a double-edged sword, where user privacy measures were exploited to hide the identities and locations of fraudsters, easing cross-border transfers and untraceable payments. Fraudsters groom children to provide inappropriate content or services that are paid in virtual currencies, such as bitcoin, to conceal the traces of illegal funds (Yulia and Sofian, 2024; Febriansyah, et al., 2024; Fransisco, et al., 2024).

Furthermore, it is worth noting that Indonesia is not only a victim of online scams, but also a victim of human trafficking. The Director of Protection of Indonesian Citizens and Legal Entities from the Ministry of Foreign Affairs confirmed that as of February 2025, there have been 6.800 cases of Indonesian citizens involved in online scams since 2020, and the number will most likely continue to increase (AntaraNews, 2025). Syndicates attract victims on social media by advertising jobs (e.g., marketing, human resources, translation, finance, casinos, hotels, and IT) with simple and easy job requirements, false promises of high salaries, bonuses, free accommodations, logistics, and the opportunity to work overseas. However, some were also recruited by close peers, such as family members, friends, and neighbors (IOIM, 2023; LSCW, 2024).

Individuals who are in their twenties, have completed secondary education, and are bilingual were found trafficked to Cambodia, Myanmar, the Philippines, and Thailand as online scam operators (IOIM, 2024). Additionally, 53 Indonesians who were trafficked in Cambodia were recruited by Indonesian nationals, thus increasing trust during recruitment (UNODC, 2023). Although most victims were deceived and violently coerced into working in scam compounds (United Nations, 2025), some would proceed nonetheless due to attractive salaries and potential commissions for good performance. Challenges for law enforcement persist, as it may be that some people do not want or need to be rescued (UNODC, 2023).

Organizational/business targets

Fraudsters have primarily targeted financial institutions, with credit card thefts causing a loss of more than USD 100 million in 2008 alone (see Annex B). With the rising adoption of technology, from 2012 to 2015, the police have caught more than 497 suspects of cyberattacks, including financial scams, and more than half of them were foreign citizens. These fraudsters sent messages that appeared closely similar to a real token message from the bank, and security loopholes were reported in large e-commerce sites like Bukalapak, Tokopedia, and Sribu. Aside from financial motives, government and corporate websites were also hacked for political motives. Despite the major losses incurred from online scams in Indonesia, almost all cases were kept confidential with very limited public disclosure (Edy et al., 2017).

Emerging Trends

The use of Artificial Intelligence for online scams in Indonesia has only started to emerge in 2023, utilizing mainly deepfake and voice cloning technology to steal identities and deceive victims into believing they are someone trusted, and creating fake scenarios to trick them into transferring money. Most of the losses incurred were derived from deepfake videos, where faces of well-known public figures were stolen to verbally promote malicious sites or counterfeit programs, such as claiming they provide promising returns from online gambling or are distributing financial aid. These videos often have phone numbers attached for victims to contact before they are asked to transfer money in advance, usually with the promise of it being returned or as an administration fee, only to realize they will be sent to the fraudsters' accounts. On the other hand, news articles on voice cloning scams show that rechecking the person whose identity is being stolen effectively detects scams and avoids further damage (see Annex C on deepfakes cases in Indonesia).

POLICY ASSESSMENT AND ADDRESSING SCAMS

National Initiatives and Policies

Electronic Information and Transactions Law

The primary legal framework regulating the digital and cyber domain in Indonesia is the Electronic Information and Transactions (EIT) Law. Indonesia's EIT Law aims to regulate a clean, safe, ethical, productive, and just digital landscape to protect the public from misusing electronic information, documents, and transactions, and any cyberthreats. The table below outlines key provisions of the EIT Law that address cyberthreats and misinformation.

Table 4.1 Summary of Penalties Related to Online Scams in the Policy Document

Crime	Details	Penalties	Article
Online gambling	Creating, distributing, transmitting, and/or making electronic information and/or records related to gambling	Maximum of 10 years in prison or Rp 10 billion fine	45 (3) in (1/2024)
Disinformation	Distributing and/or transmitting electronic information and/or records with false information and causing	Maximum 6 years in prison and/or Rp 1 billion fine	45 A (1) in (1/2024)

	material loss		
Data theft	Unauthorized or unlawfully alters, adds, reduces, transmits, tampers with, deletes, moves, or hides electronic information and/or electronic records of other persons or the public.	Maximum 8 years in prison and/or Rp 2 billion fine	32 (1), 48 (1) in (11/ 2008)
Data theft	Unauthorized or unlawful moves or transfers of electronic information and/or electronic records to electronic systems of unauthorized persons.	Maximum 9 years in prison and/or Rp 3 billion fine	32 (2), 48 (2) in (11/ 2008)
Data theft	Compromising confidential information for public access	Maximum 10 years in prison and/or Rp 5 billion fine	32 (3), 48 (3) in (11/ 2008)
Malware, Ransomware, Trojan viruses	Unauthorized or unlawful acts resulting in faults in electronic systems, and/or resulting in them working improperly	Maximum 10 years in prison and/or Rp 10 billion fine	33, 49 in (11/ 2008)
Possession, distribution, or sale of tools	Unauthorized or unlawfully produces, sells, causes to be used, imports, distributes, provides, or owns hardware, software, passwords, or access codes for cybercrime	Maximum 10 years in prison and/or Rp 10 billion fine	34, 50 in (11/ 2008)
Phishing, identity theft, deepfake, voice cloning	Unauthorized or unlawful manipulation, creation, alteration, deletion, and tampering of electronic information and/or records with the intent that such seem authentic	Maximum 12 years in prison and/or Rp 12 billion fine	35, 51 (1) in (11/ 2008)

Furthermore, as a derivative regulation under the Electronic Information and Transactions Law, the Ministry of Communications and Digital Regulation (KOMINFO) 5/2020 requires electronic system providers in the private sector to ensure regulatory compliance in digital platforms. Electronic system providers may include e-commerce, financial services, digital content distribution services, communication services, search engines, and personal data processing services. Although the document only explicitly states terrorism, child pornography, and content that causes public distress as prohibited electronic content, online scams may fall under the last category.

Table 4.2. Summary of private-sector obligations in digital platforms based on the policy document

Obligations	Article
User-generated content must have governance regarding electronic information and/or documents, and provide reporting platforms	1 (7)
Electronic systems must not contain and spread prohibited information and/or documents	9 (3)
When instructed, electronic system operators must take down prohibited electronic information and/or documents at the latest 1 x 24 hours after a warrant is issued	11c
In the case that electronic system operators fail to take down prohibited electronic information and/or documents, the Ministry will take down or order Internet Service Providers to take down the electronic system (access blocking)	15 (7)
Electronic system operators who fail to take down prohibited electronic information and/or documents will receive an administrative fine according to the provisions of laws and regulations regarding non-tax state revenues	15 (10)
Electronic system operators are required to provide access to electronic systems and/or data to the ministries or institutions for supervision under specific laws and regulations	21
Electronic system operators established in foreign countries or are permanently domiciled in foreign countries but provide services, conduct businesses, and offer services in Indonesia must also be registered under the law.	4

Anti-Fraud Measures by The Financial Services Authority

The financial services authority (OJK) has outlined four main pillars for Financial Institutions (FIs) to establish anti-fraud strategies in POJK 12/2024, including online scams (e.g., online gambling, fictional online investments, online prostitution, and other crimes with financial motives). Based on the document, FIs may include banks, securities, insurance, brokerage companies, pension funds, venture capital, microfinance institutions, pawnbrokers, and other regulated financial entities, regardless of whether they are operated under conventional or Sharia principles. Furthermore, they must establish a working unit or function to manage anti-fraud strategies, where heads or officials in charge must have a certification and experience in anti-fraud, and/or adequate experience in relevant fields.

Table 4.3. Summary of the four pillars of anti-fraud strategy for Financial Institutions

Pillars	Strategy
Prevention	• Raise awareness of employees and stakeholders through training sessions, workshops, and internal policies • Actively assess operations most vulnerable to fraud • Impose strict hiring policies to filter trusted employees, and reward employees who adhere to anti-fraud measures • Educate customers on fraud patterns using various media (e.g., brochures, campaigns, posters)
Detection	• Ensure a secure and anonymous whistleblowing mechanism • Conduct random inspections, especially in high-risk units • Actively track transactions and operational activities • Establish a clear procedure for customers and employees to report fraud, and the steps to respond to them.
Enforcement	• Collect solid evidence for fraud cases (e.g., forensic accounting, digital track records, interviews) • Comprehensively report fraud cases to OJK based on their guidelines • Impose clear, fair, and strict sanctions on fraud perpetrators. • Ensure transparency during case investigations.
Assessment	• Maintain an updated database of fraud incidents. • Actively review patterns of past fraud cases and identify room to improve anti-fraud strategies. • Ensure all employees are updated with the latest anti-fraud strategy.

To protect the public from the increasing spread of scams in Indonesia, the Financial Services Authority (OJK) established a coordination body called SATGAS PASTI. This task force consists of multiple sectors, including the Ministry of Investment, the Ministry of Communication and Digital Affairs, the Ministry of Cooperatives, the National Police, the State Intelligence Agency (BIN), the National Cyber and Crypto Agency (BSSN), and others. The formation of this multi-sectoral task force is essential to address coordination challenges in combating scams, given the wide range of fraudulent activities—spanning investment scams, institutional fraud, and trade-related deception. Additionally, scams are not always a purely domestic issue; many originate from or are linked to foreign entities. To enhance its effectiveness, the task force established the Indonesia Anti-Scam Center (IASC), providing a platform for the public to easily report scam activities.

Data Protection Law

Indonesia has enacted the Personal Data Protection Law (UU PDP) under Law No. 27 of 2022, which establishes the principle that personal data is a fundamental right that must be safeguarded and protected. Personal data plays a crucial role in protecting the public from the threat of scams. The UU PDP sets standards and guidelines for all institutions—both private and governmental—that collect and process personal data. It aims to ensure that data is securely stored and handled to prevent misuse. While Indonesia has a strong legal foundation for data protection, as of the time this report was written, no specific institution has been designated to oversee its implementation and enforcement.

Other Initiatives

Private sector initiatives

Various sectors, including online platforms, e-commerce, and financial institutions have undertaken multiple initiatives to strengthen network security against the growing threat of online fraud and scams (see Annex D). Besides, private companies are also started to utilizing AI technology to upgrade their security measures, such as:

- Real-time fraud detection systems
- Machine learning to analyze transaction patterns, detect deepfakes, and prevent synthetic identity fraud.
- Enhanced security layers and Know Your Customer (KYC) processes through two-factor authentication (2FA) and biometric verification to prevent account takeovers and unauthorized transactions.
- New merchants undergo risk assessments before being allowed to list products, reducing scam storefronts.
- Automated scam reporting system: Users will soon be able to report scams directly via an integrated industry-wide portal.
- Deploying deepfake detection algorithms to flag suspicious videos and voices.

Multi-stakeholder initiatives

The cross-sectoral nature of online scams demands coordinated efforts across various stakeholders to enhance the effectiveness of prevention and response strategies. Addressing this issue in silos – whether by individual organizations or sectors – will limit the effectiveness of mitigation and case handling efforts. Insights from our expert survey indicate that there have been collaborative initiatives between the government and private sector, one example being the establishment of the Task Force for Eradication of Illegal Financial Activities *(Satgas PASTI)*.

On February 11th, 2025, the financial authority (OJK), the Task Force, and industry players (e.g., payment service providers, e-commerce, and other relevant parties) launched the Indonesia Anti Scam Centre (IASC) to respond to fraud reports according to applicable provisions. The public can report fraud incidents by contacting OJK's customer service at 157 or filling in a form at iasc.ojk.or.id with personal data (national ID, driver's license), proof of bank account ownership, chronological order of the incident, and proof of the transaction occurring.

Once a report is logged, IASC members will promptly conduct verifications, block fraudulent transactions, identify perpetrators, and coordinate legal actions with law enforcement. Victims can track their report progress via the IASC system or the customer services of the financial services platform affected. The retrieval of lost funds can be attempted, though it may take time to coordinate between banks and financial services under the following conditions:

1. The recipient's account still has remaining funds, and transactions were verified originating from the victim's account.
2. In the case of multiple victims, refunds will be prioritized based on the order of refund requests received, the availability of remaining funds in the victim's account, and a mutual agreement among the victims.
3. If the victims fail to reach an agreement, refunds will be distributed based on a final court ruling.
4. A refund may not be processed if the recipient's account is blocked or seized by authorities.

Other initiatives include a UNODC webinar on the Digital Financial Threat Landscape and Law Enforcement in Indonesia. This webinar was funded by the Ministry of Justice of the Government of the Republic of Korea, inviting discussions with PPATK, the Director of Criminal Justice at Optima, and the Crime Prevention and Criminal Justice Officer at the Terrorism Prevention Branch of the UN Office on Drugs and Crime. The webinar highlighted the challenges in investigating financial scams and the urgency for increased information security, stakeholder mapping, and cross-border collaborations in cybercrime investigations (UNODC, 2022).

In addition, there is also an initiative to have sharing databases as to improve the warning systems from the potential online scams treats. This sharing database systems include:

- Cross-platform fraud intelligence sharing: E-commerce companies share scammer lists to prevent repeat offenders from migrating between platforms.
- Merchant blacklist system: Shared database of fraudulent merchants, ensuring they cannot reopen accounts easily.
- International cooperation: Some platforms work with Interpol and ASEAN cybersecurity bodies to track cross-border fraud networks.

CHALLENGES IN ADDRESSING SCAMS

Despite various initiatives undertaken by different stakeholders, Indonesia continues to face significant challenges in addressing scams. These challenges are not limited to the government alone but also extend to other parties, as combating scams requires strong inter-agency cooperation to enhance public protection.

Government Institutions

Challenges in Consumer Protection and Personal Data Framework

One of the key challenges in consumer protection efforts in Indonesia is the fragmented nature of regulations across different sectors, coupled with the outdated Consumer Protection Law. Indonesia's Consumer Protection Law was enacted in 1999, making it ill-equipped to address emerging challenges in the digital era. Although a new Consumer Protection Law has been included in the national legislative priority program (Prolegnas), Indonesia has yet to enact an updated version.

Another challenge in safeguarding consumers and the public is the personal data protection framework. While Indonesia has already passed the Personal Data Protection Law (UU PDP), the necessary implementing regulations have yet to be issued. These regulations are essential for providing clearer guidelines, enabling both government and private institutions to comply effectively with the UU PDP. Additionally, an independent oversight body has not yet been established to monitor data misuse. Without a dedicated regulatory body, ensuring personal data security and strengthening data infrastructure and governance will be significantly more challenging.

As technology continues to advance—especially with the increasing use of generative AI in scams—the role of data infrastructure and governance becomes even more critical. Without a robust data governance framework, scammers could exploit personal data for highly targeted scams. In the worst-case scenario, deepfake technology could be used to mimic family members, making individuals even more vulnerable than before.

Weak Enforcement Measures

As previously discussed, Indonesia currently lacks a single authoritative institution responsible for handling scam-related issues. Institutional silos remain a major challenge, as each institution has its own mechanisms for addressing scams. This fragmented approach creates a lack of clarity for the public on where and how to report scams, ultimately discouraging victims from coming forward.

Another issue is the complexity of the reporting system, which is often seen as burdensome by the public. Many victims find the reporting process non-straightforward and difficult to navigate. Furthermore, expert interviews indicate that only a small number of reports receive official responses. The lack of response could stem from regulatory bottlenecks or incomplete documentation from the complainants—an issue that needs further investigation. To improve scam prevention efforts, enhancing the reporting mechanism and providing assistance to complainants could help eliminate documentation issues on the victims' end. This, in turn, would allow regulators to respond more effectively to scam-related complaints.

Private Sector

The private sector's challenges in combating online scams in Indonesia include inconsistent policies across jurisdictions, privacy laws restricting collaboration between platforms and authorities, and incomplete scam data that may reduce response effectiveness. In detail, past studies have highlighted challenges in the following platforms:

a) **Digital banking** systems may impose extensive identity verification measures that users find complicated. As a result, a portion of Indonesians have stopped or reduced the use of credit cards (32 percent) and personal bank accounts (27 percent) due to finding identity checks too difficult and time-consuming. However, more than half surveyed had a strong preference and belief that fingerprint and face scans provide excellent security. In Asia Pacific, 60 percent would only answer up to 10 questions before abandoning the platform and seeking alternatives. Additionally, 23 percent of the Indonesian sample believes there are circumstances when falsifying personal information for digital loan applications is acceptable, while 11 percent believe it is a normal practice (FICO Consumer Survey, 2023).

b) **E-wallets** do not require strict identification, allowing fraudsters to create alternate identities by relying on phone numbers to register and cash out without a bank account. The platform can only see transaction amounts and parties, with little information on the purpose and intent of the payments, enabling them to transact without leaving a significant trace. To avoid suspicion, funds are transferred in small amounts, making detection in transaction monitoring systems increasingly challenging (Fransisco, et al., 2024; Yulia and Sofian, 2024).

c) **E-commerce** platforms may offer "Cash on Delivery (COD)" methods, which can be exploited by buyers who refuse to pay and sellers who ship incorrect goods with limited protection for both parties. Due to gaps in labor protection, couriers are also vulnerable to e-commerce scams (Fadillah, et al., 2023). Additionally, transactions conducted outside official platforms—without a third-party intermediary—such as social commerce are often exploited by scammers, leaving victims more vulnerable. Despite existing regulations regarding online scams, there are still regulations that do not specifically explain fraud involving e-commerce, and the collection of digital evidence remains a challenge (Widhaningroem and Widowati, 2024).

d) **Social media** platforms are vulnerable to click-farming operations, where informal workers provide services to inflate engagement metrics (e.g., likes, views, followers) by generating fake accounts using bots or software that run automated scripts, harvesting real accounts from exchanged or stolen login credentials via websites offering free followers, and selling these services to online shops or public figures, such as influencers and politicians. A mixture of fake and real accounts continues to challenge detection algorithms, and the entry barrier to becoming a perpetrator is low because websites may offer simple procedures that do not require programming skills (Lindquist, 2018).

e) **The telecommunications industry's role** needs to be strengthened in efforts to combat scams in Indonesia. This is because the primary channels for scam distribution are messaging apps and phone calls. The linkage between phone numbers and national identity numbers (NIK) presents an opportunity to more effectively address scams, not only within the telecommunications sector but also in digital services that require phone numbers for registration, such as e-commerce, digital financial services, and others.

One key initiative that should be encouraged is greater collaboration between the telecommunications industry and other sectors. While telecom companies have already introduced the Open Gateway initiative, its benefits have yet to be fully utilized by other industries that scammers exploit for fraud. In addition, the implementation of facial recognition technology for SIM card registration should be welcomed as a positive step in scam prevention. However, the potential misuse of facial recognition remains a challenge, especially with the rise of deepfake technology, which could further complicate security measures in the future.

Public

One of the main challenges in preventing scams in Indonesia is that increased internet access has not been accompanied by improvements in digital skills and literacy. Overall, Indonesia's digital literacy rate remains low, while the awareness related to digital security is even lower. The Indonesian Digital Society Index 2024 reports that out of the four pillars adapted from the G20 Toolkit for Measuring Digital Skills and Digital Literacy stated that:

- Indonesia scored the highest in the digital skills pillar (58,25 percent), while it scored the lowest on the empowerment pillar (25,66 percent), which shows that the increase in digital technology competencies remains insufficient to support productive economic activities.
- Less than 50 percent of the sample have a habit of ensuring the credibility of sources when engaging with digital information.
- Less than 50 percent of the sample stores backup data, use two-step verifications, and understand security threats in digital tools.
- Low adoption of digital upskilling, as only 5 percent have followed online courses, and only 2 percent have been paid instructors in an online course.
- Low usage of digital financial tools, such as Internet/mobile banking (40 percent), e-wallet (38 percent), online investments (4 percent), online loans (5 percent), and online lending (1 percent)

Another major challenge in combating scams in Indonesia is the low level of financial literacy among the public. Financial literacy can be defined as a set of skills that enables individuals to comprehend and manage their finances, including planning future finances, managing risks, and actively participating in financial markets (Arifin, et al., 2024). Without sufficient knowledge of digital financial products, people are more susceptible to scams, particularly those promising unrealistic investment returns. Based on the National Survey on Financial Literacy and Inclusion 2024 by OJK:

- The financial literacy index has increased from 21,854 percent in 2013 to 65,43 percent in 2024.

- Despite that, disparities persist between the population in urban (69,71 percent) and rural areas (59,25 percent).
- The lowest scores were in the 15-17 age category (51,70 percent) and the 51- 79 age category (52,51 percent).
- In terms of gender, females (66,75 percent) ranked higher in financial literacy than males (64,14).
- Based on occupation, unemployed (42,18 percent), students/university students (56,42 percent), retired persons/military veterans (57,55 percent), farmers/gardeners/fishers, and occupations other than employees, professionals, and entrepreneurs are of concern.
- Education levels are also in parallel with financial literacy, as those who completed university had the highest financial literacy index (88.29 percent), and those who did not enroll in any formal education scored the lowest (51,53 percent).

Moreover, in terms of cybersecurity enforcement, 30 percent of problems in Indonesia's cybersecurity landscape are due to the shortage of cybersecurity experts (Saleh and Winata, 2023). Based on Marwi and Oskar (2023), users may be discouraged from reporting scam cases they have encountered due to the following reasons:

- Lack of understanding of reporting systems
- Unsatisfactory banking hotlines with high phone credit rates
- The feeling of embarrassment and the feeling that the problem could not be resolved. Victims with higher education backgrounds refused to report their cases due to embarrassment.
- The police claimed to update the victims on the case, but there were no further updates from them
- The emphasis on the burden of proof was placed on victims
- Despite having seen warnings of scams, they did not remember them when they encountered similar schemes

RECOMMENDATIONS

To address these challenges, a series of initiatives must be implemented in multiple stages. Ideally, the most effective way to combat scams is by enhancing public literacy and awareness of fraudulent activities. However, this is not an easy task and requires a long-term effort. Given the current low levels of digital literacy in Indonesia, regulators and other stakeholders must focus on proactive measures to tackle scams more effectively. The following are key strategies that should be pursued to bridge the existing policy gaps in Indonesia:

a) **A data sharing mechanism involving relevant stakeholders from the private and public sectors.** When a scam attack occurs on a digital platform, records of the perpetrator *(e.g., the pattern of attack, IP address, identities)* are documented in a collaborative database where other stakeholders, such as e-commerce, banks, the government, and financial technology companies can access. Thus, when a user who matches the identities of the perpetrator is identified in another digital platform, they would not be able to continue creating or using their accounts until further inspections. Although our expert survey reported that members of an e-commerce association have a shared merchant fraud database, a similar mechanism has yet to be implemented by other actors.

   Of course, the data sharing initiative must be conducted in accordance with proper data governance principles, as mandated by the Personal Data Protection Law and robust international best practices. One of the main challenges in implementing data sharing is the existence of confidentiality regulations, particularly in sectors like banking, which make data exchange difficult. Additionally, the absence of implementing regulations for the UU PDP creates further uncertainty regarding the extent to which institutions can share data and whether certain exceptions may be allowed for specific purposes. To effectively combat scams in Indonesia, it is essential to establish a legal framework for data sharing that is specifically designed for fraud prevention. This framework must be built on strong governance principles while prioritizing personal data protection.

b) **The use of AI for scams prevention.** The use of new technologies, such as AI, should also be leveraged to address scams. AI has the potential to analyze suspicious data from scammer behavior across various platforms—whether in messaging apps, phone calls, or digital platforms—enabling early detection of potential scams. This would allow the public to be notified of possible scam threats in real time.

   However, AI and technology are not silver bullet solutions. First, our understanding of AI is still limited, making it challenging to fully map the opportunities and risks associated with its use. Despite the need to encourage the use of AI for this purpose, fundamental principles such as transparency, fairness, accountability, and others must remain a cornerstone of its application. Second, it is also important to first assess existing horizontal regulations and laws whether the current framework sufficiently addresses emerging AI risks. Leveraging existing regulatory and legal frameworks within specific sectors provides an adaptable foundation for AI governance. This approach supports ethical AI development while enabling targeted, effective responses to evolving threats like deepfakes and sophisticated scams.

c) **A single institution designated to surveil, document, and respond to online scam cases.** The existing policy landscape illustrates an unclear division of roles and responsibilities in addressing scams between the government, such as KOMINFO, and the financial regulator, OJK. In simple terms, Indonesia currently has various methods for reporting scams, for instance the one that is under KOMDIGI and OJK. However, the absence of a single designated institution and a clear mechanism creates confusion among the public. Additionally, there are challenges related to the complex and time-consuming reporting procedures. Therefore, there is a need for one unified reporting mechanism that is simple, easy to remember, accessible, and user-friendly, to facilitate the public in reporting scam activities.

d) **Targeting digital literacy interventions to include scam awareness, identification, and reporting.** Established efforts to promote digital literacy lack depth for the public to be equipped with the knowledge and confidence in identifying scams. Other than public awareness campaigns on print and online media, programs leaned more towards onboarding sessions for users to operate digital platforms, such as training merchants to utilize e-commerce applications. To ensure program effectiveness, interventions should prioritize vulnerable populations, such as the older generation and those from a lower socioeconomic background. Furthermore, scam awareness can also be integrated into the formal educational curriculum at all levels, as has been done by OJK to enhance digital literacy.

e) **Expanding multi-level international cooperation.** As online scams operate in the digital space, cases of foreign syndicates and cross-country victims demand multinational cooperation. Collaboration between anti-scam initiatives across countries needs to be expanded, one of which can be achieved by establishing common standards and guidelines for addressing cross-border scams. A unified framework and set of standards are essential, covering areas such as prevention efforts, response to the spread of scams, victim protection, and more, especially considering that the leading institutions overseeing anti-scam initiatives vary by country.

Multilateral cooperation (not just bilateral) is critical because domestic efforts alone will never be effective, particularly since the spread of scams via the internet transcends national jurisdictions. This cooperation should also extend beyond just tackling the spread of scams and victim protection to include the growing concern of human trafficking. It is hoped that multilateral collaboration will increase the effectiveness of governmental efforts in combating scams.

ANNEXES

Annex A. Table of a sample online scam cases targeting individuals in Indonesia

Year	Platform	Scam type	Details	Socioeconomic implications
2016	OLX, Kaskus, Bukalapak, Tokopedia (Sasongko, 2016)	E-commerce scam	Fraudsters created fake online stores, received money from customers, and deleted purchasing history	93 victims were reported, with a loss of Rp 10,1 billion
2016	SMS (Pinrang & Syamsuddin, 2016)	Prize scam	Fraudsters sent randomized text messages to 5.000 phone numbers claiming they won millions of rupiah. Prizes can be redeemed after a specific transfer amount.	For every Rp 10.000 of transactions, one fraudster received Rp 3.000. 3 laptops, 6 cellphones, hundreds of phone cards, and Rp 65 million were confiscated.
2016	Phone call (Amelia, 2016)	Lottery scam	Fraudsters from Jakarta, Surabaya, and China called victims claiming they won money from a lottery. Prizes can be redeemed if they paid Rp 2,6 billion	52 satellite phones, 6 handphones, and 8 laptops were confiscated
2020	Instagram (Luxiana, 2020)	Shopping scam	Four 15-16-year-olds claimed to sell rare and branded items on several Instagram accounts, but have never sent anything after receiving money from customers.	Dozens of victims with a loss of over Rp 100 million.
2022	Online loan platform (BBC, 2022)	Investment scam	A bogus investment scheme promises a 10 percent return on investment every month. The return was only paid on the first month.	331 victims with a loss of Rp 2 million to Rp 10 - Rp 19 million each, and an estimated total loss of Rp 2,1 billion.
2022	Instagram (Tempo, 2022)	Shopping and impersonation scam	A fraudster impersonating Indonesia's Customs Office contacted victims claiming an online purchase was illegal, forging documents, and demanding payments.	A total loss of Rp 11.5 million for one victim and Rp 8.1 million for another.
2024	E-commerce (Syafaruddin, 2024)	Dropshipping scam	A fraudster posted a dropshipping ad, luring the victim to pay for a 'warehouse'. When there was an expensive order, they offered her a 40% loan. The victim was tricked into believing the business was profitable, and she was blocked from withdrawing her money from the fake e-commerce site.	A total loss of Rp 115 million for the victim.

2024	INDODAX, Cryptocurrency platform (Greig, 2024)	Cryptocurrency fraud	Fraud under the name of INDODAX; sending out refund invitations or personal requests in the platform, which has 5 million users.	At least US $230 million worth of cryptocurrency was lost
2024	Instagram (Setiawati, 2024)	Romance and impersonation scam	Fraudsters approached victims on Instagram; in one case posed as an oil and gas engineer in Papua, claiming their salary was withheld and had a heart attack with fake medical bills and funeral costs. Victims were contacted by fake 'friends' to continue the fraud.	The largest loss was recorded by a single parent of over 50 years old with Rp 600 million, while others lost millions to hundreds of millions of rupiah.
2024	WhatsApp (CNN, 2024)	Malware	Fraudsters sent an application scam (.apk file) disguised as a letter from the regional police via WhatsApp. Once clicked, hackers can access the victim's SMS, allowing them to steal OTP codes and drain bank accounts.	Undisclosed
2025	Dating application (The Jakarta Post, 2025)	Romance, investment, cryptocurrency scam	Gambir police arrested 20 suspects, headed by a Chinese national were suspected of creating fake identities to lure mostly women foreigners to invest in fraudulent cryptocurrency scams.	The operation's leaders earned Rp 7 million, while scammers earned Rp 5 million

Annex B. Table of a sample online scam cases targeting organizations in Indonesia

Year	Organization	Scam type	# of data affected	Socioeconomic implications
2013	Garuda Indonesia (Panji, 2013)	Data theft	<20 credit card records	Undisclosed
2013	PT. Bumi Resources Tbk (BUMI) (detikFinance, 2013)	Data breach (Trojan virus)	All data from 3 computers (1,5 terabytes)	Undisclosed
2015	Mandiri Bank (Heriyanto, 2015)	Malware	Undisclosed, one claimed losing up to Rp 13 million	Undisclosed
2017	Tiket.com (CNN, 2017)	Data theft	Undisclosed; 4 syndicates successfully hacked 400 other sites	Loss of Rp 1,9 billion
2020	Tokopedia (Mulia, 2020)	Data theft	91 milion user records	Sold for US$ 5.000 on the dark web
2020	Kreditplus (Clinten & Yusuf, 2020)	Data theft	890 thousand records for 78 MB of data	Sold for about Rp 50.000 on the dark web
2021	Indonesia's Healthcare and Social Security Agency (BPJS Kesehatan) (Mulia, 2021)	Data theft	279 million records	Undisclosed

2022	Bank Indonesia (CISO MAG, 2022)	Ransomware	Undisclosed; mitigation measures were undertaken and had no impact on critical data	Undisclosed
2023	Directorate General of Immigration (Hope, 2023)	Data theft	34 million passport records	Undisclosed
2023	Bank Syariah Indonesia (BSI) (The Cyber Express, 2023)	Ransomware	1.5 terabytes of data; over 15 million customers and employees	Data was released due to failure to meet the ransom demand of US$ 20 million
2024	Taxpayer Identification Numbers (NPWP) (Dinilhag, 2024)	Data theft	6 milion taxpayer records	Sold for US$ 10.000 on the dark web
2024	National Data Centre Ransomware Attack (PDNS) (Reuters, 2024)	Ransomware	Disrupted 160 government agencies, including immigration and airport operations	US$ 8 million to unlock encrypted data, but later apologized and decrypted data without payment
2024	General Elections Commission (KPU) (Paganini, 2024)	Data theft	252 million voter records	Sold for US$ 74.000 or 2 bitcoins

Annex C. Table of a sample online scams using AI technology in Indonesia

Year	Platform	Scam type	Details	Socioeconomic implications
2023	E-commerce (Expert Survey)	Deepfake	Fraudsters used deepfake images and videos to impersonate real sellers or executives	Financial losses: Chargebacks and refunds, revenue loss, additional operational costs for security measures, legal fees, and investigation Non-financial losses: Reputation damage, regulatory and compliance risks
2024	Various online platforms (CNN, 2024)	Deepfake	A deepfake clip of Indonesian public figures, such as Najwa Shihab, Raffi Ahmad, and Atta Halilintar promoting online gambling sites circulated the internet.	Undisclosed
2024	WhatsApp (Fernando, 2024)	Voice cloning	A victim claimed receiving a text and phone call from someone he thought was his close friend. He did not suspect anything as it sounded exactly like him. The fraudster offered cheap auction items (e.g., iPhone, Canon camera, electronics) for Rp 10 million, encouraging him that it could be sold for a more expensive price.	No financial losses were incurred; the victim rechecked with their friend and found their WhatsApp status warning that there have been scam incidents under the guise of their name.
2025	WhatsApp (France 24, 2025; Tempo, 2025)	Deepfake	A deepfake clip of the Indonesian president, Prabowo Subianto, uttering *“Who hasn’t received aid from me? What are your needs right now?”*, was circulated with a WhatsApp number attached. Victims were asked to transfer Rp 250 thousand to Rp 1 million as an “administrative fee” to redeem the ‘aid’.	100 people were scammed from 20 provinces. A suspect pocketed Rp 65 million from the scam.
2025	Social media	Deepfake	A deepfake clip of Indonesian public figures, such as the vice president, Gibran Rakabuming Raka, and the	A loss of approximately Rp 30 million in the last 4 months.

	(CNN, 2025)		finance minister Sri Mulyani offering financial aid for citizens in need, with a phone number attached as a 'call center.' Victims were asked to fill in a registration form with an administration fee.	
2025	WhatsApp (Aprilia, 2025)	Voice cloning	A victim received a phone call from someone they thought was their friend, with the possibility of voice cloning.	No financial losses were incurred; the victim rechecked with their friend and found that the same incident had happened to three other people.
2025	Digital payment system (Expert Survey)	Not specified	A fraudster might have used AI to replicate identities	Fraudsters did not repay the financial damages, and the platform was reported to the police

Annex D. Table of a sample of private sector initiatives to prevent online scams

Sectors	Company	Initiative
Digital financial services	Dana	Dana joins the Global Anti-Scam Alliance (GASA) (2025): This collaboration gains Dana access to a global network of experts to enhance fraud prevention with AI-powered detection and cybersecurity innovation, among others.
E-commerce	Shopee	Shopee Guarantee (2024): A product can be labeled '100% Original' when it meets specific criteria; the label can only be declared by the Shopee team to protect users from shopping fraud.
E-commerce	Blibli	Partnership with Vesta (2023): Blibli hired Vesta, a US-based transaction guarantee platform that uses machine learning, AI, and global data to protect Blibli's card-not-present (CNP) transactions, eliminating the risk of chargebacks, and an enhanced fraud management system.
Bank	Bank Central Asia	Don't Know? Say No! (2023): Campaign to raise awareness of banking fraud, featuring a public figure in the entertainment industry with more than 8 million views on YouTube.
E-commerce	Tokopedia	Penalty System: Merchants that manipulate transactions, reviews, and products sold to enhance their shop's reputation, misuse promos for personal matters, the use bots can be given penalties, such as a permanent account/store closure, withdrawal of subsidies, or a deduction of balances from the Merchant.
E-commerce, ride-hailing, fintech	Grab, Ovo, Link Aja	GrabDefence: Provides access to a full suite of tools, technologies, and intelligence that are tried and tested in millions of data points for real-time protection against fraud and financial crime through 3 steps: 1. Provides a set of APIs for tools enabling data collection, data preparation, and tool integration. 2. Applies a combination of risk rules and machine learning algorithms at key checkpoints of the user's journey to instill protection. 3. Iteratively managing risks through continuous monitoring, experimentation, and fine-tuning.

E-commerce, ride-hailing, fintech	Go-jek	JARVIS (2018): A tool to automate manual data retrieval and basic analysis. What used to take a human analyst 30 minutes now takes 3 seconds to prevent fraud at scale and speed.
Telco industry	Telkomsel, Indosat, XL, Smartfren	Open Gateway initiatives to improve more robust authentication, detects SIM swap service, detect potential fraud from GPS manipulations.

REFERENCES

6,800 Indonesians involved in online fraud overseas: Govt. (2025, February 21). Antara News. https://en.antaranews.com/news/345845/6800-indonesians-involved-in-online-fraud-overseas-govt

Amanta, F. (2022, July 6). *Unpacking Indonesia's Digital Accessibility*. CIPS | Think Tank. https://www.cips-indonesia.org/post/opinion-unpacking-indonesia-s-digital-accessibility

ASEAN-Australia Counter Trafficking. (2024, May). *Human Trafficking & Forced Labour in Cambodia's Cyber-Scam Industry*. https://www.aseanact.org/wp-content/uploads/2024/05/202405-LSCW-Cyber-scams-and-HT-report-design-1.pdf

Assessing the Digital Financial Threat Landscape in Indonesia. (2022, April). https://www.unodc.org/roseap/en/what-we-do/anti-corruption/topics/2022/03-assessing-digital-financial-threat-landscape-indonesia.html

Badan Pengembangan Sumber Daya Manusia Komunikasi dan Digital. (2024). *Indeks Masyarakat Digital Indonesia 2024*. https://imdi.sdmdigital.id/publikasi/02122024_Buku%20IMDI_BAB%201-5_V6_compressed.pdf

Badan Pengkajian dan Penerapan Teknologi. (2020). *Strategi Nasional Kecerdasan Artifisial Indonesia 2020—2045*. https://ai-innovation.id/images/gallery/ebook/stranas-ka.pdf#page=1

Bank Syariah Indonesia Cyber Attack: LockBit Demands $20m Ransom. (2023, May 16). https://thecyberexpress.com/lockbit-bank-syariah-indonesia-cyber-attack/

Begini Cara Hacker Bobol Situs Tiket.com. (2017, March 31). CNN Indonesia. https://www.cnnindonesia.com/teknologi/20170331145137-185-204065/begini-cara-hacker-bobol-situs-tiketcom

CISOMAG. (2022, January 21). Bank Indonesia Suffers Ransomware Attack, Suspects Conti Involvement. *CISO MAG | Cyber Security Magazine*. https://cisomag.com/bank-indonesia-suffers-ransomware-attack-suspects-conti-involvement/

DANA Indonesia. (2025, February). *DANA Joins GASA*. https://www.linkedin.com/posts/dana-indonesia_dana-joins-gasa-activity-7307355028527140865-Z_pa/

Edy, S., Gunawan, W., & Wijanarko, B. D. (2017). Analysing the trends of cyber attacks: Case study in Indonesia during period 2013-Early 2017. *2017 International Conference on Innovative and Creative Information Technology (ICITech)*, 1–6. https://doi.org/10.1109/INNOCIT.2017.8319146

Email Perusahaan Tambang Bakrie Kena Hack, Seluruh Data Dicuri. (2013, February 12). detikfinance. https://finance.detik.com/bursa-dan-valas/d-2168234/email-perusahaan-tambang-bakrie-kena-hack-seluruh-data-dicuri

Fadillah, T. (2023). *E-Commerce: A New Media that Creates New Disasters*. OSF. https://doi.org/10.31219/osf.io/hpb6w

FICO. (2023). *Consumer Survey 2023—Digital banking, customer preferences, and fraud controls*. Retrieved April 17, 2025, from https://www.fico.com/en/latest-thinking/ebook/consumer-survey-2023-digital-banking-customer-preferences-and-fraud-controls

Forrester. (2022). *Staying Ahead Of The Fight Against Fraud In Southeast Asia (SEA)*. https://assets.grab.com/wp-content/uploads/sites/4/2022/02/22102958/Forrester_Staying_Ahead_Of_The_Fight_Against_Fraud_SEA.pdf

Fraud, Scam and Fincrime Detection, Digital Risk Security Solutions | GrabDefence. (n.d.). Retrieved April 17, 2025, from https://defence.grab.com/

Greig, J. (2024, September 13). *Largest crypto exchange in Indonesia pledges to reimburse users after $22 million theft*. https://therecord.media/indodax-crypto-exchange-pledges-to-reimburse-after-theft?utm_source=chatgpt.com

Harwanto, F., Febriansyah, A., & Irwantika, N. (2024). *Cryptocurrency, Crime, And Children: Unveiling The Dark Side of Financial Technology in Child Sexual Exploitation*. 29–35. https://doi.org/10.2991/978-2-38476-325-2_4

Hasibuan, E. S. (2023). The Police are Indecisive: Online Gambling is Rising. Facts about the Eradication of Online Gambling in the Field. *Journal of Social Research*, *2*(10), 3365–3370. https://doi.org/10.55324/josr.v2i10.1405

Heriyanto, T. (n.d.). *Selain BCA, Nasabah Mandiri Juga Kena Malware Pencuri Uang*. teknologi. Retrieved April 17, 2025, from https://www.cnnindonesia.com/teknologi/20150306104201-185-37163/selain-bca-nasabah-mandiri-juga-kena-malware-pencuri-uang

Herman, A. D. (n.d.). *6 Million Taxpayer IDs, Including President's, Allegedly Leaked and Sold for $10,000*. Jakarta Globe. Retrieved April 17, 2025, from https://jakartaglobe.id/news/6-million-taxpayer-ids-including-presidents-allegedly-leaked-and-sold-for-10000

Hope, A. (2023, July 13). 34 million Indonesian Passports Exposed in a Massive Immigration Directorate Data Breach. *CPO Magazine*. https://www.cpomagazine.com/cyber-security/34-million-indonesian-passports-exposed-in-a-massive-immigration-directorate-data-breach/

Indonesia Anti-Phishing Data Exchange. (2024). *Laporan Aktivitas Abuse Domain .ID*. https://api.idadx.id/documents/uploads/1724725529_Laporan%20Q2%202024.pdf.pdf

Indonesian ecommerce platform Blibli hires Vesta for payments security. (2023, January 24). https://thepaypers.com/digital-identity-security-online-fraud/indonesian-ecommerce-platform-blibli-hires-vesta-for-payments-security--1259990

IOM UN Migration. (n.d.). *Information on Forced Labor and Trafficking in Persons (TIP)—Indicated Cases in Online Scamming Industry Overseas*. https://indonesia.iom.int/sites/g/files/tmzbdl1491/files/documents/2023-08/infosheet-online-scams-english.pdf

IOM UN Migration. (2024, February). *IOM's Regional Situation Report on Trafficking in Persons into Forced Criminality in Online Scamming Centres in Southeast Asia.* https://roasiapacific.iom.int/sites/g/files/tmzbdl671/files/documents/2024-02/iom-southeast-asia-trafficking-for-forced-criminality-update_december-2023.pdf

Juditha, C. (2015). *Pola Komunikasi Dalam Cybercrime (Kasus Love Scams)*. *6*(2). https://media.neliti.com/media/publications/122582-ID-none.pdf

Junaedi, J. (2024). England is the Largest Center for Online Gambling Activity in the World, Versus Indonesia is Exposed to Online Gambling Emergency Stage Five. *International Journal of Law, Crime and Justice*, *1*(3), 100–114. https://doi.org/10.62951/ijlcj.v1i3.134

Khan, M. A. (2024). Understanding the Impact of Artificial Intelligence (AI) on Traditional Businesses in Indonesia. *Journal of Management Studies and Development*, *3*(02), Article 02. https://doi.org/10.56741/jmsd.v3i02.584

Kristanto, K., Ismail, K., Fransisco, F., & Ronaldi, R. (2024). *Criminal Liability of Child Sexual Exploitation Perpetrators Using Social Engineering Techniques Through Digital Wallets in Indonesia*. 20–28. https://doi.org/10.2991/978-2-38476-325-2_3

Kurni, N., Rahayu, Wendratama, E., Monggilo, Z., Damayanti, A., Angendari, D. A., Abisono, F., Shafira, I., & Desmalinda. (2022). *Penipuan Digital di Indonesia*. https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2022/08/PDF-Monograf-Penipuan-Digital-di-Indonesia-Modus-Medium-dan-Rekomendasi.pdf

Law of the Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions. https://www.icnl.org/wp-content/uploads/Indonesia_elec.pdf

Lindquist, J. (2018). Illicit economies of the internet: Click farming in Indonesia and beyond. *Made in China Journal*, *3*(4), 88–91. https://doi.org/10.3316/informit.035564674568222

Luxiana, K. M. (n.d.). *Puluhan Orang Korban Penipuan Online Sindikat Bocah SMP Rugi Rp 100 Juta*. detiknews. Retrieved April 17, 2025, from https://news.detik.com/berita/d-5178941/puluhan-orang-korban-penipuan-online-sindikat-bocah-smp-rugi-rp-100-juta

Maghfirah, F., & Husna, F. (2022). CYBER CRIME AND PRIVACY RIGHT VIOLATION CASES OF ONLINE LOANS IN INDONESIA. *PROCEEDINGS: Dirundeng International Conference on Islamic Studies*, 1–18. https://doi.org/10.47498/dicis.v1i1.1009

Marwi, H., & Oskar, I. (2023). Analysis Of Increasing Types Of Online Fraud And Level Of Public Awareness In Indonesia. *Journal of Embedded Systems, Security and Intelligent Systems*, 70–84. https://doi.org/10.59562/jessi.v4i2.722

Media, K. C. (2013, November 21). *Situs Webnya Diserang, Ini Penjelasan Garuda Indonesia*. KOMPAS.com. https://tekno.kompas.com/read/xml/2013/11/21/1724512/Situs.Webnya.Diserang.Ini.Penjelasan.Garuda.Indonesia

Media, K. C. (2016, February 13). *Tujuh Pelaku Penipuan via SMS Dibekuk, Salah Satunya Pegawai Bank*. KOMPAS.com. https://regional.kompas.com/read/xml/2016/02/13/11585501/Tujuh.Pelaku.Penipuan.via.SMS.Dibekuk.Salah.Satunya.Pegawai.Bank

Media, K. C. (2020, August 4). *Data Ratusan Ribu Nasabah Kredit Plus Diduga Bocor dan Dijual di Internet*. KOMPAS.com. https://tekno.kompas.com/read/2020/08/04/07150007/data-ratusan-ribu-nasabah-kredit-plus-diduga-bocor-dan-dijual-di-internet

Mulia, K. (2020, May 6). *What can we learn from Tokopedia's alleged 91-million data leak?* KrASIA. https://kr-asia.com/what-can-we-learn-from-tokopedias-alleged-91-million-data-leak

Mulia, K. (2021, June 15). *Indonesians' personal information is up for sale. Who's buying?* KrASIA. https://kr-asia.com/indonesians-personal-information-is-up-for-sale-whos-buying

Naibaho, R. (2025, March 29). *5 Fakta Bareskrim Bongkar Kasus Scam Kripto Internasional Rp 105 Miliar*. https://news.detik.com/berita/d-7832118/5-fakta-bareskrim-bongkar-kasus-scam-kripto-internasional-rp-105-miliar

Niman, S., Parulian, T. S., & Rothhaar, T. (2023). Online love fraud and the experiences of indonesian women: A qualitative study. *International Journal of Public Health Science (IJPHS)*, *12*(3), 1200. https://doi.org/10.11591/ijphs.v12i3.22617

Novianty, D. (2025, March 10). *Riset: Lebih dari 500 Ribu Serangan Phishing pada Bisnis di Asia Tenggara 2024, Indonesia Nomor Dua di Asia Tenggara*. https://www.suara.com/tekno/2025/03/10/110259/riset-lebih-dari-500-ribu-serangan-phishing-pada-bisnis-di-asia-tenggara-2024-indonesia-nomor-dua-di-asia-tenggara

Otoritas Jasa Keuangan. (2024, August 2). *Joint Press Release: OJK And Statistics Indonesia Present National Survey On Financial Literacy And Inclusion 2024 Findings*. https://ojk.go.id/en/berita-dan-kegiatan/siaran-pers/Pages/OJK-And-Statistics-Indonesia-Present-National-Survey-On-Financial-Literacy-And-Inclusion-2024-Findings.aspx

Paganini, P. (2024, January 12). Vast Voter Data Leaks Cast Shadow Over Indonesia 's 2024 Presidential Election. *Security Affairs*. https://securityaffairs.com/157357/deep-web/hackers-data-leak-indonesia-elections.html

Paramitha, D. D. (2022, Desember | 20.15 WIB). *Cerita Kasus Penipuan Berkedok Bea Cukai, Beli Barang via Medsos Berujung Pemerasan | tempo.co*. Tempo. https://www.tempo.co/ekonomi/cerita-kasus-penipuan-berkedok-bea-cukai-beli-barang-via-medsos-berujung-pemerasan-236913

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020. (n.d.). Retrieved April 17, 2025, from https://jdih.komdigi.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020

Peraturan OJK No. 12 Tahun 2024. (n.d.). Database Peraturan | JDIH BPK. Retrieved April 17, 2025, from http://peraturan.bpk.go.id/Details/301737/peraturan-ojk-no-12-tahun-2024

Post, T. J. (n.d.). *Gambir Police nab 20 suspects in love scam targeting foreigners—Jakarta*. The Jakarta Post. Retrieved April 17, 2025, from https://www.thejakartapost.com/indonesia/2025/01/29/gambir-police-nab-20-suspects-in-love-scam-targeting-foreigners.html

Prabowo, H. Y. (2023). When gullibility becomes us: Exploring the cultural roots of Indonesians' susceptibility to investment fraud. *Journal of Financial Crime*, *31*(1), 14–32. https://doi.org/10.1108/JFC-11-2022-0271

Putra, F. H., Suhardjanto, D., Trinugroho, I., & Arifin, T. (2024). Overcoming Barriers to Inclusion: The Role of Financial Literacy and Digital Divide in Expanding Financial Access in Indonesia. *Journal of Ecohumanism*, *3*(8), Article 8. https://doi.org/10.62754/joe.v3i8.5608

R, M. A. (2016, February 1). *Polda Metro Bekuk Sindikat Penipuan Online Jaringan China di Surabaya*. detiknews. Retrieved April 17, 2025, from https://news.detik.com/berita/d-3132271/polda-metro-bekuk-sindikat-penipuan-online-jaringan-china-di-surabaya

Ratusan mahasiswa IPB jadi korban penipuan, kini diteror penagih pinjol—'Sudah jatuh, tertimpa tangga'. (2022, November 17). BBC News Indonesia. https://www.bbc.com/indonesia/articles/c165dj3lzl2o

Redaksi, T. (2025, March 11). Dominasi Korban Penipuan Online Adalah Perempuan Selama Tahun 2022. *BaliNews.Id*. https://balinews.id/dominasi-korban-penipuan-online-adalah-perempuan-selama-tahun-2022/

Saleh, A. I., & Winata, M. D. (2023). *Indonesia's Cyber Security Strategy: Problems and Challenges*. 1675–1696. https://doi.org/10.2991/978-2-38476-152-4_169

Saleh, G. (2022). JURIDICAL ANALYSIS OF THE CRIME OF ONLINE STORE FRAUD IN INDONESIA. *Jurnal Hukum Dan Peradilan*, *11*(1), Article 1. https://doi.org/10.25216/jhp.11.1.2022.151-175

Sasongko, J. P. (2016, February 22). *Polisi Tangkap Kelompok Penipu Jual-Beli Online*. nasional. Retrieved April 17, 2025, from https://www.cnnindonesia.com/nasional/20160222161552-12-112638/polisi-tangkap-kelompok-penipu-jual-beli-online

Setiawati, S. (2024, September 28). *Uang Kandas, Cinta Pun Melayang: Love Scamming Buat Rugi Rp600 Juta!* CNBC Indonesia. Retrieved April 17, 2025, from https://www.cnbcindonesia.com/research/20240922174024-128-573665/uang-kandas-cinta-pun-melayang-love-scamming-buat-rugi-rp600-juta

Shaw, K. (2023, December 13). Bank Central Asia says "Don't Know? Say No!" in new FCN Creative - Flock campaign. *Campaign Brief Asia*. https://campaignbriefasia.com/2023/12/13/bank-central-asia-says-dont-know-say-no-in-new-fcn-creative-flock-campaign/

Shofa, J. N., & Muslim, A. (2024, October 15). *Indonesia's Internet Users More than Double Over Past Decade*. Jakarta Globe. https://jakartaglobe.id/tech/indonesias-internet-users-more-than-double-over-past-decade

Sistem Penalti Pelanggaran Ketentuan Transaksi. (n.d.). Tokopedia Care. Retrieved April 17, 2025, from https://www.tokopedia.com/help/article/apa-itu-sistem-penalti-pelanggaran-ketentuan-transaksi

Syafaruddin, M. (2024, June 20). *Perempuan Asal Surabaya Jadi Korban Penipuan Online, Rp115 Juta Melayang*. https://www.suarasurabaya.net/kelanakota/2024/perempuan-asal-surabaya-jadi-korban-penipuan-online-rp115-juta-melayang/

Tentang Kami—IASC. (n.d.). Retrieved April 17, 2025, from https://iasc.ojk.go.id/about-us

Tentang Shopee Garansi 100% Ori dan Keuntungannya | Pusat Edukasi Penjual Shopee Indonesia. (n.d.). Retrieved April 17, 2025, from https://seller.shopee.co.id/edu/article/6840

Teresia, A. (2024, July 12). Indonesia says it has begun recovering data after major ransomware attack. *Reuters*. https://www.reuters.com/technology/cybersecurity/indonesia-says-it-has-begun-recovering-data-after-major-ransomware-attack-2024-07-12/

UNODC. (2023). *Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia*. https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf

UU No. 1 Tahun 2024. (n.d.). Database Peraturan | JDIH BPK. Retrieved April 17, 2025, from http://peraturan.bpk.go.id/details/274494/uu-no-1-tahun-2024

Viral Penipuan Modus File APK "Surat Panggilan Polda Metro Jaya." (2024, April 10). https://www.cnnindonesia.com/teknologi/20240410151720-185-1085028/viral-penipuan-modus-file-apk-surat-panggilan-polda-metro-jaya

Watters, P. (2024). *Exposing the Dark Side: Scams and Cybersecurity Risks in Indonesia's Illicit Sports Streaming Scene* (SSRN Scholarly Paper 4954969). Social Science Research Network. https://doi.org/10.2139/ssrn.4954969

Yulia, R., & Sofian, A. (2024). *E-Wallet Misuse in Online Child Prostitution Transactions; How Does Indonesian Law Respond?* 36–43. https://doi.org/10.2991/978-2-38476-325-2_5

Yusriadi, Y., Rusnaedi, R., Siregar, N. A., Megawati, S., & Sakkir, G. (2023). Implementation of artificial intelligence in Indonesia. *International Journal of Data and Network Science*, *7*(1), 283–294. https://doi.org/10.5267/j.ijdns.2022.10.005

Zhu, N. (2018, June 18). *A day in the life of Go-Jek's VP of fraud*. Tech in Asia. https://www.techinasia.com/talk/day-life-vp-fraud-gojek

Safer Internet Lab

saferinternetlab.org

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

Find Us On

CSIS Indonesia | Safer Internet Lab