

**Research report**

# Online Fraud and Scams in Thailand

---

Safer Internet Lab

# Online Fraud and Scams in Thailand

Dr. Saliltorn Thongmeensuk<sup>1</sup>

## PATTERNS AND TRENDS

Online fraud and scams have become a significant issue in Thailand's digital landscape. According to the Cyber Crime Investigation Bureau, approximately 700 cases of online fraud and scams are reported daily<sup>2</sup>. These crimes are carried out using various methods. Statistics from the Anti-Online Scam Operation Center (AOC 1441) reveal that between 2024 and 2025, the five major online fraud cases resulted in a combined total loss of \$610,000. Scammers employed different tactics to deceive victims, including fraudulent social media posts or messages, misleading online platform advertisements, fake job offers, and deceptive phone messages. These approaches exploit social media platforms and digital communication channels to manipulate individuals into financial losses, highlighting the urgent need for stricter online security measures and public awareness campaigns.

Moreover, data from the Global Anti-Scam Alliance's survey indicates that in 2024, scammers primarily used scam calls, text messages, social media, and online advertisements to target victims. Additionally, with the rise of AI-powered text generation, a majority of survey participants reported that more than half of the scam messages they received appeared to be AI-generated, making them more sophisticated and difficult to detect. The survey also revealed an increasing trend in identity theft, where scammers impersonate government officials or law enforcement officers to manipulate victims into providing sensitive information or making fraudulent payments.<sup>3</sup>

The growing trend of identity theft has become even more alarming with the emergence of AI-assisted identity fraud, which significantly enhances the sophistication of these crimes. In February 2025, a notable case of AI-assisted identity theft occurred, where scammers used AI-powered face-altering technology during video calls to make their deception more convincing. This scheme successfully tricked 163 victims, including a well-known influencer who suffered a financial loss of over four million baht<sup>4</sup>. Another shocking incident took place in January 2025, involving an AI-assisted scam call targeting Paetongtarn Shinawatra, the current Prime Minister of Thailand. In this case, scammers attempted to extort money by impersonating a well-known world leader using AI-generated voice cloning technology. However, Paetongtarn became suspicious of the voice's authenticity and did not

---

<sup>1</sup> Senior Research Fellow, Thailand Development Research Institute (TDRI)

<sup>2</sup> Siam Legal, *What is Thailand's Anti-Online Scam Operation Center?*, accessed February 28, 2025, <https://library.siam-legal.com/what-is-thailands-anti-online-scam-operation-center/>.

<sup>3</sup> *Nation Thailand*, "Govt sets up scam victim aid," December 26, 2024, <https://www.nationthailand.com/news/general/40042159>.

<sup>4</sup> *Bangkok Post*, "Two Men Arrested for Alleged B4M AI-Aided Scam Against Beauty Queen," January 15, 2025, <https://www.bangkokpost.com/thailand/general/2953450/two-men-arrested-for-alleged-b4m-ai-aided-scam-against-beauty-queen>.

fall victim to the scam. Despite avoiding the trap, the prime minister later stated that the AI-generated voice was highly convincing, highlighting the growing threat posed by advanced deepfake technology in cybercrime.<sup>5</sup>

Another infamous case reported by the researchers from cyber security firm – Group-IB - is when the group of hackers -GoldFactory- try to use facial recognition AI to steal money from the victim. In 2023, the group of hackers uploaded the application called “Digital Pension”, masked as a legitimate service. The application requires the victims to record the video to access the pension, then the fraudster will use facial recognition AI to record the face of the victim and use face swap AI solution to create a deepfake video<sup>6</sup>. This pattern emerged when the Bank of Thailand mandated that any digital money transfer exceeding 50,000 baht per transaction, or daily transfers surpassing 200,000 baht, require biometric authentication, specifically facial recognition, to verify the account owner's identity. This policy aimed to bolster security for high-value transactions to combat online fraud and scam<sup>7</sup>, but with exploitation of AI technology the fraudster can easily overcome this measure.

These incidents raise significant concerns about the increasing volume and sophistication of online fraud and scams, as artificial intelligence is being exploited to enhance deception. With AI-powered scams becoming more convincing, fraudsters can now manipulate voices, videos, and messages with alarming accuracy, making it increasingly difficult for victims to distinguish between legitimate and fraudulent interactions.

The rapid evolution of AI-driven cybercrime underscores the urgent need for government intervention. Authorities must implement stricter regulations, enhance cybersecurity measures, and invest in AI-driven fraud detection technologies to combat this growing threat. Additionally, public awareness campaigns, digital literacy programs, and cross-border cooperation are essential to protect individuals from falling victim to these increasingly sophisticated scams. Without proactive action, the risk of financial and personal losses due to AI-assisted fraud will continue to escalate.

## KEY STAKEHOLDERS IDENTIFICATION IN ADDRESSING ONLINE FRAUD AND SCAMS

The issue of online fraud and scams in Thailand involves multiple stakeholders, each playing a critical role in prevention, enforcement, and victim assistance. However, while existing initiatives have proven effective in mitigating fraud, challenges remain in proactively addressing emerging threats, particularly AI-enabled scams.

---

<sup>5</sup> *Nation Thailand*, "Govt to Step Up Online Scam Crackdown," February 4, 2025, <https://www.nationthailand.com/news/general/40045195>.

<sup>6</sup> Group-IB, "GoldFactory iOS Trojan," accessed February 28, 2025, <https://www.group-ib.com/blog/goldfactory-ios-trojan/>.

<sup>7</sup> Bank of Thailand (BoT), "Bank of Thailand Implements New Cybersecurity Measures," March 9, 2023, <https://www.bot.or.th/en/news-and-media/news/news-20230309.html>.

## Ministry of Digital Economy and Society (MDES)

As the primary coordinating body in the fight against online fraud, the Ministry of Digital Economy and Society (MDES) has taken a central role in policy formulation, enforcement coordination, and technological innovation. MDES has established collaborations with multiple agencies, including:

- **The Royal Thai Police's Cyber Crime Investigation Bureau** – responsible for investigating and prosecuting cybercriminals.
- **The Anti-Money Laundering Office (AMLO)** – tracks illicit financial flows linked to scam networks.
- **The Bank of Thailand (BoT) and the Thai Bankers Association** – oversee fraud prevention measures within the banking sector.
- **The Department of Special Investigation (DSI) and the Securities and Exchange Commission (SEC)** – target financial fraud, investment scams, and cyber-enabled crime.
- **The National Broadcasting and Telecommunications Commission (NBTC)** – regulates telecommunication networks, focusing on scam calls, SMS fraud, and telecom-related cybercrime.

Recognizing the need for a centralized and rapid response mechanism, MDES, in partnership with these organizations, established the Anti-Online Scam Operation Center (AOC 1441). The AOC serves as a one-stop service to combat online scams, allowing victims to report fraudulent activities and enabling immediate intervention through a 24/7 hotline (1441).

While AOC 1441 has significantly improved victim support and scam mitigation, it remains a reactive measure—primarily remedying fraud after it occurs rather than preventing scams in advance. This limitation has led MDES to develop more proactive fraud detection solutions.

To enhance prevention-oriented approach, MDES is developing the DE-fence platform, set to launch in late 2025. This initiative aims to detect fraudulent patterns before scams occur, using artificial intelligence (AI) and big data analytics to monitor and analyze suspicious financial activities, scam websites, and digital transaction behaviors.

The DE-fence system will integrate with AOC 1441, expanding its role from reactive intervention to real-time scam detection and prevention. Key expected capabilities include:

- Automated fraud detection – leveraging AI to flag scam patterns in real-time.
- Telecom and banking fraud surveillance – identifying suspicious SIM registrations and fraudulent transactions.



- Predictive threat modeling – analyzing emerging scam tactics to inform regulatory responses.

### **The Bank of Thailand (BoT) and Its Role in Fraud Prevention**

As the primary financial regulator, the Bank of Thailand (BoT) has been instrumental in mandating security policies for commercial banks to minimize fraud risks. Given that the banking sector accounts for a majority of online financial fraud cases, BoT has introduced several countermeasures, including:

1. **Mandatory Multi-Factor Authentication for High-Value Transactions**
  - o In mid-2023, the BoT required facial recognition or fingerprint authentication for transactions exceeding 50,000 THB per transfer or 200,000 THB per day. The measure was introduced to prevent unauthorized transactions and account takeovers.
2. **Continuous Adaptation to Emerging Fraud Patterns**
  - o BoT acknowledges that online financial fraud evolves rapidly—when regulations are enforced, scam activities decrease temporarily before criminals adapt with new tactics. To counter this, BoT has actively updated banking security frameworks, including guidelines for commercial banks on digital fraud prevention and investment in AI-driven security tools. In addition, BoT has encouraged financial institutions to strengthen biometric verification systems against AI-based identity fraud.
3. **Cross-Sector Collaboration to Combat Scams**
  - o BoT also works closely with MDES, law enforcement agencies, and commercial banks to formulate fraud mitigation strategies. It has also emphasized cross-border intelligence sharing to tackle transnational fraud networks.

### **Thai Bankers Association (TBA) and the Central Fraud Registry (CFR)**

Recognizing the importance of tracking financial crime across multiple institutions, the Thai Bankers Association (TBA) launched the Central Fraud Registry (CFR) in mid-2024. This initiative aims to track and eliminate mule bank accounts used for money laundering and scam operations.

### **Commercial Banks and E-Payment Platforms**

Commercial banks and e-payment service providers play a critical role in fraud prevention, transaction monitoring, and risk assessment. Under BoT's directives, financial institutions are:

- Required to implement transaction monitoring systems capable of detecting and freezing suspicious activities in real-time.

- Obligated to freeze accounts linked to fraudulent transactions and report them to the Central Fraud Registry.
- Encouraged to invest in AI-driven fraud detection to combat deepfake-assisted identity theft and AI-powered phishing scams.

## Telecommunications Sector and the Role of NBTC

Given that many online fraud schemes originate from scam calls and fraudulent SMS messages, the National Broadcasting and Telecommunications Commission (NBTC) has implemented:

- Restrictions on bulk SIM card registrations to prevent scammers from using untraceable phone numbers.
- Telecom providers are obliged to block known scam numbers and filter fraudulent messages before reaching consumers.
- Collaboration with law enforcement to track down illegal call centers, many of which operate from neighboring countries.

## POLICY OVERVIEW

### Anti-Online Scam Operation Center

The most recent government policy to combat online fraud and scams was introduced in 2023, when the Ministry of Digital Economy and Society (MDES), in collaboration with various public and private sector organizations, established the Anti-Online Scam Operation Center (AOC 1441). This initiative serves as a one-stop service designed to combat online scams using an AI-assisted platform capable of analyzing scam patterns, identifying fraudsters, and swiftly taking down their bank accounts.<sup>8</sup>

The online fraud and scam often involve several agencies to tackle the case effectively, the victim will need to contact several agencies, fill several documents and wait for months to conclude the case. However, the AOC was established from the collaboration of all the responsible agency, namely MDES (which oversees the center), the Royal Thai Police's cybercrime units, the Anti-Money Laundering Office (AMLO), the Bank of Thailand and Thai Bankers Association, the Department of Special Investigation (DSI), the Securities and Exchange Commission (SEC), and the National Broadcasting and Telecommunications Commission (NBTC)<sup>9</sup>, thus considerably shorten the time needed to tackle the case from days to within an hour.

<sup>8</sup> Ministry of Digital Economy and Society (MDES), "รวม.ดีอี Kick off ศูนย์ AOC 1441 แก้ปัญหาหลอกลวงออนไลน์ แบบ One Stop Service สำหรับประชาชน" accessed February 28, 2025, <https://www.mdes.go.th/news/detail/7535>.

<sup>9</sup> *Nation Thailand*, "Thai Gov. Tightens Cybersecurity Laws," October 17, 2024, <https://www.nationthailand.com/thailand/general/40032467>.

The AOC operates a dedicated hotline service with 100 active lines, ensuring that victims can report scams 24/7. The center has set an ambitious response time, needing only 10 minutes to investigate cases, freeze fraudulent accounts, and facilitate the return of stolen funds to victims.<sup>10</sup> Furthermore, AOC is employed AI and big data to combat fraudulent activities swiftly, the AI will analyze massive data stream from several sources – most of which is provided by the center’s partner e.g., Central Fraud Registry of the Thai Bankers’ Association and telecom data exchange system<sup>11</sup>. This technology allows AOC to take down the scammers bank account swiftly, and ensure the victims will get their money back within an hour after the call.<sup>12</sup>

Since its launch in November 2022, the AOC has demonstrated significant effectiveness in fighting cybercrime. By February 2025, the center reported receiving over one million calls from scam victims and successfully taking down 537,431 scammer-linked bank accounts. This rapid intervention has dramatically curbed the impact of online fraud. Officials reported that the daily financial damage from scams fell by 36–44% after the 1441 hotline became active<sup>13</sup>. This achievement highlights the Thai government’s proactive efforts in leveraging technology, cross-sector collaboration, and rapid-response mechanisms to mitigate the growing threat of online fraud.<sup>14</sup>

## Cybersecurity Measures

Apart from AOC, Thailand has enacted the Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 (2023) (“Cybercrime Decree”) which give the rights to the victims and authorities to ask the commercial bank and e-payment service to freeze suspicious crimes for seventy-two hours, then within the seventy-two hours the victim must file the complaint to the police. Then the police need to notify the bank or platform of the complaint, and the bank or platform needs to freeze the account for another seven days, the account can be unfrozen after seven days if there is no further extension order from the police. Furthermore, the bank or platform needs to proactively freeze the suspicious activities they find for seven days and notify the authorities, it can be unfrozen after seven if there is no extension order.<sup>15</sup>

---

<sup>10</sup> Ibid.

<sup>11</sup> *Bangkok Post*, "Govt Sets Up Scam Victim Aid," December 27, 2024, <https://www.bangkokpost.com/thailand/general/2676383/govt-sets-up-scam-victim-aid>.

<sup>12</sup> Ibid

<sup>13</sup> *Bangkok Post*, "Digital Economy and Society Ministry to Retain Key Policies," January 14, 2025, <https://www.bangkokpost.com/business/general/2866637/digital-economy-and-society-ministry-to-retain-key-policies>

<sup>14</sup> Thai Government Official Website, "AOC 1441 เตือนภัย “โจรออนไลน์” หลอกลงทุนเทรดหุ้น – ชมชู้โอนเงิน อ้างเป็นตำรวจ พบสูญเงินกว่า 16 ล้านบาท," accessed February 28, 2025, [https://www.thaigov.go.th/news/contents/ministry\\_details/93747](https://www.thaigov.go.th/news/contents/ministry_details/93747).

<sup>15</sup> Tilleke & Gibbins, "Thailand’s New Cybercrime Measures Enlist Aid of Banks and Service Providers," January 2025, <https://www.tilleke.com/insights/thailands-new-cybercrime-measures-enlist-aid-of-banks-and-service-providers/>.

Moreover, Thai cabinet approved the draft amendment to the Executive Decree on Measures to Prevent and Suppress Technological Crime 2023 which will add several obligations to the P2P cryptocurrency trading platform, commercial bank, telecom operators and social media platform to exercise due care to prevent online fraud and scam<sup>16</sup>. This amendment is expected to take effect in early 2025.

Another key figure to combat online fraud and scams are the Bank of Thailand (BOT) the regulator in banking sector and central bank of Thailand. The BOT took several proactive measures to combat online scam e.g., the central bank mandated the rule for every private bank to set up hotline to tackle online scam. Moreover, the BOT mandated a rule in 2023 to prevent the fraudulent activities in which the scammer steal one-time-password (OTP) or log-in details to siphon money from the victims<sup>17</sup>.

### The Use of AI in Addressing Scams

However, while AI technology is one of the key success factors to combat and effectively reduce online fraudulent activities and redistribute the stolen funds back to the victim, the exploitation of AI technology complicated the pattern of online fraud and scam. From the case mentioned in section I Patterns and Trends, the GoldFactory – a Chinese Hacker group – exploited the BOT's biometric prevention policy using facial recognition technology and deepfake to impersonate the victim and siphon the money out of the bank. This raises concern especially for the Bank of Thailand to tackle the use of Deepfake, the Bank of Thailand adds two more layers required for the transaction, to make a large transaction one will need to verify with his phone, 6-digit OTP and face scan before concluding the activity. The fraudster will need to obtain the victims phone number, intercept the message to get the OTP, then use face scan to conclude the transaction, which makes the siphoning activities harder. Moreover, BOT and Thai commercial Banks are working to enhance its facial recognition technology to detect deepfake video more accurately.<sup>18</sup>

Furthermore, Thai commercial banks have been proactively investing in technology to detect fraudulent activities and working together to create a database called “Central Fraud Registry” which allows banks to track fraudulent activities across the banking sector. As a result, the banking sector in Thailand is developing quickly to prevent online fraud and scams.

On the telecommunication side, the National Broadcasting and Telecommunication Commission mandated a rule that any user holding more than 5 sim cards needs to verify his usage or the sim cards

---

<sup>16</sup> Nation Thailand, "New Policy Measures to Combat Online Fraud," February 2025, <https://www.nationthailand.com/news/policy/40045647>.

<sup>17</sup> Bank of Thailand (BoT), "Regulatory Update: Strengthening Financial Cybersecurity," March 9, 2023, <https://www.bot.or.th/en/news-and-media/news/news-20230309.html>.

<sup>18</sup> Bank of Thailand (BoT), หลายมิติฯ ชัดใกล้ ติดตามกลโกงยุคใหม่ พร้อมวิธีป้องกันภัยที่ดีกว่าเดิม, accessed February 28, 2025, [https://www.bot.or.th/th/research-and-publications/articles-and-publications/bot-magazine/Phrasiam-68-1/TheKnowledge\\_cofact.html](https://www.bot.or.th/th/research-and-publications/articles-and-publications/bot-magazine/Phrasiam-68-1/TheKnowledge_cofact.html).



will be deactivated. This policy aims to tackle the call center gang who use scam calls to trick the victims.

## Regional Collaboration in Addressing Scams

Moreover, the nature of online fraud and scams often involve the crime conducted by the fraudster outside the country, which requires the cooperation from several countries to tackle the problem effectively. In the 2025 ASEAN Digital Ministers' Meeting in Bangkok, Paetongtarn Shinawatra the prime minister of Thailand states that prevention of online scam must be one of the priorities for ASEAN countries, and the use of Artificial Intelligence needs to follow an ethical guideline. Consequently, the meeting concluded with the decision to strengthen the collaboration among ASEAN countries to combat online crime through ASEAN Working Group on Anti-online Scam (WG-AS) and strengthen AI governance through ASEAN Working Group on Artificial Intelligence Governance (WG-AI)<sup>19</sup>. Moreover, the ASEAN countries will employ ASEAN Cybersecurity Coordinating Centre to share data regarding the pattern of AI-enabled scam among members to introduce new measure to combat the problem<sup>20</sup>.

Moreover, Thailand and China work together to tackle the scammers located in neighboring countries like Myanmar, Cambodia, and Laos. In a high-level agreement in January 2025, Thailand and China announced they will set up a joint coordination center to combat illegal call center networks along the Thailand-Myanmar and Thailand-Cambodia borders. The coordination center is based in Bangkok and the other coordination center will be established in Mae Sot. The center brings Thai and Chinese police together to share intelligence and co-direct operations against the syndicates<sup>21</sup>. The joint effort was successful with a coordinated crackdown in early 2025 led to the rescue or detention of over 7,000 people from scam centers in Myanmar's Myawaddy region, many of them trafficked workers forced to run scams.<sup>22</sup>

## IMPACT ANALYSIS IMPLICATIONS OF SCAMS

Prior to the implementation of targeted interventions, online fraud and scams in Thailand had escalated to unprecedented levels. According to the Cyber Crime Investigation Bureau, from March 2022 to May 2024, Thailand recorded approximately 300,000 cases of online financial fraud, resulting in total economic losses exceeding 63 billion THB (approximately USD 1.8 billion)<sup>23</sup>

---

<sup>19</sup> ASEAN, "Bangkok Digital Declaration," January 2025, <https://asean.org/wp-content/uploads/2025/01/14-ENDORSED-BANGKOK-DIGITAL-DECLARATION.pdf>.

<sup>20</sup> Ibid

<sup>21</sup> Reuters, "Thailand, China Set Up Coordination Centre to Combat Scam Call Networks," January 24, 2025, <https://www.reuters.com/world/asia-pacific/thailand-china-set-up-coordination-centre-combat-scam-call-networks-2025-01-24>.

<sup>22</sup> The Irish News, "Crackdown Sees Thousands of Scam Centre Workers Awaiting Repatriation," February 2025, <https://www.irishnews.com/news/world/crackdown-sees-thousands-of-scam-centre-workers-awaiting-repatriation-6LAWDMNCLZLD5GUKX4RQGQWLC4/>.

<sup>23</sup> Royal Thai Police, Cyber Crime Investigation Bureau, Media Release, November 2023.

Beyond direct financial losses, fraudulent activities have had a broader economic impact. Online scams led to reduced consumer confidence in digital financial services, directly affecting e-commerce growth and financial technology (fintech) adoption. A survey conducted by the Electronic Transactions Development Agency (ETDA) in 2023 revealed that 43% of Thai respondents expressed reluctance to conduct online transactions due to fraud concerns, while 29% indicated that they had reduced their usage of mobile banking services following exposure to scam attempts<sup>24</sup>

In response to that, Thai authorities implemented a series of countermeasures between 2022 and 2024, focusing on financial security, law enforcement coordination, and cross-border cooperation.

To enhance security in digital transactions, the Bank of Thailand (BoT) introduced mandatory biometric verification for transactions exceeding 50,000 THB per transfer (or 200,000 THB per day) in mid-2023. By requiring facial recognition or fingerprint authentication, this policy aimed to reduce unauthorized access to digital banking services. The outcome of this intervention has yet to be publicly announced.

Moreover, The Central Fraud Registry (CFR) was introduced in 2024 to consolidate fraudulent account data across banks. By mid-2024, Thai banks collectively closed 1.8–1.9 million mule accounts<sup>25</sup>, reducing the ability of scammers to launder stolen funds. Though the intervention has taken down several mule accounts, the number of such accounts has continued to increase substantially, which calls for stronger intervention.

Furthermore, Bank of Thailand's report shows that online financial fraud evolves quickly. When there is a new intervention, the fraud will reduce significantly until the new generation of online fraud emerges, calling for the authorities to introduce a new regulation, which will eventually reduce the new generation fraud pattern. This trend shows that the regulation regarding online fraud and scam needs to be constantly updated to keep up with the new pattern of fraudulent activities.<sup>26</sup>

Apart from the effort exclusively in the banking sector, the joint effort among stakeholders involving online fraud and scam has been introduced as the establishment of The Anti-Online Scam Operation Center (AOC 1441) was established in late 2023 to enable rapid intervention in fraud cases. The center's 24/7 hotline allowed victims to report scams in real-time, triggering an immediate freeze of suspect accounts within an average response time of 10 minutes<sup>27</sup>. The impact of this intervention recorded from November 2023 to February 2025, the AOC received 1,461,074 calls and froze 517,954 accounts.<sup>28</sup>

---

<sup>24</sup> Electronic Transactions Development Agency (ETDA), 2023 Survey on Online Transaction Behavior:

<sup>25</sup> *ibid*

<sup>26</sup> <https://www.bot.or.th/content/dam/bot/documents/th/news-and-media/news/2024/news-th-20240613-attach1.pdf>

<sup>27</sup> <https://edulampang.prd.go.th/th/content/category/detail/id/57/iid/340064>

<sup>28</sup> *ibid*

However, these interventions aim to tackle online fraud and scam activity in more traditional ways which involve text message, scam call, online advertising and social media platforms. However, advanced technology like Artificial Intelligence will make fraud and scam become much more sophisticated and harder to detect.

### AI-Powered Scams: The Emerging Threat

The increase in exploitation of AI technology in organized crime might be the result of the increase in accessibility of the technology. The emergence of AI and Deepfake technology lead to an increase in open-source AI tools and acceleration in Generative AI deployments make AI technology more accessible. Which leads to emerging risks from AI technology as follows:<sup>29</sup>

- **Deployment in cyber-enabled fraud:** Advanced technology provides the scammer with more ways to conduct the fraudulent activities e.g., automatic scripts for social engineering, impersonating scam, KYC bypass.
- **Evolution and Scalability:** The rapid deployment of Generative AI enables less tech-savvy scammers to conduct cyber-enabled fraud, making the cyber-enabled fraud become much more scalable (automatically generate text messages).

The APAC region experiences a rise in cyber-fraudulent involving artificial intelligence such as the rise in Deepfake-related crime in 2023 which increased by more than 1500 percent. Thailand, too, experienced the rise in these crimes, the infamous cases include:

- Deepfake fraud (impersonation of CEOs, government officials, or family members)
- AI-generated phishing emails and voice cloning scams
- Face-swapping technology to bypass biometric authentication

In a recent case, deepfake scam where fraudsters used AI to impersonate police officers during a video call which results in more than 190 victims, Moreover, one of the most shocking cases is the voice cloning scammers impersonate the world leader's voice and try to extort the prime minister of Thailand.

Another case is the attempts of a group of hackers trying to steal biometric data from Thai citizens involving launching an application luring the victims to upload their video and use facial recognition AI to capture the biometric data of the victim to siphon money from their account.

For these reasons, although there may not be statistics pointing out the exact impact of AI-enabled fraud in Thailand, the cases from these fraudulent activities raise concerns for the use of AI in online fraud and scams.

---

<sup>29</sup> [https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC\\_Convergence\\_Report\\_2024.pdf](https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf)

## BEST PRACTICE AND POLICY RECOMMENDATIONS

Thailand initially faced high volumes of online fraud, but through multi-stakeholder collaboration, led by the Ministry of Digital Economy and Society (MDES), the country has successfully mitigated these threats. The establishment of AOC 1441 was a major step in reducing fraud, enabling faster intervention and enhanced coordination between government agencies.

The Bank of Thailand's biometric authentication mandate has shown promise in preventing traditional fraud. However, scammers quickly adapt to new regulations, requiring continuous policy adjustments to stay ahead of evolving threats.

In terms of public-private collaborations, Google and the Ministry of Digital Economy and Society (MDES) partnered to enhance Google Play Protect in April 2024.<sup>30</sup> The partnership has resulted in the blockage of more than 6.6 million high-risk app installation attempts as of April 2nd, 2025. Additionally, Thailand's National Cyber Security Agency (NCSA) and Google Cloud have also announced a strategic collaboration and engage in AI-powered cyber defense through threat intelligence sharing and incident response capability building to address evolving threats and boost online safety for Thailand citizens and residents.<sup>31</sup>

At the international level, the joint Thai-Chinese crackdown on cybercrime near the Myanmar border was a notable success, highlighting the importance of cross-border cooperation. Additionally, the establishment of ASEAN's working group on AI and online fraud prevention is a significant step toward ensuring regional cybersecurity.


Despite these efforts, AI-powered fraud remains an emerging threat in Thailand. While the country has introduced AI ethics guidelines, they lack regulatory enforcement mechanisms, leaving high-risk AI applications unregulated.

### Policy Recommendations

- A combined effort among government agencies within the country is crucial to tackling online fraud and scams. This approach requires a robust database and advanced analytical tools (e.g., artificial intelligence) to identify crime patterns and enable swift action.
- Prevention-oriented measures are necessary to enhance online safety, but such an approach requires cutting-edge technology and data analytics for effective implementation.
- International collaboration is essential, as online fraud often involves cross-border organized crime networks.
- Online fraud evolves rapidly with the increasing accessibility of generative AI and advanced AI solutions. Stakeholders must continuously adapt to counter emerging threats. Consequently,

<sup>30</sup> <https://www.bangkokpost.com/business/general/2915570/state-google-fraud-effort-blocks-scams>

<sup>31</sup> <https://thailand.googleblog.com/2025/04/strategic-cybersecurity-collaboration-NCSA.html>



data sharing and best practices between countries are critical to ensuring well-informed, timely interventions.

- Proactive partnerships with key actors in the private sector (e.g., banks, digital payment providers, telecommunication companies, e-commerce platforms, social media) should be leveraged to enhance industry expertise and strengthen joint responses for early detection, mitigation, and prompt scam responses.





## Safer Internet Lab

 [saferinternetlab.org](https://saferinternetlab.org)

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

Find Us On



CSIS Indonesia | Safer Internet Lab