Safer Internet Lab
Led by CSIS in partnership with Google

Centre for Strategic and International Studies

Google

Research report

Online Fraud and Scams in Taiwan

Safer Internet Lab

Online Fraud and Scams in Taiwan

Joanna Octavia[1]

In Taiwan, online scams have risen in prominence, with significant financial losses reported each year. As digital platforms continue to play an increasingly significant role in daily life, scammers have adapted, exploiting the anonymity and vast reach of the internet to target unsuspecting individuals and businesses. Taiwan's susceptibility to online scams is supported by its affluence, an unusually high savings rate of close to 25 per cent, and high internet connectivity, with smartphone penetration rate close to 90 per cent (Fulco, 2025).

Taiwan's scam-related losses continue to escalate, with online investment scams accounting for the largest portion, and social media emerging as the primary platform through which these scams are perpetrated. In 2024, Taiwan experienced a total scam loss of US$ 7.4 billion – the smallest in absolute terms compared to other developed markets in Asia such as Hong Kong and Singapore – but still equivalent to 1 per cent of the GDP (Abraham et al., 2024; Abraham et al., 2024b). Out of this figure, social media postings are becoming the fastest-growing source of scams in Taiwan (Abraham et al., 2024b). More recently, the National Police Agency reported that victims in Taiwan have lost US$46.7 million between March 9 and 15, 2025, with a record of 3790 cases and fraudulent investment schemes accounting for the majority of losses at US$ 25.5 million (Taiwan reports NT$1.46 billion lost, 2025).

To combat this, the Taiwanese government has introduced a range of regulatory measures aimed at curbing the rise of online scams. These include the Fraud Crime Hazard Prevention Act, new frameworks for the virtual asset industry, and version 2.0 of the anti-fraud guidelines. Despite these efforts, challenges remain in addressing the evolving nature of online scams, particularly as scammers continuously adapt their tactics. This case study explores the current landscape of online scams in Taiwan, the regulatory responses put in place to combat them, and recommendations to address the remaining gaps.

CURRENT TRENDS

Taiwan is no stranger to scams. Despite its small population of 23.4 million people, the island is a longstanding hotbed for – and exporter of – telecoms fraud (Chung, 2016). Taiwan is also one of Asia's top manufacturers of high-tech technology, a level of technical expertise that is shared by local scammers (Hale, 2022). While phone calls and text messages remain among Taiwan's top four scam

[1] Associate Lecturer, University College London

delivery methods, they are now closely followed by social media and instant messaging apps, highlighting a significant shift toward online scams (Abraham et al., 2024b).

In recent years, stronger enforcement against phone-based scams has driven the shift from telecoms fraud to online scams. As traditional telecom frauds faced increased scrutiny and blocking measures, scammers adapted by exploiting social media platforms, online advertisements, and encrypted messaging apps to target victims more effectively. Mirroring global trends, scammers are exploiting artificial intelligence and deepfake technology to make their schemes more convincing and difficult to detect. Coupled with Taiwan's rapid digital adoption during the COVID-19 pandemic, this transition has been further accelerated by regulatory gaps unique to the island, which have made Taiwan a hotspot for sophisticated online scams.

Social Media Platforms and Instant Messaging Apps

Social media platforms and messaging apps are central to online scam operations in Taiwan. Scammers use these platforms to build trust and establish relationships before launching scams, often impersonating friends or family members. In addition, phishing and investment scams are also rampant on the platforms. Facebook and LINE are the two most commonly exploited social media platforms, with scammers using them to spread phishing links, impersonate trusted figures, and promote fraudulent investment schemes. In 2023, 55 per cent of Taiwanese respondents reported encountering scam messages through social media, significantly higher than the global average of 44 per cent (Abraham et al., 2024b). In particular, scam activities through social media have increased by 21 per cent between 2023 and 2024 (Abraham et al., 2024b). Despite increasing multi-stakeholder collaborative efforts between government and industry, scams taking place on social media platforms and messaging apps remain difficult to intercept (Hsu et al., 2024).

Facebook stands out as the leading social media platform where individuals encounter online scams. Nearly 70 per cent of online scam losses stemmed from Facebook advertisements, consisting of investment scams and product endorsements by fake celebrities (Yang, 2024). Additionally, 97.9 per cent of fake ads reported to the police were found to have originated from the Meta platform (Yang, 2024). According to the Minister of Digital Affairs, Facebook's centralised and manual approach to removing fake ads has led to a surge in fraudulent advertisements in Taiwan over weekends, when enforcement teams are inactive (Yang, 2024). In November 2024, the prevalence of scams on Facebook led major Taiwanese banks to suspend advertising on the platform in order to safeguard the banks' reputations following a decline in trust toward digital platforms, which is directly attributed to the growing prevalence of scams (Abraham et al., 2024b, Wan, 2024). These developments underscore the importance of more effective measures to tackle the proliferation of fraudulent content on social media platforms.

The widespread use of LINE for scams is a distinctive feature of Taiwan's digital landscape. As Taiwan's dominant messaging app, LINE is used by more than 90 per cent of the population for daily communication, business, banking and shopping (Lange and Lee, 2020). Its popularity extends to official government agencies, banks and brands, many of which operate verified accounts on the platform. Scammers exploit LINE's credibility and trust primarily by creating fake accounts that appear to be from friends, family members, or even trusted organisations. For example, in a typical investment scam, after initial contact on Facebook, victims are directed to fake investment groups on LINE app, where scammers solicit money for fake investment opportunities and asking them to register with fake websites or apps (Su et al., 2024). LINE groups, like other messaging platforms, are private and encrypted, making it challenging for authorities to monitor potential online scam activities once they have entered these private spaces.

Fraudulent investment groups on LINE have been used by scammers to communicate with victims and persuade them to invest in fake investment opportunities. Often branded as stock investment clubs, these fraudulent groups promise exclusive stock tips, cryptocurrency opportunities or insider financial knowledge (Yao and Pan, 2023). A research by Su et al. (2024) comparing fraud and legitimate investment groups on LINE found that the volume of messages in fraud groups exceeded that of the legitimate group, with messages sent predominantly in the afternoon. By creating the appearance of active investment discussions, fraudulent groups sought to influence victims and make them feel more confident about their investment choices (Su et al., 2024). Following closed chat groups, the scammers may continue to engage victims in one-on-one conversations, where they continue to try to persuade victims to invest in fraudulent investment schemes. In response to these tactics, LINE has introduced warnings across multiple scenarios, such as adding unknown contacts, to alert users to potential scam risks (Ministry of Digital Affairs, 2024).

Phishing attacks attempting to take over LINE accounts for scam activities are common. Users have reported cases where their LINE accounts are being hacked and used to scam their friends and family. A common tactic involves fraudulent invitations to participate in a poll, where victims are prompted to enter their LINE username and password in order to cast their vote (Cheng, 2025; Yao and Yeh, 2025). Once scammers gain access, they use the compromised account to impersonate the victim and send messages to contacts, leveraging personal trust to request money or sensitive information.

Another common scam tactic that exploits the reach of these social networks is by using 'one-page scam posts'. In this tactic, scammers show fraudulent content and links on social media or instant messaging apps, leading victims to other web pages that collect their personal information or trick them into buying fake products (Li, 2024). These one-page scam posts are typically characterised by their use of one long page websites that mix simplified and traditional Chinese characters, and the lack of customer service information (Hiciano, 2025). However, the pages often use names of famous people or organisations, such as the prominent research institution Academia Sinica in Taiwan, to appear legitimate. Moreover, other supporting social media posts that purport similar news are often circulated at the same time to build on the credibility of the fraudulent claims (Li, 2024).

Fake Celebrity Endorsements and Investment Scams

Fake celebrity endorsements are widespread in Taiwan, largely due to the strong idol culture and deep public trust in celebrities. Scammers exploit this trust by using high-profile figures, particularly well-known entrepreneurs, financial experts, politicians and entertainment stars, to lend credibility to their scams and defraud individuals (Yao and Pan, 2023).

One of the most prevalent scam types involving fake celebrity endorsements is investment scams. Alongside fake celebrity endorsements, other common sales tactics used in advertisements for investment scams include free lists of stock picks and high-return investment strategies (Hiciano, 2025). In these scams, users are lured through fake celebrity advertisements on platforms like Facebook and LINE, which feature doctored images or videos of famous individuals endorsing so-called legitimate investment opportunities (Yao and Pan, 2023). Scammers create fake accounts or advertisements featuring their names and images, tricking unsuspecting users into clicking on the links, after which they will try to con victims in the closed chats (Shan, 2023a). In a case involving the impersonation of Lai Xian-zheng, a well-known financial expert, victims were instructed to download a fake app that appeared to be from a trustworthy Japanese securities company and transfer money to a designated bank account (LaMattina, 2024). Many victims believe fake celebrity endorsements are legitimate, as the celebrities used in the ads are widely recognised and respected in Taiwan.

Tackling fake celebrity endorsements in investment scams is crucial, given the significant financial losses associated with these schemes, reputational impact they have on celebrities, and potential scam amplification. In the fourth quarter of last year, investment scams accounted for the largest share of total scam-related losses, at 56.9 per cent of total losses of US$ 1.23 billion (Lee and Pan, 2025). Well-known figures whose images have been used to endorse these scams have filed complaints to the police, leading the police to collaborate with digital platforms such as Google, Meta and others to take down these ads (Yao and Pan, 2024b). The potential for online scam reach and impact to be amplified due to the large followings of these celebrities further underscores the importance of addressing these scams.

Cryptocurrencies

The rise of cryptocurrencies has made it harder to fight online scams in Taiwan. Cryptocurrencies are favoured by scammers targeting Taiwanese users due to reasons such as anonymity, decentralised nature, and ability to operate cross-border (Hung and Van Trieste, 2025). Several unique aspects of Taiwan's cryptocurrency landscape and regulatory environment, such as regulatory gaps in the governance of virtual assets, have made it a significant focal point for crypto-related crime.

Cryptocurrencies are integrated into a typical scam workflow in Taiwan. Since 2019, scammers have started tricking victims by installing fake apps and helping them with cryptocurrency transactions, making the process seem legitimate before stealing their money (Shih and Tsai, 2024). In a typical online scam workflow in Taiwan, online scammers will make initial contact on a public social media platform like Facebook, followed by closed chats as well as one-on-one conversations on LINE. Afterward, scammers will ask the victims to invest in crypto investment scams. After the money is transferred, scammers often attempt to launder it or convert it into cryptocurrency to make it harder for authorities to trace or recover (Lin et al., 2024).

Taiwan's cryptocurrency regulation has historically been relatively light, making it a soft target for crypto-related scams. When markets across Asia such as Singapore, Hong Kong, and China tightened their cryptocurrency regulations, Taiwan positioned itself as a regional crypto hub, attracting investors with its rapidly growing transaction volumes and relatively loose regulatory environment (Tobin, 2023). Taiwan currently does not have a comprehensive regulatory framework for the entire crypto industry, allowing local crypto exchanges to operate with a high level of autonomy. The lack of oversight for crypto exchanges has become a loophole for scammers, while the hands-off stance also meant there was little public education and knowledge on the risks associated with cryptocurrencies and virtual assets.

MISUSE OF AI IN SCAMS IN TAIWAN

The rising misuse of AI in online scams is becoming a major concern in Taiwan, especially due to the public's limited awareness of the risks involved. AI-driven deception, which manipulates both visual and auditory elements, introduces new risks for individuals. While many Taiwanese are aware of AI-generated text and chatbots, fewer recognise its use in manipulated images and videos (Abraham et al., 2024b) This is particularly alarming as most scams in Taiwan occur through phone calls and social media, leaving users vulnerable to deepfake images, videos, and voice recordings designed to deceive them.

A significant risk is the use of deepfake technology to impersonate individuals familiar to the victim. This tactic, used by scammers to enhance the credibility of their deception, may build on the widespread phishing of LINE accounts. Furthermore, this tactic aligns with the prevalence of short-term scams in Taiwan, where 39 percent of scams are completed within 24 hours of initial contact (Abraham et al., 2024b). Such concerns over the misuse of AI-altered likeness in scam video calls have been raised by Taiwanese authorities in 2023, following similar trends in China and potential rapid spillover of scams to Taiwan (Liu et al., 2023). This was proven by a case in 2024, whereby scammers used AI to deceive a Taiwanese woman into believing that she was having a video call with Hong Kong celebrity Andy Lau after visiting what she believed was Lau's fan website (Hsu and Pan, 2024).

The usage of AI-generated images and videos to scam individuals in Taiwan is often combined with other technologies, such as social media, online dating sites, or cryptocurrency. This combination has been used in longer-term scams, such as romance and investment scams, which depend on gaining the victim's trust, either through building up a relationship or proving small returns on initial investment. In January 2025, Hong Kong police arrested 31 individuals involved in a syndicate that used deepfake technology to defraud victims in Taiwan (Ma, 2025). In these romance-investment scams, the scammers created and deployed AI-generated images and videos to impersonate wealthy women and engage victims in online relationships. Using social engineering tactics, the scammers convinced victims to invest in fraudulent schemes, successfully gaining over US$4.3 million as a result (Ma, 2025).

The involvement of technology experts, with their knowledge of AI, machine learning, and data analysis, increases the risk of cross-border scam operations scaling at an alarming rate. The Taiwanese government has raised the concern that online scammers increasingly have the capacity to hire more programmers and obtain greater computing power to run more scams on the internet (Lin et al., 2024). In August 2024, another arrest in Hong Kong led to the capture of a number of digital media and technology university graduates, who were running a global deepfake romance scam operation targeting men around the world, including Taiwan (Yeung, 2024). As scam groups constantly innovate their technologies and tactics, the Taiwanese public, with their limited awareness of AI-generated images and videos in online scams, faces increasing risk of falling for fraudulent schemes.

POLICY GAPS

Taiwan has made significant progress in addressing the rising challenges of online scams. In July 2024, the Legislative Yuan passed several key anti-fraud laws, such as the Fraud Crime Hazard Prevention Act, along with amendments to the Code of Criminal Procedure, Communication Security and Surveillance Act, and Money Laundering Control Act. The passage of these laws strengthened regulations on online scams and gave greater power to law enforcement (Chung, 2024a; Executive Yuan, 2024). These were followed by the new version 2.0 of the anti-fraud guidelines (2025-2026), which was passed in November 2024 and primarily focused on financial sector fraud prevention, crypto industry regulations and scam awareness (Executive Yuan, 2024). The new centralised coordination of scam-fighting efforts between agencies, particularly in the monitoring of the financial sector and digital platforms, ensures a more unified and efficient response. However, despite these advancements, there are still policy gaps that need to be addressed for optimal effectiveness.

A big focus of the new policy consists of measures to curb the spread of online scams through online advertising and to increase platform accountability. For example, the real-name system obliges digital platforms to clearly disclose who is running an ad and how the ads are being managed. While this measure could make it harder for scammers to hide behind anonymous ads, it could also expose individual users that are running ads, such as sole proprietors, to privacy risks and safety-related harms. Furthermore, the regulation does not explicitly address user-generated content, such as scam posts made by individual users. This creates a regulatory gap, as online scams can still be perpetrated through non-advertising content.

Meanwhile, the mandatory 24-hour removal of fraudulent ads aims to stop scammers from running harmful ads for long periods and ensures digital platforms take responsibility for removing fraud as soon as they are alerted. This builds on the government's development of an AI-powered system that scans ads and articles on major platforms like Google and Instagram. If the system detects suspicious content, the government will notify the platforms and request prompt removal (Lin et al., 2024). Nonetheless, there may be challenges in ensuring uniform enforcement across all digital platforms, especially when dealing with international platforms outside of Taiwan's jurisdiction. A short turnaround time and insufficient time to thoroughly assess the material can also lead to overblocking of legitimate content.

A key aspect of the new anti-scam guideline is anti-fraud measures in the financial sector, aimed at intercepting fraud via money flows. The FSC is promoting the establishment of mechanisms to detect and flag financial accounts suspected of fraudulent activities, while the mandatory reporting and collaboration among financial institutions facilitates the tracking and freezing of fraudulent accounts (Executive Yuan, 2024; FSC, 2024). This builds on an existing alliance between the Ministry of Digital Affairs with several partners in the financial industry in Taiwan, including 35 banks (Lin et al., 2024).

Since 2023, the use of deepfakes for online scams has been criminalised in Taiwan. In May 2023, Taiwan's Legislature revised its criminal law to combat deepfake-related scams, raising the maximum prison sentence for those convicted to seven years (Shan, 2023b, Kazaz, 2024). A policy gap here is the limited focus on proactive monitoring and removal of deepfake content that is used to defraud. Furthermore, considering that many online scams involving deepfakes are cross-border with perpetrators based outside of Taiwan, the island's lack of diplomatic ties with some countries, including scam hotspots in Southeast Asia such as Myanmar and Cambodia, make direct prosecution difficult. Additionally, Taiwan is neither a member state nor an observer of Interpol, and therefore is unable to access Interpol's 19 criminal intelligence databases and systems for requesting international cooperation (Coyne, 2024).

The Taiwanese government has moved towards clearer crypto regulations, primarily in response to a significant increase in scams and fraudulent activities within the crypto space, though a fully comprehensive regulation remains to be seen. In 2024, Taiwan introduced new anti-money laundering (AML) for virtual asset service providers (VASPs), mandating them to register by September 2025. Meanwhile, the Financial Supervisory Commission (FSC) is considering new legislation to regulate the cryptocurrency industry (Chung, 2025). Under the new regulations, all VASPs would be classified as financial institutions, and personal trading would be prohibited once the law is enacted (Chung, 2025).

As of March 2025, Taiwan's Financial Supervisory Commission (FSC) has released the draft VASA for public consultation, with feedback open until the end of May. The legislation, expected to be enacted later in 2025, aims to establish a comprehensive regulatory framework for virtual assets. Key provisions include requiring VASPs to join the industry self-regulatory body, which will set and enforce codes of conduct and be subject to oversight by the FSC (Pintu, 2025). However, more details on clear, enforceable consumer protection mechanisms specifically related to crypto-related scams, including the responsibility of VASPs to ensure the security of transactions and prevent scams involving virtual assets, remain to be seen. Furthermore, while the licensing regime ensures that only regulated and compliant VASPs can operate in Taiwan, scammers can still use unregulated foreign crypto exchanges to target Taiwanese users. Tackling this challenge thoroughly will require stronger international cooperation.

POLICY RECOMMENDATIONS

Based on the policy gaps, the following recommendations are proposed:

1. **Expand anti-scam scope to user-generated scam content while ensuring responsible moderation and user protection:** Recognising that online scams in Taiwan increasingly leverage user-generated content (UGC) – such as posts, comments, fake profiles, the regulatory efforts must broaden their focus beyond just paid advertisements. The government should strengthen mechanisms for timely and fair removal of scam-related UGC through efficient notice-and-takedown procedures grounded in internationally recognized safe harbour principles. It is crucial to adopt a fair approach to content moderation that is transparent and proportionate, protects free speech, and aligns with international internet governance standards. Additionally, this approach should avoid requiring general monitoring of UGC, as it could undermine individual users' privacy and freedom of expression.

2. **Implement privacy safeguards for small advertisers:** To protect privacy, sole proprietors and individuals who run advertisements on digital platforms should be allowed to verify their identity without publicly disclosing sensitive personal data. One way to do so is by creating anonymised verification badges ("verified advertiser").

3. **Categorise potentially scam ads into tiered risks:** Instead of applying the same 24-hour turnaround time for all flagged content, the government could implement a tiered system where high-risk, clearly fraudulent ads are prioritised for rapid removal. It would require advanced technology, combined with human oversight, to assess the risk levels of flagged content in real time.

4. **Issue proactive regulations to address the misuse of deepfakes:** Taiwan should introduce proactive measures aimed at addressing the misuse of AI and deepfake technologies in scams. These could include mandatory reporting or labelling for deepfake content by digital platforms and promoting AI literacy for consumers to recognise deepfakes.

5. **Create clear guidelines for tackling crypto scams:** The government should introduce more stringent consumer protection regulations for crypto transactions, including ensuring transparency of operations by VASPs and holding them accountable for scam-related activities conducted on their platforms. VASPs should also be required to educate their users on potential risks related to crypto scams.

6. **Strengthen international cooperation:** Given the cross-border nature of online scams, Taiwan should work with international partners to ensure better tracking and removal of deepfake content used in online scams, and to track down and prosecute international crypto scam groups. This could take the form of sharing intelligence and working through international regulatory bodies such as Interpol and other jurisdictions.

REFERENCES

Abraham, J., Rogers, S., Njoki, C., & Greening, J. (2024). *Asia Scam Report 2024.* Global Anti-Scam Alliance. https://www.gasa.org/_files/ugd/7bdaac_e7fad80cd72141c4ac73119be1c9378a.pdf

Abraham, J., Rogers, S., Njoki, C., & Greening, J. (2024b). *The State of Scams in Taiwan 2024.* Global Anti-Scam Alliance. https://www.gasa.org/_files/ugd/7bdaac_479a5775921d4dd598d0af2ca79962e9.pdf

Cheng, J. (2025, January 18). Be more vigilant against scammers. *Taipei Times*. https://www.taipeitimes.com/News/editorials/archives/2025/01/18/2003830404

Chung, J. (2024a, November 29). Cabinet passes new anti-scam guidelines. *Taipei Times*. https://www.taipeitimes.com/News/taiwan/archives/2024/11/29/2003827677

Chung, J. (2024b, December 22). Scams cost NT$12.6bn last month: NPA. *Taipei Times*. https://www.taipeitimes.com/News/taiwan/archives/2024/12/22/2003828899

Chung, J. (2025, February 2). FSC mulls cryptocurrency regulation. *Taipei Times*. http://taipeitimes.com/News/front/archives/2025/02/02/2003831191

Chung, N. (2016, October 27). Taiwan's cross-strait export of phone scams 'no good for island', former president says. *The South China Morning Post.* https://www.scmp.com/news/china/policies-politics/article/2040413/taiwans-cross-strait-export-phone-scams-no-good-island

Coyne, J. (2024, June 27). *Taiwan's exclusion from Interpol is the world's loss.* Australian Strategic Policy Institute. https://www.aspistrategist.org.au/taiwans-exclusion-from-interpol-is-the-worlds-loss/

Executive Yuan. (2024, December 6). *Next-generation anti-fraud strategy guidelines, version 2.0* [Press release]. https://english.ey.gov.tw/News3/9E5540D592A5FECD/faccc48c-1d4c-45c8-aa1b-73d9c283a73d

Financial Supervisory Commission. (2025, January 22). *Measures to enhance fraud prevention in Taiwan's financial sector* [Press release]. https://www.banking.gov.tw/en/home.jsp?id=87&parentpath=0&mcustomize=multimessage_view.jsp&dataserno=202501220001&dtable=News#:~:text=In%20terms%20of%20fraud%20prevention,accounts%2C%20(3)%20Requiring%20card

Fulco, M. (2025, February 17). *Taiwan grapples with intensifying cybercrime.* Taiwan Business TOPICS. https://topics.amcham.com.tw/2025/02/taiwan-grapples-with-intensifying-cybercrime/

Hale, E. (2022, December 5). Taiwan's front-line battle against mobile phone fraud. *BBC.* https://www.bbc.co.uk/news/business-63075729

Hiciano, L. (2025, February 19). MODA shares scam warning signs. *Taipei Times.* https://www.taipeitimes.com/News/taiwan/archives/2025/02/19/2003832150

Hiciano, L. (2025, February 20). MODA reveals common online scam key words. *Taipei Times.* https://www.taipeitimes.com/News/taiwan/archives/2025/02/20/2003832194

Hsu, S. & Pan, J. (2024, July 2). Scammers use AI to cheat woman out of NT$2.64m. *Taipei Times.* https://www.taipeitimes.com/News/taiwan/archives/2024/07/02/2003820211

Hsu, H-C., Gillespie-Jones, C., Kaushal, A., & Yasukagawa, K. (2024, August 21-23). *Messaging Scam and Combatting to Protect Human Rights and Democracy* [Conference presentation]. Asia-Pacific Regional Internet Governance Forum, Taipei, Taiwan. https://aprigf.tw/programs/messaging-scam-and-combatting-to-protect-human-rights-and-democracy/

Kazaz, J. (2024). *Regulating Deepfakes: Global Approaches to Combating AI-Driven Manipulation.* GLOBSEC. https://www.globsec.org/what-we-do/publications/regulating-deepfakes-global-approaches-combatting-ai-driven-manipulation

Lange, E. & Lee, D. (2020, November 23). How One Social Media App is Beating Disinformation. *Foreign Policy*. https://foreignpolicy.com/2020/11/23/line-taiwan-disinformation-social-media-public-private-united-states/

LaMattina, L. (2024, August 8). Police investigate 27 suspects over NT$400 million investment fraud in north Taiwan. *Taiwan News*. https://taiwannews.com.tw/news/5916118

Lee, W. & Pan, J. (2025, January 20). Investment scams topped losses from fraud in 4th quarter. *Taipei Times*. https://www.taipeitimes.com/News/front/archives/2025/01/20/2003830510

Li, W. (2024, April 29). Too good to be true - Online scams in Taiwan. *Taiwan FactCheck Center*. https://en.tfc-taiwan.org.tw/too-good-to-be-true-online-scams-in-taiwan/

Lin, Y., Sahel, J., Chan, J., Octavia, J., & Chung, E. (2024, August 21-23). *From Innovation to Impact: Responsible AI - Challenges and Opportunities to Tackle Online Fraud and Scams* [Conference presentation]. Asia-Pacific Regional Internet Governance Forum, Taipei, Taiwan.

Liu, C., Lin, C., & Madjar, K. (2023, May 30). Police warn against scams using deepfake videos. *Taipei Times*. https://www.taipeitimes.com/News/taiwan/archives/2023/05/30/2003800665

Losses from scams hit NT$239.5bn. (2024, October 2). *Taipei Times*. https://www.taipeitimes.com/News/front/archives/2024/10/02/2003824665

Ma, J. (2025, January 5). Hong Kong police arrest 31 over deepfakes used to scam victims in Singapore, Malaysia. *The Straits Times*. https://www.scmp.com/news/hong-kong/law-and-crime/article/3293476/hong-kong-police-arrest-31-who-used-deepfakes-scam-victims-singapore-malaysia

Ministry of Digital Affairs. (2024, June 26). *Ministry of Digital Affairs Coordinate with Google and LINE to Strengthen Online Fraud Prevention Measures* [Press release]. https://moda.gov.tw/en/press/press-releases/13010

Pintu. (2025, March 27). *New Regulation of Crypto Assets in Taiwan: What Impact for Investors?* https://pintu.co.id/en/news/143170-new-regulation-of-crypto-assets-in-taiwan

Shan, S. (2023a, May 2). Google joins effort to combat online scam ads in Taiwan. *Taipei Times*. https://www.taipeitimes.com/News/taiwan/archives/2023/05/02/2003798981

Shan, S. (2023b, May 17). Legislature passes stiffer jail, fine for deepfake fraud. *Taipei Times*. https://www.taipeitimes.com/News/front/archives/2023/05/17/2003799936

Shen, T. (2024, November 28). Taiwan fast-tracks stricter crypto AML rules to take effect Nov. 30. *The Block*. https://www.theblock.co/post/328729/taiwan-fast-tracks-aml-rules-stricter-crypto

Shih, C. & Tsai, M. (2024). Application of Money Flow Analysis Technology in the Investigation of Money Laundering Crimes in Taiwan. *Procedia Computer Science*, 246, 4524-4533.

Su, Y., Shih, C., & Yang, T. O. (2024). Investment Fraud Cases Study in Chinese Context of Instant Messaging Software. *28th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2024).* Procedia Computer Science 246 (2024) 391-402.

Taiwan reports NT$ 1.46 billion lost to scams in one week. (2025, March 27). *TVBS News.* https://news.tvbs.com.tw/english/2810509?from=english_content_pack

Tobin, M. (2023, January 3). Taiwan goes all in on crypto, despite the global crash. *Rest of World*. https://restofworld.org/2023/taiwan-asia-crypto-capital/

Wan, C. (2024, November 19). Taiwanese Banks Curtail Facebook Ads Over Scam Concerns. https://www.bloomberg.com/news/articles/2024-11-19/taiwanese-banks-curtail-facebook-advertising-over-scam-concerns

Yang, J. (2024, December 25). Facebook at the Heart of Why Taiwan Can't Stop Scams. *Commonwealth Magazine*. https://english.cw.com.tw/article/article.action?id=3889

Yao, Y. & Pan, J. (2023, December 19). Stock investment scams are on the rise, bureau warns. *Taipei Times*. https://www.taipeitimes.com/News/taiwan/archives/2023/12/19/2003810846

Yao, Y. & Pan, J. (2024, February 24). Most online fraud on Facebook: report. https://www.taipeitimes.com/News/taiwan/archives/2024/02/24/2003814012

Yao, Y. & Pan, J. (2024, August 6). Meta pulls more than 46,500 fraud ads. https://www.taipeitimes.com/News/taiwan/archives/2024/08/06/2003821850

Yao, Y. & Yeh, E. (2025, March 19). CIB issues warning about hijacked social media accounts. *Taipei Times*. https://www.taipeitimes.com/News/taiwan/archives/2025/03/19/2003833689

Yeung, J. (2024, October 15). Deepfake scams raked in $46 million from men across Asia, police say. *CNN.* https://edition.cnn.com/2024/10/15/asia/hong-kong-deepfake-romance-scam-intl-hnk

Safer Internet Lab

saferinternetlab.org

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

Find Us On

CSIS Indonesia | Safer Internet Lab