Safer Internet Lab
Led by CSIS in partnership with Google

Centre for Strategic and International Studies

Google

Research report

Online Fraud and Scams in Singapore

Safer Internet Lab

Online Fraud and Scams in Singapore

Joanna Octavia[1]

In recent years, Singapore has seen a surge of online scams, with cybercriminals using increasingly sophisticated tactics to defraud individuals and businesses. As a high-income market, Singapore is attractive for scammers, who target the affluent population and extensive digital connectivity. In 2024, Singapore recorded over 50,000 scam cases, equating to approximately one in every 100 people in Singapore falling victim (Abraham et al., 2024). According to the Global Anti-Scam Alliance (GASA), victims in Singapore suffered the highest average financial losses globally, surpassing victims in Switzerland and Austria (Wong, 2024b). The increasingly complex nature of these scams, combined with advancements in technology and the widespread use of AI, has exacerbated the problem.

As one of the most globally connected markets, Singapore's high levels of connectivity, along with its well-developed financial infrastructure and international banking links, make it an attractive target for scammers. In 2024, Singapore retained its position as the world's most financially inclusive market for the third consecutive year, reflecting the country's robust financial systems and widespread access to financial services (Principal, 2024). The country's strong digital connectivity further supports this status , with 99 per cent of households connected to the internet and 96 percent have smartphones in 2024 (IMDA, n.d.). However, the country's push toward a cashless society, supported by the widespread use of digital wallets, QR code payments and contactless transactions, has introduced new vulnerabilities that scammers can capitalise on. Singapore's digital economy, which is built on high levels of trust, further meant that people may be less sceptical about schemes that are fraudulent.

Despite having high digital literacy, Singapore remains vulnerable to online scam attacks. According to the Singapore Police Force, self-effected transfers made up 82.4 percent of all reported scam cases in Singapore in 2024, underscoring the significant role of social engineering in these scams (SPF, 2024a). This phenomenon can be attributed to several factors, such as the use of increasingly sophisticated scam tactics, overconfidence in detecting scams, and the exploitation of social values and trusted communication channels by scammers. To combat these challenges, the government is ramping up public-private collaboration between regulators, financial institutions and technology companies. Of note is the increased enforcement powers through the recent passage of the Protection from Scams Bill, continued collaboration between financial institutions and law enforcement, and public awareness raising.

[1] Associate Lecturer, University College London

CURRENT TRENDS

Social media and instant messaging

Social media platforms and instant messaging apps, both of which are central to communication and commerce, are ranked in the top two contact methods used by scammers (SPF, 2024a). The widespread use of these digital platforms, coupled with Singapore's high rate of social media adoption, made them a fertile ground for scammers to reach a large audience with ease. Three products from Meta, namely Facebook, WhatsApp and Instagram, remain consistently overrepresented among the platforms exploited by scammers (SPF, 2024a).

Social media platforms serve as a key tool for scammers to target and deceive potential victims. About 88 percent of Singapore's population use social media, making it a widely used and trusted communication channel (Technode Global, 2024). Among other uses, these platforms have been misused to advertise fake investment schemes; host fake accounts or pages that mimic legitimate organisations to run phishing schemes; and build rapport and relationships with potential victims through social engineering tactics (Koh, 2023; Chia, 2024b; Chiu, 2024; Sim, 2024).

Meanwhile, instant messaging apps are typically used as the more direct and private channel to manipulate victims. They are the most common means for scammers to contact potential victims, with WhatsApp and Telegram as two of the most widely exploited apps (SPF, 2024a). A survey published by GASA (see Abraham et al., 2024) found that nearly three-quarters of respondents were contacted by scammers via WhatsApp, highlighting how scammers exploit the speed, reach, and personal nature of these channels to target potential victims (Abraham et al., 2024). Documented uses of instant messaging apps in online scams in Singapore range from chat rooms perpetrating fraudulent investment schemes, to government official impersonation scams (Tan, 2025; Yasmine, 2025). However, scam-related content on these apps is often beyond direct government oversight due to their encryption and privacy features. Beyond private messaging, these apps also allow for rapid sharing, which can amplify the reach of scam content and make it difficult to contain.

Government official impersonation scams

Government official impersonation scams are one of two types of scams that cause higher losses than others, the other being investment scams (Yasmine, 2025). From January to October 2024, there have been at least 1100 cases reported with total losses amounting to at least SG$ 120 million, almost double to that in the same period in 2023 (MAS, 2025). These scams are highly effective in Singapore primarily due to the strong trust in government institutions and officials, as well as strict law enforcement and law penalties, which made victims fear getting into legal trouble.

Government official impersonation scams are complex schemes that typically involve multiple stages and several scammers. A scammer, posing as a bank officer, would call a potential victim and falsely claim that a victim's credit card was issued, or suspicious transactions had occurred. If the victim denies involvement, the scammer escalates the situation by transferring the call to an accomplice impersonating a Monetary Authority of Singapore (MAS) official or law enforcement officer. Using video calls, the scammers would attempt to build their credibility using fake credentials, agency logos, or fabricated warrant cards and official documents, before shifting the conversation to WhatsApp (MAS, 2024c). Once they are communicating through private messaging channels, the scammers would then pressure victims to transfer money to "safety accounts" under the guise of aiding investigations, ultimately stealing their funds (MAS, 2024c). The complexity of the schemes illustrates the sophisticated tactics employed by scammers. By using various methods and layers of deception, scammers make it difficult for victims to detect that they have been manipulated until it is too late.

Cryptocurrency and investment scams

The rising popularity of cryptocurrencies in Singapore provided a way for scammers to lure victims in Singapore into seemingly lucrative cryptocurrency investments, which are fake. The general public's limited understanding of crypto's risks, combined with the hype around digital assets, made them an effective attraction for victims who may not fully grasp the risks involved. Investment scams comprise the highest total amount lost compared to other types of scams in Singapore, reaching at least SG$320.7 million in 2024, underscoring their severity and financial impact (SPF, 2024a).

Investment scams in Singapore leverage the growing interest in cryptocurrencies and the opaque, complex nature of digital assets. After meeting on digital platforms like Facebook, Instagram, Telegram or dating apps, scammers would encourage investment scam victims to invest a small amount of money at the start, which - following a small 'profit' - would be followed by escalation of investment (Police warns of investment scams, 2025). They are asked to open accounts at crypto exchanges and transfer money to the account to buy cryptocurrencies. Once larger amounts of monies or cryptocurrencies have been transferred by the victims to a fraudulent trading platform or the scammers' own wallets, they would begin to experience difficulties in withdrawing their 'investments' (SPF, 2024a; Police warns of investment scams, 2025). In other instances, victims are defrauded by fake advertisements on social media platforms such as Facebook or Instagram, featuring false endorsements from political figures or celebrities, which lead them to messaging platforms or fraudulent trading sites (Police warns of investment scams, 2025).

The increased vulnerability of younger people to online investment scams is a concern. The majority of investment scam victims were aged 30 to 49, making up 44.2 percent of victims of this scam type (SPF, 2024a). This age group's active pursuit of investment opportunities makes them prime targets for scammers, who use the allure of quick returns to persuade them into making risky investment decisions.

Job Scams and Singpass credentials

Another recent phenomenon in Singapore's online scam landscape involves the compromising of Singpass (Singapore Personal Access). Singpass is a key digital identity system that provides access to government services and transactions. Scams involving Singpass have serious implications, as scammers can use it to commit identity theft, gain access to the victim's bank details, or make changes to official government records.

The most common method used by scammers is posting fraudulent job offers online or on communication platforms. In one recent case, some suspects were found to have allegedly sold their Singpass credentials for S$10,000 each, with the credentials then being used by scammers to open bank accounts and register for mobile phone lines (Koh, 2024). In other instances, scammers would send screenshots of Singpass QR codes and ask the victims to scan the code with their mobile phones, so that their personal information can be checked for the job (At least 219 victims duped, 2024). To address this growing problem, banks in Singapore will progressively implement Singpass face verification to strengthen authentication methods (MAS, 2024a).

Selling or giving away Singpass credentials to scammers is fundamentally different from falling for other scam types, as it is considered a criminal offense in Singapore. Those who willingly sell or give away Singpass credentials are legally liable for facilitating scam activities and will be treated as an accomplice rather than as a scam victim. The prevalence of scams involving Singpass exploits the public's digital trust in the government-linked digital identity system, indicating a lack of awareness of how their credentials can be misused.

Overconfidence in identifying scams

Users in Singapore exhibit overconfidence in identifying scams, which can be a significant risk in the digital age, where scams are becoming increasingly sophisticated. A survey by GASA (see Abraham et al., 2024) indicates that 62 per cent of survey respondents in Singapore are confident in identifying scams. Similarly, in a recent survey conducted by the Ministry of Digital Development and Information (MDDI), 56 percent of respondents across all age groups were moderately or extremely confident about identifying scam calls, while 45 percent felt the same about identifying scams on social media (Tan, 2024). However, 67 per cent of those aged 15 to 29 reported that they were either moderately or extremely confident in spotting scams on messaging platforms (Tan, 2024). However, the reality suggests that young people may not be as scam-savvy as they believe, with 29.7 per cent of scam victims aged 29 and below (SPF, 2024a). When the age group was expanded to include individuals under 50, 70.9 per cent of scam victims were found to be youths, young adults, and adults under 50 (SPF, 2024a).

People's confidence in their ability to spot online scams often do not match their actual success in detecting them (Wang et al., 2016). When many individuals, particularly those who spend much of their time online, believe they are capable of spotting fraudulent activity easily, this could lead to a false sense of security. Overconfidence can result in lower levels of vigilance, which causes people to overlook subtle red flags or dismiss warning signs. This may help explain why, despite high levels of digital literacy, users in Singapore remain vulnerable to falling for online scams.

Increased vulnerability of elderly individuals

The increased vulnerability of elderly individuals is a significant concern. While the elderly represent one of the smaller age groups among scam victims in Singapore, the amount they lose per incident is significantly higher than that of victims in other age groups (SPF, 2024a). This is especially concerning because the financial losses sustained from such scams have the potential to deplete their life savings. Unlike younger people, they often lack the time and resources to rebuild their financial security after falling for a scam.

Many elderly individuals are susceptible to online scams due to their limited familiarity with digital platforms and heightened trust in strangers. This vulnerability may be in part attributed to their social isolation and loneliness (Wen et al., 2022). In one case, a 74-year-old man chatted online for six hours with a friendly roast duck seller he met on Facebook, who turned out to be a scammer who infected his phone with malware and syphoned funds from his online bank accounts (Sim, 2024). In another case, a 65-year-old Singaporean retiree lost her life savings of more than SG$1 million after falling for a scam by a Facebook friend (Hamzah, 2024). As online scams are becoming more sophisticated, the elderly are at heightened risk of falling for digital deception, which could have long-term impacts on their financial and emotional well-being if left unaddressed.

MISUSE OF AI IN SCAMS IN SINGAPORE

The misuse of AI across the value chain has revolutionised the way scams targeting individuals in Singapore are conducted, making them more sophisticated and difficult to detect. AI is used in a variety of ways in scams targeting users in Singapore, ranging from chatbots that generate phishing emails at scale, to deepfake videos and voice cloning techniques used to impersonate trusted figures (Cyber Security Agency of Singapore, 2023; Chiu, 2024; Koh, 2023). Most Singaporeans have expressed a high level of awareness of the negative effects of AI technology on online scams, though this remains lower for AI-generated voices and videos (Abraham et al., 2024).

One observable trend in Singapore is the use of AI-powered chatbots like ChatGPT, which have facilitated the production of phishing emails and messages at scale. By using generative AI, messages have become more official-sounding with near-perfect language, mimicking genuine e-mails and messages from various organisations (Chia, 2024a). An example of this involved scammers posing as Consumers Association of Singapore (Case) officers distributing fake surveys via WhatsApp (Qing, 2024). Coupled with other tactics to make the scams look more credible, such as by using the https protocol and .com links, leveraging AI advancements make scam attempts harder to detect, as the language appears to be credible (Chia, 2024a).

Another notable trend is the increasingly sophisticated scams using deepfake technology. To illustrate the scale of the challenge, Singapore is facing an increase of 240 percent in deepfake attacks, the second highest in Asia-Pacific jointly with Cambodia (Koh, 2024). Scammers are leveraging AI to create realistic audio and video of trusted figures, such as government officials, in an attempt to deceive victims into believing that what they are seeing and hearing is genuine. Footage of Singapore's leaders Prime Minister Lawrence Wong and Senior Minister Lee Hsien-Loong were used to promote fraudulent investment products and circulated on social media platforms (Chiu, 2024; Koh, 2023). Deepfakes are also being used to create fake social media profiles, with a local Hong Kong syndicate found to have approached victims in Singapore with deepfaked images of good-looking women they found online (Ma, 2025).

There is emerging evidence that deepfakes are used in scams targeting individual users in Singapore. It is believed that these digital manipulations were used to change the appearances of scammers impersonating government officials or other high-ranking executives to persuade victims (MAS, 2025). Another risk involves the use of localised accents in deepfake audio, which can make scam calls appear far more authentic and difficult to detect. Victims in Singapore, who are used to specific local speech patterns, are more likely to trust a voice that sounds familiar, as opposed to distinctly foreign accents (Ng, 2025). The Cyber Security Agency of Singapore (2024, p.15) noted that the use of deepfake technology in online scams will continue to grow, "given the widespread accessibility of tools to create highly convincing deepfakes at a relatively low cost". That deepfake technology will be increasingly used in scams has caused widespread worry in Singapore, with more than three-quarters citizens and permanent residents expressing concern (Verian, 2024).

The value chain of AI-powered scams extends beyond Singapore, involving international networks of criminals from outside of the country, often based in other Southeast Asian countries or beyond (UNODC, 2024). These syndicates typically operate from countries with more lax regulatory environments or less stringent enforcement against cybercrime and extend their reach to Singapore by using digital platforms and untraceable payment methods to scam victims. Although online scams operate cross-border, digital governance fragmentation means that cybercrime laws are specific to local jurisdictions, making them difficult to enforce. Meanwhile, there is growing evidence of cross-border operations targeting users in Singapore. In January 2025, Hong Kong police arrested 31 individuals from a local syndicate involved in creating deepfake romance and investment scams to defraud victims in several countries, including Singapore (Ma, 2025). Syndicates capitalise on the transnational nature of these scams by combining social engineering tactics with AI-driven tools, tailoring their strategies to suit specific cultural and economic contexts. This targeted approach enhances the credibility of their scams and makes them seem more convincing.

POLICY GAPS

The Singaporean government has implemented a multi-layered strategy to combat online scams, focusing on prevention, enforcement, and public education. The Protection from Scams Bill, which was passed by the Singapore Parliament in January 2025 and expected to take effect in the second half of 2025, seeks to tackle the increasing number of self-effected transfers, in which victims willingly transfer the funds to scammers. To address this challenge, the bill empowers the police to issue Restriction Orders (ROs) to temporarily freeze the bank accounts of individuals suspected of falling victim to scams (Rajah & Tann Singapore, 2025). Despite critics of the Bill have argued that it may actively interfere with individuals' financial autonomy, the Bill is not expected to have much pushback from the public (Sun, 2024). A policy gap is that the Bill is relatively limited in scope, since the ROs currently do not cover other entities that are often involved in scam workflows such as cryptocurrency exchanges and e-wallet providers (Rajah & Tann Singapore, 2025; Sun, 2025).

Singapore is driving specific measures that digital platforms must adopt to prevent scam activities online. The Online Criminal Harms Act (OCHA), effective 1 February 2024, requires digital platforms such as Carousell and Facebook Marketplace to verify 'risky' sellers and advertisers against government-issued records (Lee & Tan, 2024). Facebook has since required all its advertisers to verify their identities by the end of June 2025, following a 12 per cent rise in scam ad reports during a pilot test from June to December 2024 (Chia, 2025). Carousell, on the other hand, was granted a six-month extension to reduce scams after showing an 11 per cent decline, but must verify all sellers by October if improvements stall (Chia, 2025). Meanwhile, platforms like Facebook, WhatsApp, Instagram, Telegram and WeChat are mandated to create a fast-track channel to receive and act on reports from the authorities (Lee & Tan, 2024). However, while the current law focuses on sellers and advertisers verification, scammers can also operate as buyers, creating a policy gap (Hamzah, 2024b). Another gap also exists when messaging apps like Instagram or Whatsapp, which are classified as online communication services, are used for informal e-commerce by scammers. In these scams, scammers can bypass government ID verification rules required for traditional ecommerce sites. Additionally, there is limited oversight if transactions are taken off-platform.

The government has also initiated efforts to enhance accountability among stakeholders in tackling online scams. Established by MAS, the Shared Responsibility Framework (SRF) aims to complement legislative efforts by distributing accountability for phishing scams between consumers, financial institutions, and telecommunication operators (telcos) (MAS, 2024b).. However, the framework excludes scams where victims authorise payments to the scammer (i.e., self-effected transfers), as well as scams where victims were deceived into giving away credentials to the scammer directly. This means that scams with the highest total amount lost, such as investment scams and government official impersonation scams, are not covered by the SRF.

Singapore's current regulations do not explicitly address deepfakes, but there are several measures that can indirectly tackle this issue. The Protection from Online Falsehoods and Manipulation Act (POFMA) addresses the spread of falsehoods online and can be used to address manipulated content (Government of Singapore, 2025). Additionally, OCHA allows the government to direct digital platforms to remove potential scam related content, including those that are deepfake-enabled, to reach Singapore users (Ministry of Digital Development and Information, 2024). This is being complemented by efforts to strengthen the government's capabilities in addressing these threats, such as through industry collaboration and technological development of deepfakes detection by the SPF and the Home Team Science and Technology Agency (HTX) (Ministry of Digital Development and Information, 2024). The government has stated that laws such as POFMA and OCHA can be used to address deepfakes in contexts outside of elections (Teo, 2024). Furthermore, the government has also publicly indicated its intent to introduce a Code of Practice on how to handle digitally manipulated content beyond election periods, suggesting a policy shift towards preventive measures in content governance (Rise of AI and deepfakes, 2025).

Beyond regulatory intervention, multi-stakeholder and cross-border collaborations are central to the Singaporean government's effort in tackling online scams. The SPF has established the Anti-Scam Command (ASCom) to coordinate efforts across various agencies to address scams in real time. The ASCom is a dedicated unit within the SPF that proactively detects and intervenes in potential scam situations by collaborating with banks and digital platforms. With staff from major banks co-located at the centre and leveraging advanced Robotic Process Automation technology to automate the process of information sharing and processing, the combined expertise of key stakeholders has the potential to strengthen the public safeguards against online scams (SPF, 2024b). This success was demonstrated by the recovery of more than US$310 million from scammers between 2019 and 2023 (Wong, 2024a). Additionally, the ASCom also serves as a point of contact for cross-border collaborations. For example, ASCom and Malaysia's National Scam Response Centre (NRSC) successfully ran a joint anti-scam operation between February and March 2025, freezing more than 3400 bank accounts (Lim, 2025). While the ASCom has made significant strides in combating scams through its collaborative approach, there is still room for improvement, such as increasing the involvement of digital platforms involved in the scam workflow beyond Carousell and Shopee and enhancing cross-border cooperation with countries identified as scam hotspots (Chua, 2024).

Public education is another key pillar of Singapore's anti-scam efforts. Singapore has launched large-scale national anti-scam campaigns, such as the 'I can ACT against scams' campaign launched in January 2023. In the omni-channel campaign, anti-scam messages and advisories are widely disseminated across various channels, including television, radio advertisements, posters, digital ads, and local news outlets, typically with more publicity when there are emerging scam variants (Ministry of Home Affairs, 2024). Another notable innovation is the ScamShield app, which helps users to identify and block potential scam calls and messages. It also educates users about scam types and includes real-time alerts (Theseira, 2024). An important area to explore further is whether public education is backed by robust networks that can effectively reach and engage the most vulnerable communities, alongside the integration of comprehensive impact analysis.

POLICY RECOMMENDATIONS

Based on the identified gaps, the following are several recommendations that could improve the existing measures:

1. **Expand the scope of scam prevention:** The Protection from Scams Bill should explicitly include other entities such as cryptocurrency exchanges and e-wallet providers. This will ensure a more comprehensive framework for scam prevention across digital financial services.
2. **Enhance collaborative frameworks for combating online scams**: This could involve clarifying the roles and responsibilities of various stakeholders, including government bodies, digital platforms, and financial institutions, in addressing scam-related content and activities. Exploring incentives for proactive scam prevention measures across the digital ecosystem, potentially drawing on existing models like the SRF, could be beneficial. Additionally, the development and promotion of secure online transaction payment options that prioritise user safety are critical to maintaining a trustworthy digital ecosystem. Reviewing codes of practice for converging online communication and e-commerce services may also be necessary to establish clearer, shared expectations for mitigating risks. Furthermore, fostering strengthened actions by law enforcement, alongside supportive multi-stakeholder cooperation, is crucial to tackling the organized criminal networks as the root cause, which are understood to be a primary source of the issue.
3. **Include deepfakes in broader online harm prevention:** Given that Singapore already has a robust legal framework to address online harms, strengthening and expanding existing laws could be a viable alternative to creating standalone deepfake regulations. One way to do so can be by enhancing the Code of Practice for Online Communication Services to include specific provisions for detection and labeling.
4. **Implement active deepfake detection and traceability measures:** Digital platforms should be expected to develop and adopt AI-driven tools for deepfake detection and proactively labelling them when they appear on the platform. In particular, private messaging apps like WhatsApp would benefit from centralised content scanning system that can actively flag scam-related deepfake content. Additionally, tracing the origin, alterations, and distribution of content can help curb the spread of deepfakes at their source.
5. **Strengthen informal networks as support for vulnerable groups:** Data has shown that the elderly are at risk of losing large amounts of funds - including their life savings - to online scams, while younger people are increasingly more vulnerable to investment scams. To help mitigate these risks, informal networks such as family members, close friends and community

groups or leaders can play a crucial role in strengthening community bonds, sharing best practices for anti-scam prevention, and providing support.

6. **Conduct comprehensive impact analysis:** Impact analysis can assess how well interventions have reduced users' vulnerability to social engineering tactics, which underlie much of the self-affected transfers. Understanding the effectiveness of existing strategies can reveal areas where users are still susceptible to manipulation and help design more targeted approaches.
7. **Improve the participation of digital platforms at Anti-Scam Command:** Requiring digital platforms to engage with the Anti-Scam Command as a proportionate response when platforms are found to be behaving irresponsibly would foster a more coordinated approach to tackling scams in Singapore. This targeted strategy allocates resources and oversight where they are needed by focusing on platforms that have demonstrated a need for improved scam prevention outcomes.
8. **Strengthen regional cooperation:** Scam syndicates operating in other Southeast Asian countries like Cambodia or Myanmar can be difficult to track and prosecute due to differences in governance, as well as varied levels in law enforcement and cybersecurity capabilities. Greater regional cooperation through ASEAN could help standardise approaches and improve unified responses to cross-border online scams across Southeast Asia. This should include standards for criminalising the use of deepfakes for malicious purposes, such as scams.

REFERENCES

At least 219 victims duped into revealing Singpass credentials to scammers since January. (2024, May 19). *The Straits Times.* https://www.straitstimes.com/singapore/at-least-219-victims-duped-into-revealing-singpass-credentials-to-scammers-since-january

Abraham, J., Rogers, S., Njoki, C., & Greening, J. (2024). *The State of Scams in Singapore 2024.* Global Anti-Scam Alliance. https://www.gasa.org/_files/ugd/7bdaac_7dceee4e90f9493eac18bccb1425304f.pdf

Chia, O. (2024a, July 30). 13% of phishing scams analysed likely to be AI-generated: CSA. *The Straits Times*. https://www.straitstimes.com/singapore/13-of-phishing-scams-analysed-likely-to-be-ai-generated-csa

Chia, O. (2024b, October 30). Look out for these scams on Facebook, Instagram and WhatsApp. *The Straits Times*. https://www.straitstimes.com/singapore/look-out-for-these-scams-on-facebook-instagram-and-whatsapp

Chia, O. (2025, March 11). Facebook advertisers must verify their identities by end-June following rise of scam ads. The Straits Times. https://www.straitstimes.com/singapore/all-facebook-advertisers-need-to-verify-identity-by-june-following-rise-of-scam-ads

Chiu, C. (2024, January 4). PM Lee warns against responding to deepfake videos of him promoting investment scams. *The Straits Times*. https://www.straitstimes.com/singapore/pm-lee-warns-against-responding-to-deepfake-videos-of-him-promoting-investment-scams

Chua, N. (2024, May 9). MHA to consider mandating deployment of staff from online platforms to police's Anti-Scam Command. *The Straits Times*. https://www.straitstimes.com/singapore/politics/mha-to-consider-mandating-deployment-of-staff-from-online-platforms-to-police-s-anti-scam-command

Cyber Security Agency of Singapore. (2024). *Singapore Cyber Landscape 2023*. https://www.csa.gov.sg/resources/publications/singapore-cyber-landscape-2023/

Government of Singapore. (2025, March 20). *Singapore's fight against Misinformation*. https://www.gov.sg/explainers/singapore-fight-against-misinformation

Hamzah, A. (2024, November 13). Over $1m lost in 15 days: S'porean retiree loses life savings in scam by fake Facebook friend. *The Straits Times*. https://www.straitstimes.com/singapore/gone-in-15-days-40-years-of-savings-amounting-to-more-than-1-million

Hamzah, A. (2024, November 25). At least 877 people duped by fake buyers on Carousell since December. *The Straits Times.* https://www.straitstimes.com/singapore/at-least-877-people-duped-by-fake-buyers-on-carousell-since-december

Digital Society. (n.d.). Infocomm Media Development Authority. https://www.imda.gov.sg/About-IMDA/Research-and-Statistics/Digital-Society

Koh, S. (2023, December 29). Deepfake video of DPM Lawrence Wong promoting investment scam circulating on social media. *The Straits Times*. https://www.straitstimes.com/singapore/deepfake-video-of-dpm-lawrence-wong-promoting-investment-scam-circulating-on-social-media

Koh, S. (2024, April 23). 78 people probed for allegedly giving Singpass details to scammers. *The Straits Times.*

https://www.straitstimes.com/singapore/courts-crime/78-people-investigated-for-allegedly-giving-singpass-details-to-scammers

Koh, F. (2024, 22 November). Singapore registers Asia-Pacific's biggest spike in identity fraud, driven by deepfake surge. https://www.channelnewsasia.com/singapore/identity-fraud-deepfakes-scams-ai-4761836

Lee, L. Y. & Tan, C. (2024, June 29). New codes of practice require Carousell, Facebook to verify 'risky' sellers, advertisers to curb scams. *The Straits Times*. https://www.straitstimes.com/singapore/new-codes-of-practice-require-carousell-facebook-to-verify-risky-sellers-advertisers-to-curb-scams

Lim, K. (2025, March 19). More than 850 people being investigated in Singapore-Malaysia joint anti-scam operation; victims lost at least $8.1m. A*siaOne.* https://www.asiaone.com/singapore/more-850-people-being-investigated-singapore-malaysia-joint-anti-scam-operation-victims

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 Development and Information. (2024, February 24). *MCI's response to PQ on Regulations to Tackle Deepfake Software Used in Scam and Fraud Cases*. https://www.mddi.gov.sg/media-centre/parliamentary-questions/pq-on-regulations-to-tackle-deepfake-software/

Ministry of Home Affairs. (2024, January 9). *Written Reply to Parliamentary Question on Frequency of Anti-Scam Campaigns in the Media.* http://mha.gov.sg/mediaroom/parliamentary/written-reply-to-pq-on-frequency-of-anti-scam-campaigns-in-the-media/

Monetary Authority of Singapore. (2024a, September 18). *Major retail banks to introduce Singpass Face Verification, further strengthening resilience against phishing scams* [Press release]. https://www.mas.gov.sg/news/media-releases/2024/major-retail-banks-to-introduce-singpass-face-verification

Monetary Authority of Singapore. (2024b, October 24). *MAS and IMDA Announce Implementation of Shared Responsibility Framework from 16 December 2024* [Press release]. https://www.mas.gov.sg/news/media-releases/2024/mas-and-imda-announce-implementation-of-shared-responsibility-framework-from-16-december-2024

Monetary Authority of Singapore. (2024c, November 30). *Joint Advisory on Rise of Government Official Impersonation Scam Variant Featuring Impersonation of Banks* [Press release]. https://www.mas.gov.sg/news/media-releases/2024/rise-in-government-official-impersonation-scam-variant

Monetary Authority of Singapore. (2025, March 12). *Joint Advisory on Scams Involving Digital Manipulation* [Press release]. https://www.mas.gov.sg/news/media-releases/2025/joint-pnr-by-spf-mas-and-csa

Ng, D. (2025, March 19). Commentary: A close call showed me that anyone can get scammed – even me. *Channel News Asia.* https://www.channelnewsasia.com/commentary/scam-phone-call-fraud-prevention-awareness-4997496

Police warns of investment scams; at least $32.6 million lost in over a month. (2025, February 11). *CNA*. https://www.channelnewsasia.com/singapore/investment-scams-victims-social-media-dating-app-coffee-meets-bagel-4930741

Principal. (2024). 2024 Global Financial Inclusion Index. https://www.principal.com/financial-inclusion

Qing, A. (2024, November 22). Shopping survey on WhatsApp that offers $13 payment is a new scam, warns Case. *The Straits Times*. https://www.straitstimes.com/singapore/case-warns-against-scam-on-whatsapp-which-promises-13-for-completing-fake-survey

Rajah & Tann Singapore. (2025, February 7). *Protection from Scams Bill Passed in Parliament.* https://sg.rajahtannasia.com/viewpoints/protection-from-scams-bill-passed-in-parliament/

Rise of AI and deepfakes in lead-up to GE2025. (2025, April 11). Channel News Asia. https://www.channelnewsasia.com/interactive/ge2025-deepfake/

Sim, S. (2024, November 15). 74-year old man loses $70k after downloading third-party app to buy Peking duck. *The Straits Times.* https://www.straitstimes.com/singapore/74-year-old-man-loses-70k-after-downloading-third-party-app-to-buy-roast-duck

Singapore Police Force. (2024a). *Annual Scams and Cybercrime Brief 2024.* https://www.police.gov.sg/Media-Room/Police-Life/2025/02/Five-Things-You-Should-Know-about-the-Annual-Scams-and-Cybercrime-Brief-2024

Singapore Police Force. (2024b, September 6). *Joint operation between the Anti-Scam Centre and six partnering banks led to the disruption of more than 2,016 scams* [Press release].

https://www.police.gov.sg/media-room/news/20240906_joint_operation_between_the_anti_scam_centre

Sun, D. (2024, November 17). How did S'pore end up needing 'nanny' laws to save scam victims from themselves? *The Straits Times*. https://www.straitstimes.com/singapore/how-did-we-end-up-needing-nanny-laws-to-save-scam-victims-from-themselves

Sun, X. (2025, January 7). *Second Reading of the Protection From Scams Bill - Wrap-Up Speech by Ms Sun Xueling, Minister of State, Ministry of Home Affairs and Ministry of Social and Family Development* [Transcript]. Ministry of Home Affairs. https://www.mha.gov.sg/mediaroom/parliamentary/second-reading-of-the-protection-from-scams-bill-wrap-up-speech/

Tan, C. (2024, November 14). Young people say in MCI survey say they can identify scams, but police crime statistics show otherwise. *The Straits Times*. https://www.straitstimes.com/singapore/courts-crime/young-people-say-in-mci-survey-they-can-identify-scams-but-police-crime-statistics-show-otherwise

Tan, C. (2025, March 19). Woman loses $1.2m to scammers who pretended to be officers from police's Anti-Scam Centre. https://www.straitstimes.com/singapore/woman-loses-1-2m-to-scammers-who-pretended-to-be-officers-from-polices-anti-scam-centre

Technode Global. (2025, February 11). *Digital 2025: Nearly Two Thirds of Southeast Asia's Population are on Social Media.* https://technode.global/2025/02/11/digital-2025-nearly-two-thirds-of-southeast-asias-population-are-on-social-media/

Teo, J. (2024, October 15). Closing Speech by Minister Josephine Teo at the Second Reading of the ELIONA Bill. Ministry of Digital Development and Information. https://www.mddi.gov.sg/closing-speech-by-minister-josephine-teo-at-the-second-reading-of-the-eliona-bill/

Theseira, J. (2024, September 29). Easier to check, report and recall: How the new ScamShield Suite can help you outsmart scammers. *The Straits Times*. https://www.straitstimes.com/singapore/easier-to-check-report-and-recall-how-the-new-scamshield-suite-can-help-you-outsmart-scammers

United Nations Office on Drugs and Crime (UNODC). (2024). *Transnational Organised Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape.*

https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

Verian. (2024, April 8). *Three quarters of Singaporeans concerned about the use of deepfakes in scams.* https://www.veriangroup.com/news-and-insights/three-quarters-of-singaporeans-concerned-about-the-use-of-deepfakes-in-scams

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in Phishing Email Detection. *Journal of the Association for Information Systems, 17*(11), 759-783. https://doi.org/10.17705/1jais.00442

Wen, J., Yang, H., Zhang, Q., & Shao, J. (2022). Understanding the mechanisms underlying the effects of loneliness on vulnerability to fraud among older adults. *Journal of Elder Abuse and Neglect, 34*(1), 1-19. https://doi.org/10.1080/08946566.2021.2024105

Wong, S. (2024a, August 4). More countries set up anti-scam centres: increased teamwork, speed vital to retrieve lost funds: SPF. https://www.straitstimes.com/singapore/more-countries-set-up-anti-scam-centres-increased-teamwork-speed-vital-to-retrieve-lost-funds-spf

Wong, S. (2024b, November 13). $1.4 trillion lost to scams globally: S'pore victims lost the most on average: Study. *The Straits Times*. https://www.straitstimes.com/world/14-trillion-lost-to-scams-globally-s-pore-victims-lost-the-most-on-average-study

Yasmine, R. (2025, February 9). Over $1.32 million seized, 46 people arrested in operation targeting higher-loss scams. *The Straits Times*. https://www.straitstimes.com/singapore/over-1-32m-seized-46-people-arrested-in-operation-targeting-higher-loss-scams

Safer Internet Lab

saferinternetlab.org

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

Find Us On

CSIS Indonesia | Safer Internet Lab