Protecting A Nation Under Digital Siege

In August 2021, twenty-one-year-old police full-time national serviceman Finnegan Tan Yao Jie took his service revolver to a bathroom at the Special Operations Command base and ended his life with a gunshot to the head.[1]

Tan had recently lost $10,000 to a scam. He had written on his private Instagram account that he had spent the last few months trying to improve his situation, but "blew it by being a victim of a scam".[2]

This tragic incident underscored the devastating personal toll of digital scams in Singapore, a global hub for technology and finance that was grappling with a rapidly escalating crisis. In 2024, Singapore experienced a staggering $1.1 billion in losses from scams, up 70.6% from $651.8 million in 2023.[3] Scam cases surged by 213.9% between 2020 and 2024 (Figure 1), and Singaporeans lost more money per person – an average of US$4,031 each – to scams than any other country in 2023.[4]

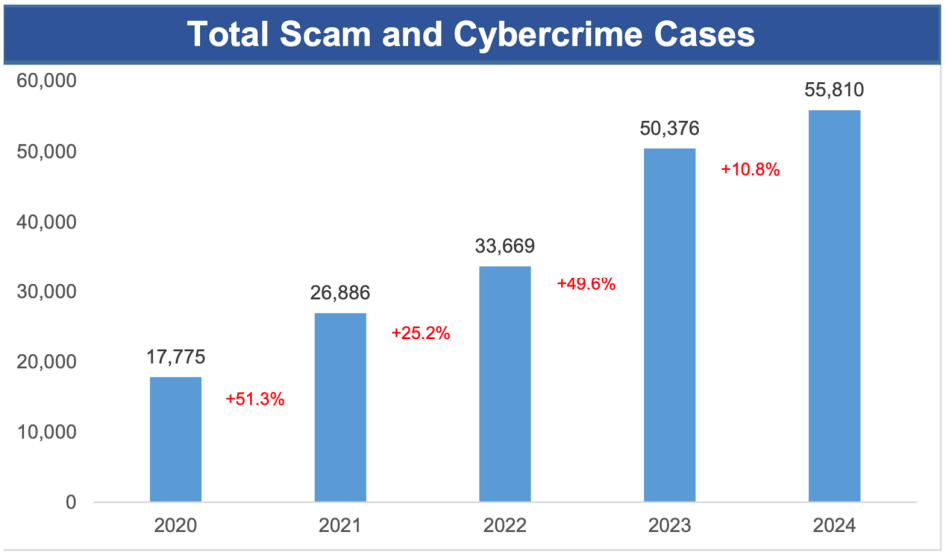


Figure 1: The number of scam and cybercrime cases in Singapore from 2020 to 2024.
Source: Singapore Police Force, "Annual Scams and Cybercrime Brief 2024".

[1] Shaffiq Alkhatib, "Police NSF who died from gunshot wound had lost over $10,000 in a scam: Coroner's Inquiry", *The Straits Times*, February 2, 2023, https://www.straitstimes.com/singapore/courts-crime/firearms-ban-was-considered-for-police-nsf-before-he-was-found-dead-with-gunshot-wound-coroner-s-inquiry?ref=inline-article.
[2] Christine Tan, "Police NSF who died from gunshot wound after losing $10k to scam ruled a suicide: Coroner", *The Straits Times*, August 11, 2023, https://www.straitstimes.com/singapore/courts-crime/police-nsf-who-died-from-gunshot-wound-after-losing-10k-to-scam-ruled-a-suicide-coroner.
[3] Singapore Police Force, "Annual Scams and Cybercrime Brief 2024", 1.
[4] Owen Walker, "'Rich and naive': why Singapore is engulfed in a 'scamdemic'", *Financial Times*, May 26, 2025, https://www.ft.com/content/3299cf7e-67bd-4654-8aa9-55fc24a66b63.

This case was written by Tara Thean Mei Feng under the guidance of Ng Kok Hoe and Jean Chia, Lee Kuan Yew School of Public Policy (LKY School), National University of Singapore and has been funded by the Lee Kuan Yew School of Public Policy. The case does not reflect the views of the sponsoring organisation nor is it intended to suggest correct or incorrect handling of the situation depicted. The case is not intended to serve as a primary source of data and is meant solely for class discussion.

Copyright © 2025 by the Lee Kuan Yew School of Public Policy at the National University of Singapore. All rights reserved. This publication can only be used for teaching purposes.

Box 1: Scam incidents in Singapore

Scams in Singapore ran the gamut from emotional manipulation to sophisticated digital fraud. Below are three real-life examples:

1. The Tanah Merah Love Scam

John (not his real name), a man with an intellectual disability, waited at the Tanah Merah ferry terminal for a person he had met online with an attractive social media picture. Their conversations were deep, and John's feelings for her intensified: he wanted to marry this person. He transferred over $100 to her, and the pair arranged for the woman to visit him in Singapore. Unfortunately, she was a no-show at the ferry terminal and abruptly cut off contact with John. People with intellectual disabilities are a prime target for scams, thanks to a desire for connection with others as well as a compromised ability to evaluate danger and recognise deceit.

2. The MNC Deepfake Scam

A multinational corporation's finance director received a WhatsApp message asking him to take part in a Zoom video call to discuss the restructuring of the firm's business and to speak to a law firm representative. The company's chief executive officer and various others joined the Zoom call – but the chief executive officer and the others were actually deepfakes, or AI-generated impersonators. The impersonators instructed the finance director to send US$499,000 from the company's bank account to a different bank account.

3. The $20,000 "Quishing" Bubble Tea Shop Scam

A 60-year-old woman scanned a QR code on a bubble tea shop window that promised a free drink for completing an online survey. The QR code led her to download a third-party phone app that gave scammers access to her phone, resulting in an unauthorised transfer of $20,000 from her bank account. In incidents such as this one, the app typically contained malware that allowed fraudsters to view and control a victim's phone screen. When the victim used their mobile banking app, the scammer could then obtain their login credentials and password. The scammer could also access their camera to see when the victim might be inactive and not using their phone, such as when they were sleeping – the perfect moment for the scammer to take over their phone and wipe out their savings.

Beyond the financial losses, scams such as these had a range of damaging non-financial impacts. The betrayal of trust could cause lasting emotional scars – John, for example, was heartbroken – and lead to depression and anxiety. Individuals with disabilities, the elderly and others with limited digital literacy often felt particularly targeted, exacerbating feelings of powerlessness and social exclusion. The fear of being scammed again could create chronic stress. Individuals could also suffer reputational damage, particularly if a scam led them to make poor decisions in their workplaces or professional lives. Meanwhile, repeated exposure to scams could lead to a heightened sense of vulnerability and mistrust towards institutions, digital platforms or even everyday communications. This erosion of trust could reduce engagement with digital services or government initiatives, which was especially problematic in highly digitised societies such as Singapore.

At the time of writing, the most popular scams included:[5]

1. Phishing scams, which deceived victims into handing over personal information such login credentials or credit card details by posing as trusted organisations and manufacturing a false sense of urgency;

2. Job scams, where scammers offered easy work-from-home jobs such as "liking" social media posts or completing surveys, paid a small commission at first to build trust and then tricked victims into transferring money with empty promises of repayment and commission;

3. E-commerce scams, where fraudsters posted fake listings with huge discounts on shopping platforms, then disappeared after payment;

4. Investment scams, which lured victims with get-rich-quick promises of high returns in areas such as cryptocurrency, real estate or even durians, but typically ended with the scammer disappearing or inventing extra fees to extract more money;

5. Fake friend call scams, where scammers pretended to be a long-lost friend with a sob story, tricking victims into giving them a loan.

Different age groups tended to fall prey to different types of scams. While most scam victims were under the age of 65 (Figure 2), elderly individuals suffered disproportionately higher financial losses on average. The Singapore government faced a complex battle to combat the relentless innovation of scams in a highly connected society where diverse groups faced evolving threats, and global technological trends created new vulnerabilities.

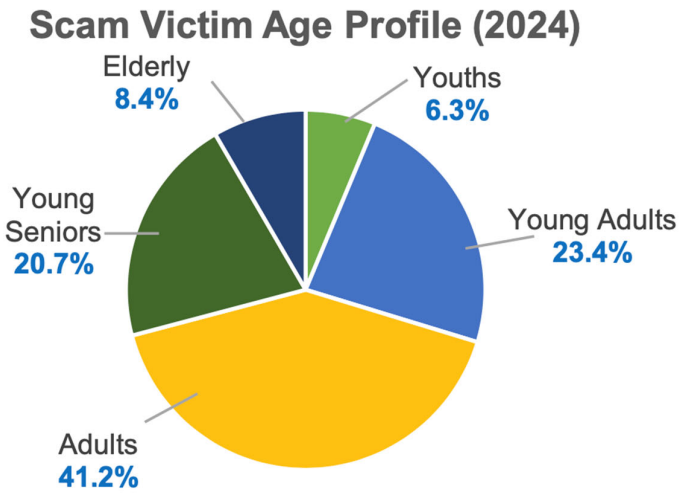


Figure 2: The age profiles of Singapore's scam victims. "Elderly" refers to those aged 65 and above.
Source: Singapore Police Force, "Annual Scams and Cybercrime Brief 2024".

[5] Government Technology Agency, "Top 5 scams in Singapore & how to avoid them (2025)", September 7, 2023, https://www.tech.gov.sg/technews/top-five-scams-in-singapore-and-how-to-protect-yourself.

Singapore's Unique Vulnerability

Digitalisation had reshaped modern life in recent decades. The very structure of how societies lived, worked and connected had undergone profound change, and Singapore was no exception. Indeed, the city-state was among the world's most digitally advanced nations. Government services, financial transactions, daily conveniences and interpersonal communication were seamlessly integrated into a highly connected digital ecosystem. This ecosystem marked a dramatic evolution from the country's humble beginnings as a developing island nation.

This remarkable digital success had brought Singapore immense efficiency and convenience, but had also created a unique set of vulnerabilities. The very qualities that had made Singapore a digital frontrunner – near-total connectivity, advanced digital infrastructure, a population accustomed to speed and efficiency – had driven significant economic and social progress. They had also created a fertile environment and new avenues for online scams to thrive, exposing structural and behavioural weaknesses that scammers were quick to exploit.

High Internet and Smartphone Penetration

Even the briefest stroll through Singapore made clear that life in the city-state ran on screens. Waiting for a meal at a hawker centre, traveling across town on the MRT, hanging out with friends in the Botanic Gardens – in all these scenarios, it was common to see residents with their heads down, immersed in their smartphones, mediating their interactions with the world through a screen. The numbers backed this observation up: 97% of residents owned smartphones, and smartphone penetration was high even among the over-65s at 89%.[6] Nearly 100% of resident households had internet connectivity.[7]

With nearly all of the population digitally connected in some form, digital platforms were the default mode of communication and transaction. This always-online culture gave scammers a wide and ever-accessible surface through which to launch phishing and spoofing attacks.

Deep Reliance on and Trust in Digital Infrastructure

Singaporeans generally embraced digital tools with confidence. Some of the most ubiquitous ones included Singpass, a national digital identity platform that authenticated over 2,700 government and private services including banking and healthcare; PayNow, a real-time funds transfer service that allowed users to transact money without bank account details; and SimplyGo; a contactless fare payment system. There were many more across a dizzying range of fields: food delivery (GrabFood, Foodpanda), ride-hailing (Grab, Gojek), telemedicine (Doctor Anywhere, WhiteCoat), restaurant bookings (Chope, Quandoo) – the list was endless. Because these digital services had become deeply embedded in everyday routines, Singaporeans had grown to see them as indispensable.

Thanks to consistent delivery of reliable, user-friendly services from the government, Singaporeans were accustomed to well-functioning systems. When problems occurred, agencies typically responded quickly and visibly, reinforcing trust that digital services would continue to meet expectations and improve over time. Further, the government's decades-long investment in and messaging about digital transformation via initiatives such as Smart Nation had built familiarity and confidence in digital systems. Scammers took advantage of this trust in government systems and established institutions. By mimicking official channels, fraudsters could convincingly pose as government agencies, police or banks, lowering users' defenses and increasing the success rate of impersonation scams.

[6] Infocomm Media Development Authority, "Singapore Digital Society Report 2023", 5.
[7] Infocomm Media Development Authority, "Singapore Digital Society Report 2023", 5.

Affluent Population and Centralised Savings

Singapore's economic success had produced a population that was relatively affluent by global standards, with a high rate of home ownership and larger median full-time incomes than those in Great Britain.[8,9] Many residents had significant savings in personal bank accounts as well as in government-managed schemes such as the Central Provident Fund, a national savings plan for retirement, housing and healthcare. These centralised and structured forms of wealth made individuals attractive targets for scammers, who knew that even ordinary Singaporeans often had substantial financial resources available.

That much of this wealth was accessible via digital channels made Singapore particularly vulnerable. Central Provident Fund accounts, for example, were linked to Singpass, a secure platform that scammers could exploit by deceiving individuals into revealing their login credentials. Meanwhile, the widespread use of instant payment systems such as PayNow meant that once a scammer gained access to a victim's identity or bank interface, they could transfer large sums quickly and irreversibly. The proliferation of online investment platforms and cryptocurrency exchanges had also created new avenues for high-yield scams, often disguised as legitimate financial products.

A Highly Urbanised, Fast-Paced Society

Life in Singapore moved quickly. Residents often prioritised speed and ease of use in a culture that, while conducive to productivity, could lead to snap decisions when responding to digital communications. Scams that created a false sense of urgency took advantage of this behavioural tendency, reducing the likelihood of verification before action (see Box 1).

Box 1: Manipulation via email

This is an example of a real scam message received via email:

"This notice is to bring to your notice that your outstanding invoice number 86ee5245dc8d is OVERDUE. Your account expiring on 04 August 2025 is SUSPENDED. TO RENEW your account (Expires on 04 August 2025), click HERE. This is the final message that we are legally required to transmit in regards to the expiration of your account."

This scam message relies on several psychological tactics, including fear, a sense of authority and the illusion of authenticity, to override critical thinking and elicit a quick response without considering red flags. First, it manufactures a strong sense of urgency by using capitalised words like "OVERDUE" and "SUSPENDED", along with a specific expiration date. These cues aim to create panic and the impression that time is running out. The mention that the account is "SUSPENDED" further amplifies this pressure by suggesting a disruption of service, while the phrase "final message we are legally required to transmit" adds a veneer of formality and legal authority to discourage the recipient from ignoring the message.

Additionally, the message uses impersonal but seemingly specific details, such as a fake invoice number, to give it a sense of legitimacy without needing to reference any actual transaction. The inclusion of a generic call-to-action link ("click HERE") exploits the sense of urgency to prompt impulsive clicking, potentially leading to phishing sites or malware downloads.

[8] Taufiq Zalizan, " The Big Read in short: The hard truths and trade-offs of homeownership in Singapore", *Today*, November 17, 2023, https://www.todayonline.com/big-read/big-read-short-hard-truths-and-trade-offs-homeownership-singapore-2307666.
[9] Banyan, "Singapore has achieved astounding economic success", *The Economist*, May 8, 2024, https://www.economist.com/asia/2024/05/08/singapore-has-achieved-astounding-economic-success.

Cultural Deference to Authority

Scammers often impersonated figures of authority such as police officers, immigration officials or bank staff. This was a shrewd strategy, given that compliance with official instructions and trust in government were high among Singaporeans.[10,11] Further, in a multilingual society such as Singapore, inconsistent language proficiency could further obscure warning signs in scam messages and reduce confidence in questioning authority, particularly among seniors or non-native English speakers.

"Some of the attributes of Singaporeans that are helpful in other contexts can be turned against them," Government Technology Agency (GovTech) Anti Scam Products founder and director Mark Chen said. "That's very sad, and so we feel the responsibility to help."[12]

A Multi-Pronged Response

Scams in Singapore took many forms and exploited numerous vulnerabilities. Their complexity demanded coordinated action that combined educational, technological and legal approaches such as the following:

Public Education and Awareness Campaigns

Singapore used proactive public education as a core tool for combating digital scams, recognising that an informed and alert public was a powerful line of defence against fraud. Public education initiatives targeted common scam formats with memorable visuals, relatable scenarios and consistent messaging across multiple platforms. Examples of these efforts included:

National Campaigns

Various national campaigns aimed to equip individuals with the knowledge to identify scams and encourage proactive behaviour to prevent victimisation. The "Spot the Signs. Stop the Crimes." campaign, launched by the National Crime Prevention Council and the Singapore Police Force, aimed to increase scam awareness by sharing real-life scam examples. The messaging was sharp and scenario-based – "No government agency will ask you to make a payment via WhatsApp", for example. Meanwhile, the "I can ACT against scams" campaign used the acronym ACT – **A**dd, **C**heck, **T**ell – to suggest taking three actions to safeguard against scams: **Add** security features such as two-factor authentication or the ScamShield app, **Check** before acting by verifying messages or requests with official sources and **Tell** the authorities and loved ones about any suspicious encounters.

ScamShield

The ScamShield suite was an integrated anti-scam system that combined public reporting, message- and call-filtering and educational resources to help individuals and authorities stay ahead of evolving threats. It included the following:

[10] Chew Hui Min, "Government remains most trusted institution in Singapore, amid global trend of societal polarisation: Survey", *Channel News Asia*, March 15, 2023, https://www.channelnewsasia.com/singapore/edelman-trust-barometer-2023-government-business-polarisation-inequality-3345571.
[11] Vanessa W. Lim, Rachel L. Lim, Yi Roe Tan, Alexius S. E. Soh, Mei Xuan Tan, Norhudah Bte Othman, Sue Borame Dickens, Tun-Linn Thein, May O. Lwin, Rick Twee-Hee Ong, Yee-Sin Leo, Vernon J. Lee, and Mark I. C. Chen, "Government trust, perceptions of COVID-19 and behaviour change: cohort surveys, Singapore," Bulletin of the World Health Organization 99, no. 2 (2021): 92-101, https://doi.org/10.2471/BLT.20.269142.
[12] Mark Chen, interview by Tara Thean Mei Feng, August 12, 2025.

i. ScamShield Mobile App: Available on iOS and Android, the app allowed users to determine whether websites and messages, including SMSes, Whatsapps and Telegrams, were scams. It also automatically blocked calls from known scam numbers and filtered scam-related SMSes using AI and crowdsourced data. Users could report scam messages and calls directly through the app, contributing to a national database of scam tactics.

ii. ScamShield Website: This website offered resources to educate the public on the latest scam tactics and stay up-to-date on scam trends in Singapore. The "I've Been Scammed" section offered clear instructions for steps a victim could take following a scam to protect themselves, including an easy link to file an online police report.

iii. Scamshield Helpline: The 24/7 anti-scam support service assisted individuals who needed to verify suspicious communications or figure out what to do if they had been scammed.

Influencer Partnerships and Community Engagement

To reach younger and more digitally active audiences, the authorities enlisted influencers and social media platforms to spread anti-scam messages in authentic, relatable ways. Trusted voices normalised scam awareness on TikTok videos, Instagram reels and other forms of media. For example, Naomi Neo partnered with the Ministry of Home Affairs to create "My Mom Lost Her Money TWICE?!", a gag YouTube video in which Naomi pranks her mother into sending her money by pretending to have gotten into a car accident.[13] Memes and gamified content, such as quizzes about scam tactics, were other fun ways to spread anti-scam messages. Meanwhile, community centres and residents committees helped educate vulnerable groups such as seniors and non-English speakers through talks and interactive workshops. These sessions often included real-life testimonials, walkthroughs of common scam scenarios and advice tailored to specific groups such as migrant workers and the elderly.

Experiential Education

The Singapore government's approach to combating scams involved experiential education as a way to deepen public engagement and improve message retention by allowing individuals to interact with simulated scam scenarios rather than merely receiving information. "Unpacked" was a scam simulation tool that enabled users to engage with scams firsthand and experience common manipulation tactics. The mobile-only tool, which a group of Open Government Products employees built at a Hack for Public Good event, started with a call from a "DBS Bank employee" reporting unusual activity in an individual's bank account. The call would then be transferred to the "police", who would communicate with the user using a speaking manner based on local conventions gleaned from police advisories and interviews with officers. Finally, the user would simulate transferring large sums of money into an unknown bank account. At the time of writing, the tool's creators were developing Chinese, Malay and Tamil versions of the simulation.

"The way citizens consume scam education, such as via advertisements in MRTs and on social media, is very passive," software engineer and Unpacked team member Rayner Loh told *The Straits Times*. "We want to show things like how psychological manipulation happens in real time."[14]

[13] Naomi Neo, "My Mom Lost Her Money TWICE?!", (video, 11:46), YouTube, posted April 14, 2024, https://www.youtube.com/watch?v=iKZ9Osoba6A.
[14] Sarah Koh, "Hackathons produce scam simulation tool for education, platform identifying birds based on calls", *The Straits Times*, July 7, 2025, https://www.straitstimes.com/tech/hackathons-produce-scam-simulation-tool-for-education-and-platform-identifying-birds-based-on-calls.

Strengthening Cybersecurity and Banking Protocols

In response to rising scam losses, Singapore's financial sector, led by the Monetary Authority of Singapore, rolled out tightened cybersecurity measures aimed at reducing the success rate of fraudulent transactions. Among these measures were the following:

1. *The "money lock" feature.* This feature allowed users to ring-fence a portion of their funds that could not be digitally transferred, even in the event of account compromise.

2. *Delays for high-risk transactions*. Creating a buffer of several days between transfer initiation and deposits to new payees or foreign accounts increased the likelihood of users detecting suspicious activity before money left their accounts.

3. *Mandatory transaction alerts.* Transaction alerts delivered instantly via SMS, email or in-app notifications (example: "You're performing a FAST Transfer to [individual] (A/C No: 503840295739). If unauthorised, call [number].") acted as an early warning system, enabling users to quickly detect and report unauthorised transactions in an immediate feedback loop.

4. *Phasing out clickable links.* To limit phishing attempts, banks began phasing out clickable links in SMSes and emails, a common vector used in scam campaigns.

5. *Strengthening digital authentication.* To make user verification more secure, many Singaporean banks required biometric logins such as fingerprint or facial recognition, reducing reliance on passwords that fraudsters could easily steal or guess. The banks had also largely phased out traditional hardware tokens in favour of app-based digital tokens, which generated time-sensitive codes tied to the user's specific device. Login verification protocols had become stricter: two-factor authentication and identity checks during high-risk transactions such as overseas logins or first-time transfers were increasingly becoming the norm.

6. *Collaboration between financial institutions and telcos as well as social media platforms.* Telcos had begun masking official phone numbers to help prevent scammers from spoofing the numbers of government agencies and banks. Some carriers also auto-blocked known scam callers and suspicious SMSes that ScamShield or other threat intelligence networks flagged. Meanwhile, social media companies were deploying AI-driven systems to identify scam-related content such as fake investment ads, phishing links and impersonation profiles and remove the content preemptively before it spread.

A team within GovTech – GovTech Anti-Scam Products (GASP) – developed tools such as the Scam Analytics and Tactical Intervention System (SATIS) platform, which used AI to screen hundreds of thousands of websites for scam activity daily and blocked or displayed anti-scam warnings on suspicious websites. GovTech also ran ScamShield (see Public Education and Awareness Campaigns). GASP worked closely with agencies such as the Monetary Authority of Singapore, the Infocomm Media Development Authority and the Cyber Security Agency to protect digital banking infrastructure and support national threat intelligence sharing.

Legislative and Enforcement Actions

Singapore made clear that it considered online scams not just a nuisance, but a serious criminal threat, and updated its legal framework and boosted enforcement resources accordingly. Rather than relying on a single "anti-scam law", Singapore used a multi-pronged legal strategy that gave prosecutors flexibility in responding to scams that weren't always easy to place in neat legal boxes. Laws such as the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA), the Computer Misuse Act (CMA)

and the Miscellaneous Offences Act gave authorities broad powers to freeze assets, prosecute syndicate members, punish fraudulent solicitation and seize or confiscate ill-gotten gains. These three laws could work as follows:

Target the money (CDSA): Scams depended on moving stolen funds quickly. The CDSA enabled authorities to freeze and seize criminal proceeds, including those passing through money mules.

Target the digital infrastructure (CMA): The CMA criminalised scam activities such as gaining unauthorised access to systems or stealing credentials, as well as possessing or supplying scam-related tools such as phishing kits.

Catching edge cases (Miscellaneous Offences Act): This act provided a legal net for cases that didn't fall straightforwardly into banking or cybercrime laws, especially in hybrid scams involving offline elements such as intimidation or nuisance calls.

Box 2: How Other Countries Are Tackling Online Scams

Global Spotlight: The UK's Banking Protocol

In 2016, the UK launched a rapid-response system where bank branch staff could call the police immediately if they suspected a customer was about to become a scam victim. Officers aimed to arrive within minutes, often intercepting scammers before funds were lost. The protocol saved an estimated £202.8 million in its first five years, and £61 million in 2024.

Global Spotlight: Australia's Telco Code of Practice

Australia enforced a legally binding code requiring telcos to detect, block and report scam calls and SMSes. This code made telcos legally accountable for scam detection and reporting. From mid-2022 to end-2024, telcos blocked over 857.4 million scam texts and over 2.3 billion scam calls.

Global Spotlight: South Korea's Elderly Transfer Verification

To protect seniors from fraud, South Korea's banks were required to ask customers withdrawing over 5 million won ($4,600) voice-phishing prevention questions to ensure that the customers were not scam victims. The banks also had to ask those withdrawing 10 million won ($9200) why they needed such a large cash amount, and to check with elderly customers whether they had received a phone call prior to visiting the bank.

Below are two scam cases that illustrated the application of these laws:

Case 1: Carousell Scam

Three men between the ages of 21 and 28 faced charges after defrauding victims of at least $57,000 via a fake Pokémon Trading Cards listing on Carousell. One individual was charged under the CDSA for assisting in retaining criminal proceeds, while the other two were charged under the CMA for unauthorised access to victims' bank accounts to withdraw money.[15]

[15] Drima Chakraborty, "3 men charged for alleged involvement in Pokemon card scams; believed to have cheated victims out of $57k", *AsiaOne*, June 28, 2025, https://www.asiaone.com/singapore/3-men-charged-alleged-involvement-pokemon-card-scams-believed-have-cheated-victims-out.

Case 2: Job Scam

Three men in their twenties responded to offers on Telegram that promised fast money in exchange for sharing Singpass login credentials or bank details that enabled their bank accounts to be used to launder criminal proceeds. They faced charges under the CMA for unauthorised access and disclosure of access codes.[16]

To reflect the evolving nature of scams, which were sometimes cross-border operations with sophisticated infrastructure, Singapore worked with Interpol and its ASEAN counterparts to dismantle scam networks operating from abroad. In 2024, the police and local banks conducted an islandwide anti-scam operation involving raids and collaboration with banks and telecommunications companies. The operation resulted in the seizure of approximately $1.9 million of scam profits, the freezing of over 300 bank accounts and the arrest of 25 suspects.[17]

Emerging Challenges and Opportunities

The following scam format, which typically arrived in an email, was familiar to the point of ridicule for a broad swathe of the population in wealthy, digitally literate countries:

Box 3: The Nigerian Prince Email

Subject: Urgent Assistance Required – $27,500,000 Inheritance Transfer

Dear Respected Friend,

I am Prince Olamide Adekunle, the only surviving heir of His Excellency, the late Minister of Finance of the Federal Republic of Nigeria. Before my father's untimely passing, he secured the sum of Twenty-Seven Million, Five Hundred Thousand US Dollars ($27,500,000) in a secure bank vault in Lagos.

Due to political instability, I cannot access these funds without the cooperation of a trustworthy foreign partner. Your name came to me through divine inspiration, and I am certain you are the person destined to assist me.

If you agree to help, I will transfer the funds to your account in your country. In return for your assistance, you will receive 30% of the total amount, and the rest will be used for investment in humanitarian projects.

Please send me your full name, address, phone number and bank details urgently, so we can begin this blessed arrangement.

Yours faithfully,
Prince Olamide Adekunle
Federal Republic of Nigeria

[16] Public Affairs Department, "Four Men To Be Charged For Suspected Involvement In Separate Cases Of Money Laundering Activities And Rental Scam", Singapore Police Force, April 3, 2024, https://www.police.gov.sg/Media-Room/News/20240403_four_men_to_be_charged_for_suspected_involvement.
[17] Angelica Ang, "$1.9m seized, 25 arrested in anti-scam blitz by police and banks", *The Straits Times*, March 22, 2025, https://www.straitstimes.com/singapore/1-9m-seized-25-arrested-in-anti-scam-blitz-by-police-and-banks.

The absurd nature of emails like this was a feature rather than a bug. Many in Singapore would immediately recognise a "Nigerian prince" email as a scam and ignore it entirely, enabling the ridiculous text to act as a filter that repelled all but the most gullible. By turning away non-viable targets that would waste scammers' time and resources, the emails drastically reduced false positives for scammers and ensured that they would have a more profitable pool of likely victims.[18]

This phenomenon created a challenge for scam prevention. As governments and companies rolled out more opt-in protections that appealed to tech-savvy users, they mainly shielded the least vulnerable and left the most susceptible individuals more exposed, Chen explained.[19]

"This, in some sense, can actually empower scammers," Chen said. He provided a hypothetical example: if all non-vulnerable Singaporeans installed ScamShield on their mobile devices to block suspicious calls, that would mean that those who still picked up such calls probably would not have ScamShield installed and would thus be more likely to believe a scammer's narrative. Scammers would then be free to abandon the deliberately outrageous narratives they used for self-filtering and instead craft more believable stories tailored to this smaller audience.

Teams such as GASP were working on various measures to protect the most vulnerable demographics, including encouraging users to report potential scams on ScamShield and working on the backend to disrupt or block scam websites via SATIS. Chen noted that there was also a role for public education in helping to defend at-risk individuals, but that it had limitations: there were simply too many messages out there telling people what to do. Scam messages appeared everywhere, from landing pages during benign banking transactions to Gardenia sliced bread wrappers ("Unsure if it's a scam? Check by calling the 24/7 ScamShield Helpline at 1799").

"You do get desensitised after a while – it's difficult to get a new message in public consciousness," Chen said. "The public education piece is obviously important, but it's probably already stretched as far as it can be, or even more than it can be."[20] Teams focused on public education related to scams were working to simplify messaging and focus on conveying the one or two critical points that may help a victim realise that something was wrong.

GASP was also looking for convergence points where scammers had to interact with regulated systems, creating natural choke points for detection and intervention. These might include activities such as applying for a SIM card or opening a bank account – places where identity verification and legal oversight already existed. At these points, GASP had a "defenders advantage" thanks to tools such as machine learning that could flag suspicious patterns across large volumes of activity. This approach helped GASP to bypass the constant arms race of trying to spot scams solely from their content, which was becoming increasingly difficult as AI made deepfakes and other false material faster and cheaper to produce.

"Thinking about what scammers can do with AI, it's like a crazy Whac-A-Mole," Chen said. "It's easier to generate realistic content than to detect it."[21]

Platforms such as Facebook, WhatsApp, Instagram and Telegram – the most popular platforms for fraudsters to conduct their scams in Singapore[22] – were more challenging for entities like GASP to engage with

---

[18] Cormac Herley, "Why Do Nigerian Scammers Say They Are From Nigeria?," *Proceedings of the Workshop on the Economics of Information Security (WEIS)*, Microsoft Research, June 2012, https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/WhyFromNigeria.pdf.
[19] Chen, interview, August 12, 2025.
[20] Chen, interview, August 12, 2025.
[21] Chen, interview, August 12, 2025.
[22] Singapore Police Force, "Annual Scams and Cybercrime Brief 2024", 6.

consistently. These platforms' willingness to share information or act on findings varied, as they had to consider competing priorities such as user privacy and revenue goals. Obtaining more sensitive data from online platforms was particularly difficult due to personal data concerns, especially since these platforms were often based outside of Singapore and operated under different legal regimes. As such, GASP focused on non-sensitive intelligence such as scam URLs, collaborating with Google to block fraudulent websites on Google Safe Browsing.

At the time of writing, preventative measures appeared to have been particularly effective in decreasing the number of and money lost from social media impersonation, malware-enabled and fake friend call scams in Singapore. Phishing scams, government official impersonation scams, investment scams and e-commerce scams were still on the rise, with e-commerce scams such as fraudulent concert ticket sales being the biggest problem.[23] Self-effected scams, in which fraudsters manipulated victims into performing monetary transactions on their own, were becoming particularly ubiquitous, comprising over 80% of reported scam cases in 2024.[24] A large chunk of the 70.6% increase in money lost to scams between 2023 and 2024 came from a small number of exceptionally costly cases: four cases alone accounted for S$237.9 million of the total lost, representing a massive portion of the overall figure.[25] Of those four cases, three were related to cryptocurrency, highlighting how scammers continuously exploited emerging technologies to come up with ever more creative schemes. The scams kept changing, and each new wave demanded fresh defence tactics.

"We have to keep running just to stay still," Chen said.[26]

Discussion Questions

1. A large crypto-linked scam hits multiple victims in 24 hours. Design a 48-hour response. What gets done first, and by whom?

2. To curb scams on social platforms and messaging apps, should Singapore mandate greater data/intel sharing from platforms?

3. Why have "self-effected" scams become dominant in Singapore, and how would you help reduce their incidence without over-policing users?

4. Should high-risk transfers face a default cooling-off period (e.g. 12-24 hours)?

5. What would "success" look like in an anti-scam policy strategy over the next 12 months?

[23] Yee Loon, "Scam and cybercrime cases in Singapore surge, with victims losing S$1.1 billion in 2024", *The Online Citizen*, https://www.theonlinecitizen.com/2025/02/25/scam-and-cybercrime-cases-in-singapore-surge-with-victims-losing-s1-1-billion-in-2024/.
[24] Singapore Police Force, "Annual Scams and Cybercrime Brief 2024", 4.
[25] Ng Yun Shiean and Mike Tan, "Five Things You Should Know about the Annual Scams and Cybercrime Brief 2024", Singapore Police Force, https://www.police.gov.sg/Media-Room/Police-Life/2025/02/Five-Things-You-Should-Know-about-the-Annual-Scams-and-Cybercrime-Brief-2024.
[26] Chen, interview, August 12, 2025.