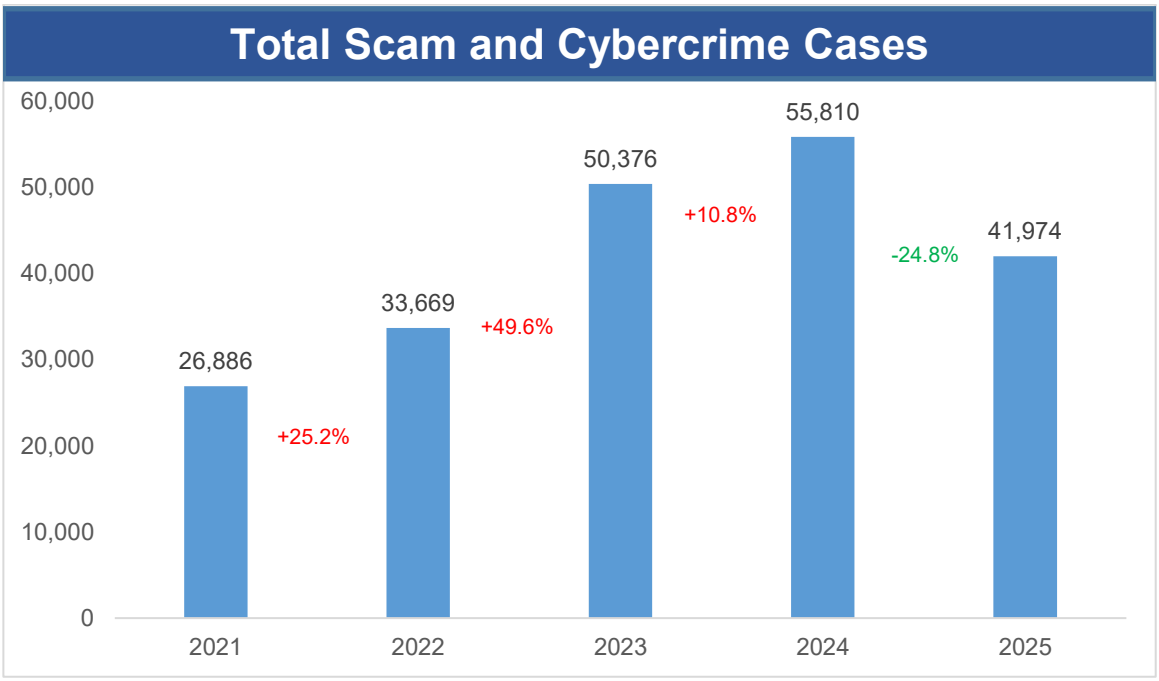
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Annual Scam and Cybercrime Brief 2025

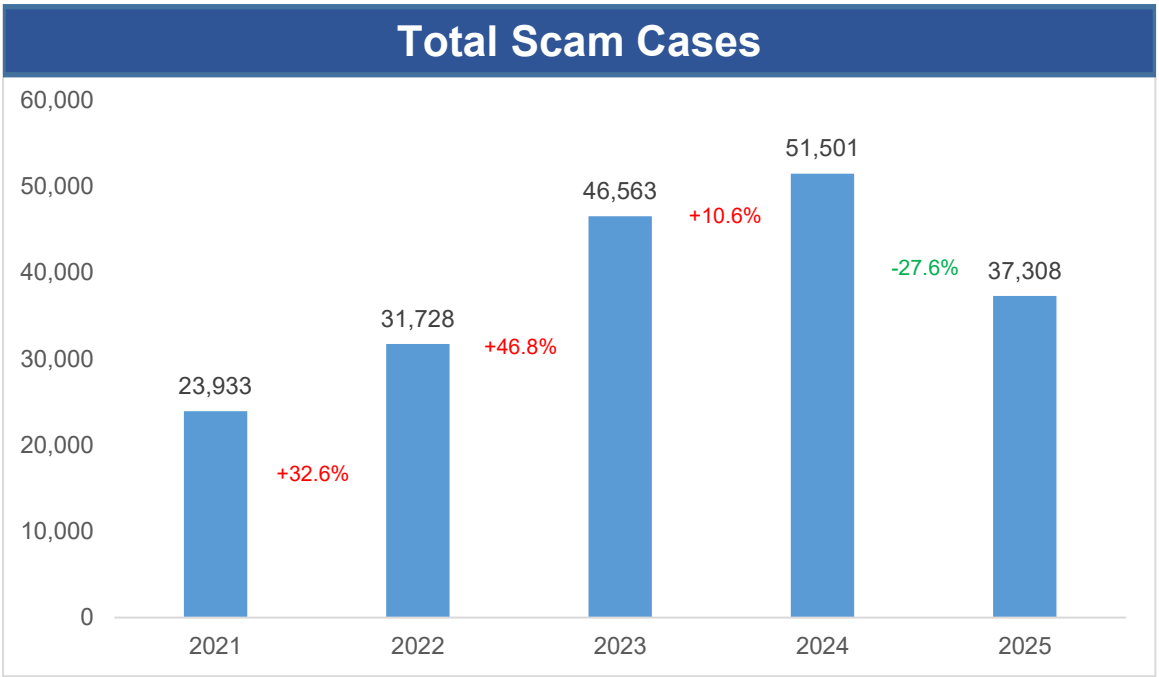
Overall Scam and Cybercrime Situation in 2025

The **number of scam and cybercrime cases decreased by 24.8% to 41,974 cases in 2025,** from 55,810 cases in 2024. In particular, **the number of scam cases fell by 27.6% to 37,308 scam cases in 2025,** from 51,501 cases in 2024. **The losses from scams also fell, by 17.9% to about $913.1 million in 2025**, from about $1,112.4 million in 2024.

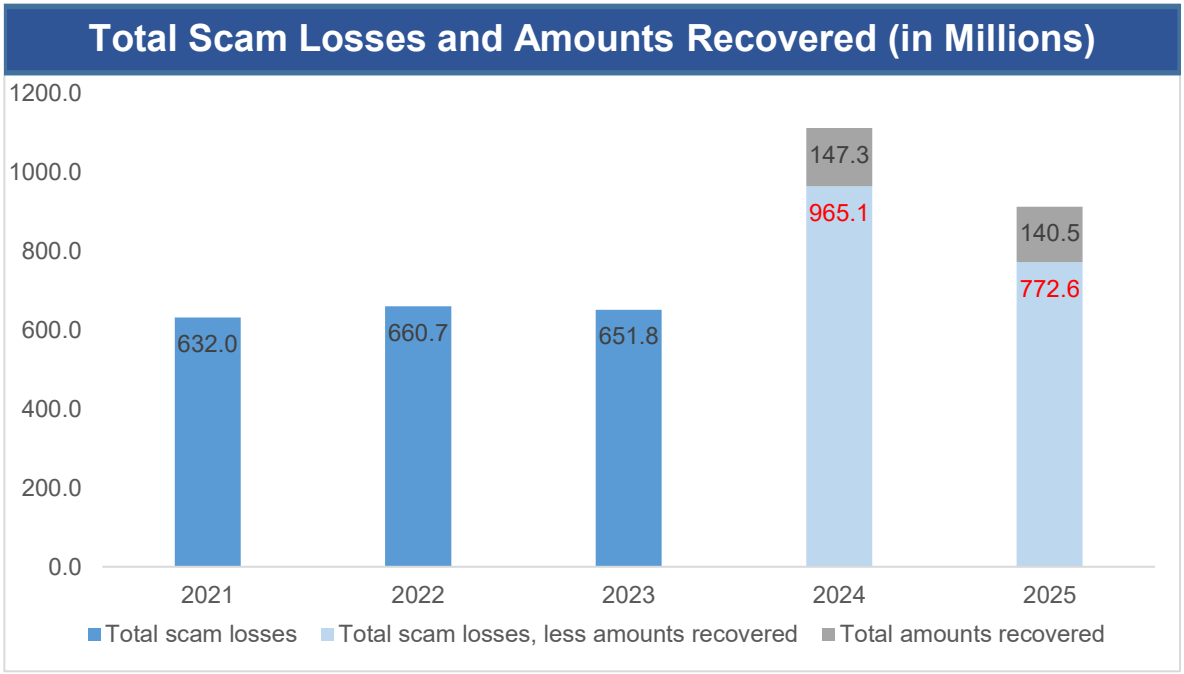
Nevertheless, the situation is still very concerning, and tackling scams remains a key priority for the Government.



2. Scams accounted for 88.9% of these 41,974 cases, which equates to a total of **37,308 scam cases in 2025**. This is a **27.6% decrease** from 51,501 cases in 2024.



3. The **amount lost to scams also fell, by 17.9% to about $913.1 million in 2025**, from about $1,112.4 million in 2024.



4. There were **significant decreases** in the number of cases reported for **e-commerce scams, job scams and fake friend call scams**. There were also **significant decreases** in the total amount lost for **malware-enabled scams, business email compromise scams, job scams and fake friend call scams.**

5. The decrease in both scam cases and scam losses suggests cautiously that the anti-scam strategies and public education measures introduced by the

Government and industry partners have made it more challenging for scammers to succeed.

6. In 2025, the Anti-Scam Command (ASCom) **successfully recovered about $140.5 million of scam losses**, which included over $117.7 million in fiat currencies and over $22.8 million in cryptocurrency.[1] Additionally, through proactive interventions with victims at various stages of being scammed, ASCom and its partners helped victims **avert at least $348 million in potential losses[2],** which included over $339.7 million in fiat currencies and over $8.8 million in cryptocurrency**.**

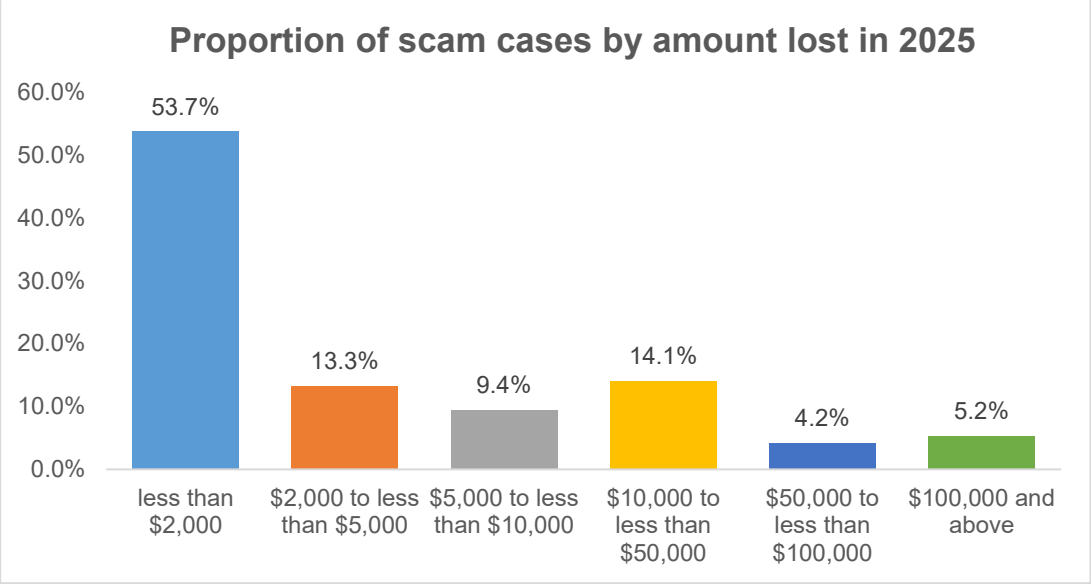
7. **Cryptocurrency losses[3] continue to form a considerable percentage of scam losses, accounting for about $182.2 million, or about 20.0% of total scam losses in 2025**. It is likely that scammers leverage cryptocurrency because of its irreversible transactions and limited traceability, making asset recovery very challenging for the authorities. **Tether, Ethereum, and Bitcoin** were the top cryptocurrencies that scam victims reported losing (details in **Annex B**) and accounted for about 91.7% of total cryptocurrency scam losses.

8. In 2025, the majority of scam cases, about 67.1%, suffered less than $5,000 in losses, while 5.2% of scam cases suffered at least $100,000 in losses. The median loss per case was $1,644.

[1] The amount of scam losses recovered refers to funds scammed from victims and transferred to the bank accounts and cryptocurrency wallets of scammers or mules, that were subsequently frozen in time by the SPF before the funds were further transferred out of these accounts and wallets and became untraceable. It does not refer to monies returned to scam victims. While SPF has recovered scam losses in previous years, only figures for 2024 and 2025 are shown as we did not capture the corresponding data based on the current methodology used to calculate scam losses recovered before 2024.

[2] The $339.7 million in non-cryptocurrency includes over $267.5 million averted through Project A.S.T.R.O. and over $72.2 million through joint interventions by ASCom and Community Policing Units. The $8.8 million in cryptocurrency refers to potential losses averted by the Crypto Tracing Team.

[3] Cryptocurrency losses refer to the outflow of cryptocurrency from victims' cryptocurrency account or wallet to scammers. It does not include losses where victims transferred money from their bank accounts to fake crypto-investment platforms. The latter is categorised as non-cryptocurrency losses.

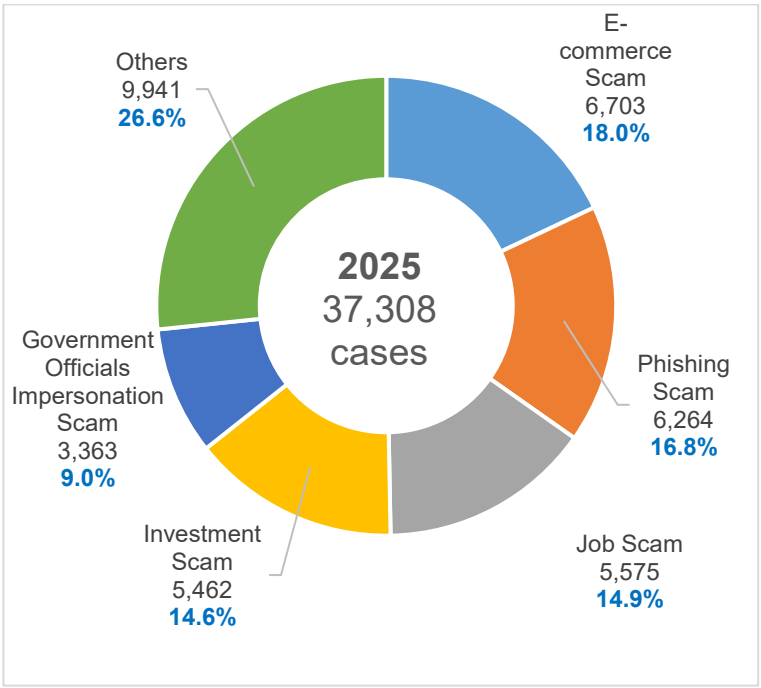


9. The percentage of total reported scams that involved **self-effected transfers** was 81.8**%** in 2025. In these cases, scammers did not gain direct control of the victims' accounts but manipulated them into performing monetary transactions through deception and social engineering. The SPF urges the public to exercise caution when making fund transfers, such as by verifying the legitimacy of such requests beforehand.

Scam and Cybercrime Types of Concern

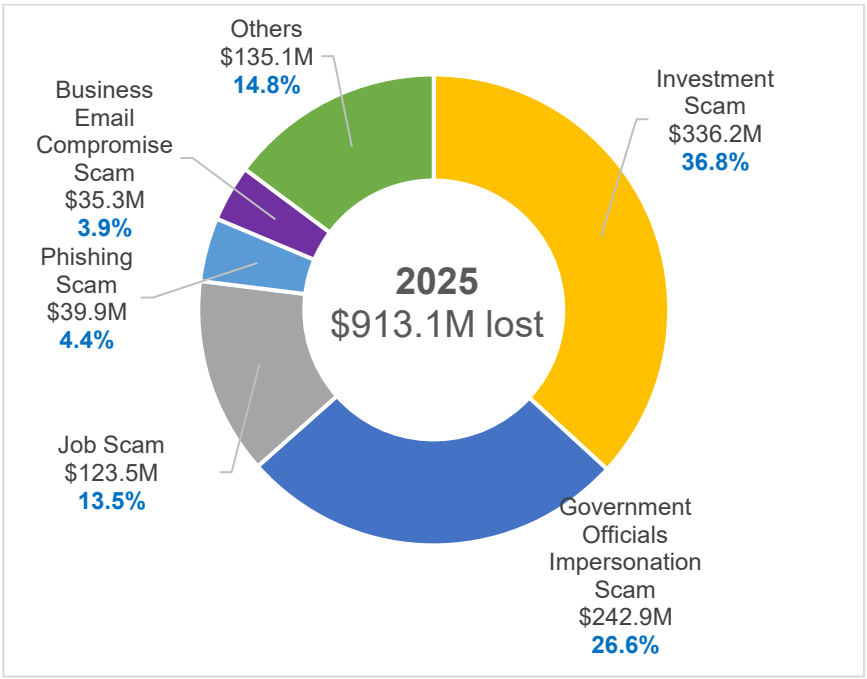
10. In 2025, the top five scam types with the most number of cases were **e-commerce scams, phishing scams, job scams, investment scams, and government officials impersonation scams**.

Breakdown of scam types by number of cases



11. In 2025, the top five scam types in terms of the amount lost were **investment scams, government officials impersonation scams, job scams, phishing scams and business email compromise scams**.

Breakdown of scam types in terms of amount lost (in millions)



12. The key scam types of concern in 2025 were:

a) Government Officials Impersonation Scams

i. **The number of government officials impersonation scams reported more than doubled,** by 123.6% to 3,363 cases in 2025, from 1,504 cases in 2024.

ii. It also recorded the second highest loss among all scam types in 2025. **The amount lost to government officials impersonation scams increased significantly** by 60.5% to about $242.9 million in 2025, from about $151.3 million in 2024.

iii. The SPF has observed new trends in monetary transfers by victims for this scam type:

- Transfer of funds from victims' bank accounts, to Payment Service Provider (e.g. YouTrip) accounts controlled by scammers, via PayNow.

- Cryptocurrency transfers by requesting the victims to create a new cryptocurrency account, fund the cryptocurrency account through fiat money transfers from the victims' bank accounts before purchasing cryptocurrency, and then transferring the cryptocurrency to scammers-controlled cryptocurrency accounts.

b) E-commerce Scams

i. Despite a 42.5% **decrease** to 6,703 cases in 2025, from 11,665 cases in 2024, e-commerce scams still recorded the highest number of reported cases among all scam types in 2025.

ii. The amount lost to e-commerce scam cases **decreased** by 4.6% to about $16.7 million in 2025, from about $17.5 million in 2024.

iii. Pokémon trading cards was the item most commonly involved in e-commerce scams in 2025, making up 13.6% of e-commerce cases. Carousell and Facebook Marketplace were the platforms most commonly used by scammers to perpetrate e-commerce scams, accounting for 29.0% and 22.2% of e-commerce scam cases respectively. After expressing interest in the product or pre-order, the victims were instructed to make payment or an initial deposit via PayNow or bank transfer. They only realised they had been scammed when they failed to receive the products, or when the sellers became uncontactable.

c) Phishing Scams

i. Phishing scams recorded the second highest number of reported cases among all scam types in 2025, even though there was a 26.8% **decrease** in number of cases to 6,264 in 2025, from 8,552 in 2024.

ii. The amount lost to phishing scam cases **decreased** by 32.8% to about $39.9 million in 2025, from about $59.4 million in 2024.

iii. The phishing scams in 2025 predominantly involved unauthorised card transactions where the victims unknowingly submitted their card details and authentication codes (via OTP/digital token) to the scammers, to complete seemingly legitimate purchases.

d) Investment Scams

i. While there was a **decrease** in investment scam cases, by 19.8% to 5,462 cases in 2025, from 6,814 cases in 2024, the number of investment scam cases remained the fourth highest among all scam types in 2025.

ii. Notably, the amount lost to investment scams in 2025, of about $336.2 million, was the highest among the various scam types. This represents a 4.8% **increase** from about $320.7 million in 2024.

e) Business Email Compromise Scams

i. The amount lost to business email compromise scams **significantly decreased** by 60.1% to $35.3 million in 2025, from $88.5 million in 2024.

ii. Through email spoofing or compromised email accounts, the scammers impersonated business entities (e.g. suppliers, vendors, clients) or individuals within the organisations (e.g. senior executives, management, staff), and deceived the victims into making payments to fraudulent bank accounts or to fulfil fraudulent monetary requests.

13. The details of the top 10 scam types in Singapore can be found in **Annex C.**

14. The background information of the other common or notable scam variants is provided in **Annex D**.

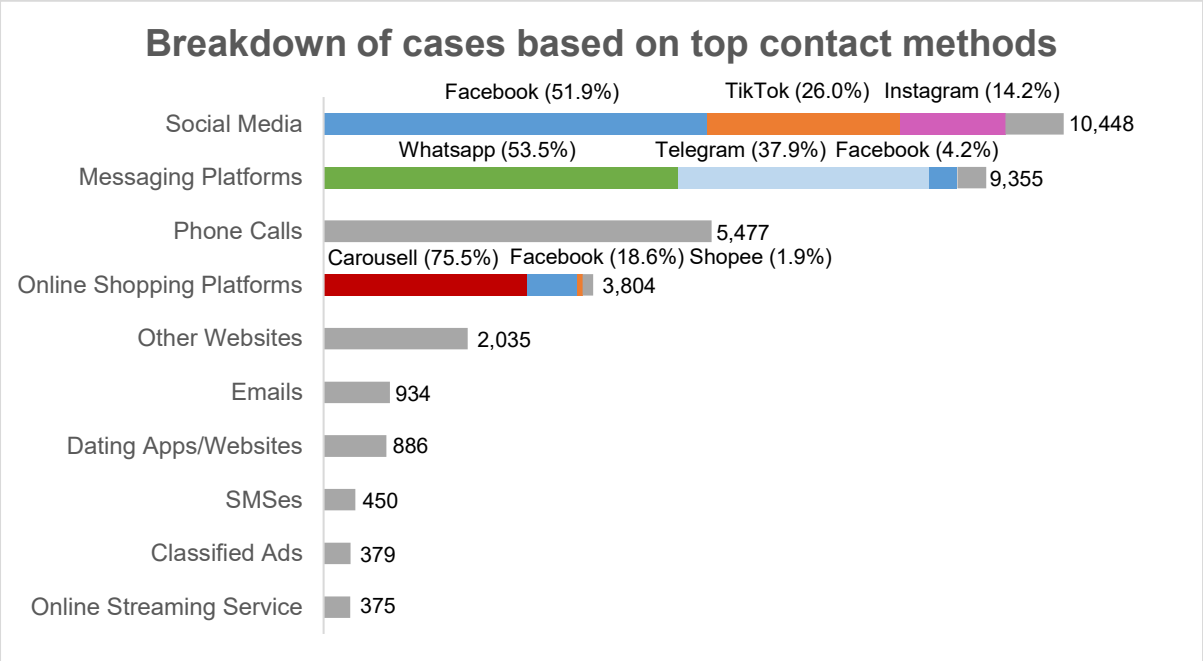
Top Contact Methods

15. **Social media, messaging platforms, phone calls and online shopping platforms** were the top contact methods used by scammers to reach victims.

16. While social media, messaging platforms and online shopping platforms remained the top contact methods for scammers, there has been a decrease in reported scam cases involving these contact methods. Notably, scam cases involving **designated online service providers**[4] **under the Online Criminal Harms Act (OCHA)**, which came into effect in 2024, have declined significantly by 36.5%.

17. Notwithstanding, the scam situation on these platforms remains worrying. Online platforms were used by scammers to reach out to victims in 84.1% of all scam cases. In particular, Meta platforms were involved in 35.4% of all scam cases, with Facebook alone accounting for 18.0% of all scam cases.

18. More details of the platforms used by scammers can be found in **Annex E**.



Scam Victim Profile

19. **In 2025, 85.2% of the scam victims were youths, young adults, and adults aged below 65.**

[4] Two Codes of Practice for online communication services and e-commerce services were issued in June 2024, requiring Meta, Telegram, WeChat and Carousell to put in place appropriate systems, processes or measures to proactively disrupt scams and malicious cyber activities affecting people in Singapore.

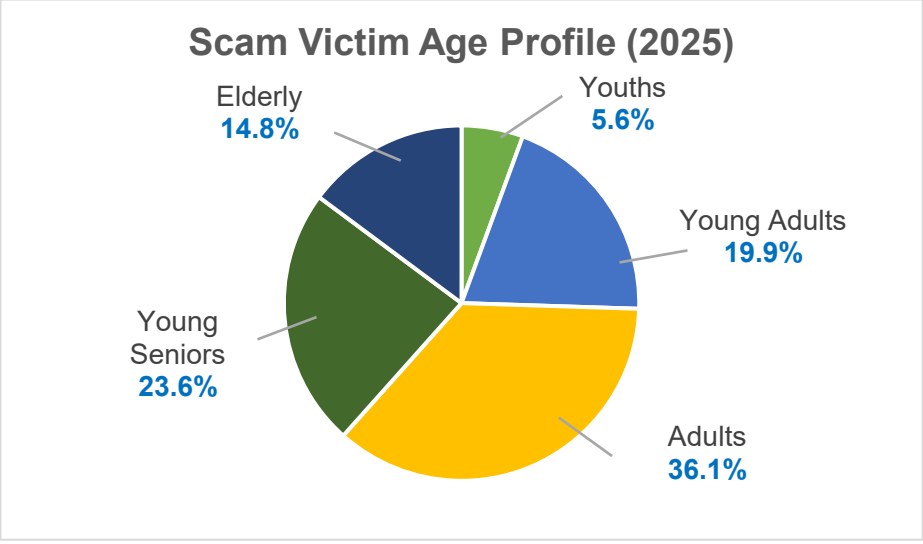
a) **Youths, aged 19 and below, made up 5.6% of scam victims.** 36.6% fell prey to e-commerce scams, while 15.1% fell prey to phishing scams and 12.8% to job scams. Youths most commonly responded to scammers via messaging platforms, online shopping platforms and social media. The average amount lost by youths to scams was $4,918 per victim.

b) **Young adults, aged 20 to 29, made up 19.9% of scam victims.** 31.5% fell prey to e-commerce scams, while 17.8% fell prey to job scams and 10.8% to phishing scams. Young adults most commonly responded to scammers via messaging platforms, social media and online shopping platforms. The average amount lost by young adults to scams was $9,118 per victim.

c) **Adults, aged 30 to 49, made up 36.1% of scam victims.** 22.4% fell prey to e-commerce scams, while 17.8% fell prey to phishing scams and 17.6% to job scams. Adults most commonly responded to scammers via social media, messaging platforms and online shopping platforms. The average amount lost by adults to scams was $22,283 per victim.

d) **Young seniors, aged 50 to 64, made up 23.6% of scam victims.** 21.6% fell prey to phishing scams, while 19.0% fell prey to investment scams and 13.8% to job scams. Young seniors most commonly responded to scammers via social media, messaging platforms and phone calls. The average amount lost by young seniors to scams was $32,983 per victim.

e) **The elderly, aged 65 and above, made up 14.8% of scam victims.** 22.5% fell prey to investment scams, while 21.0% fell prey to government officials impersonation scams and 17.2% to phishing scams. The elderly most commonly responded to scammers via social media, phone calls and messaging platforms. **The average amount lost by the elderly to scams was $37,053 per victim, which is the highest across all the age groups.**



SPF's and Whole of Government Efforts to Fight Scams and Cybercrime

20. The SPF continued to work closely with other Government agencies and private sector stakeholders to strengthen scam intervention measures.

21. **Key anti-scam initiatives recently implemented by the SPF** (more details in **Annex F**) include:

- The operationalisation of **caning for scams and scams-related offences** on 30 December 2025, as part of the Criminal Law (Miscellaneous Amendments) Bill passed on 4 November 2025. Scammers and members/recruiters of scam syndicates will face mandatory caning of at least six strokes, up to 24 strokes. Scam mules who provide payment accounts, launder scam proceeds (including money, gold and other valuables), or provide SIM cards and/or Singpass credentials, may be liable for caning of up to 12 strokes.
- The operationalisation of the **Facility Restriction Framework** for scam mules on 1 October 2025 by the SPF, alongside the Monetary Authority of Singapore (MAS), Infocomm Media Development Authority (IMDA) and Government Technology Agency of Singapore (GovTech Singapore), has resulted in **550 money mules, 801 SIM card mules[5], and 51 corporate entities being placed under restrictions** (as at 9 February 2026). Under this framework, which is being implemented in phases, scam mules may face restrictions on banking services that could be used to transfer scam funds (including digital banking, ATM services and card-based transactions), restrictions on subscriptions to new mobile lines, and restrictions on accessing existing Corppass accounts and the use of Singpass to register for high-risk services that could be exploited for scams. Restrictions on Corppass and Singpass will take effect at a later phase.
- The operationalisation of the **Protection from Scams Act** on 1 July 2025, with **12 Restriction Orders** issued by the SPF to banks (as at 1 February 2026) to restrict the banking and credit facilities of scam victims who continued to believe the scammers despite Police engagement.
- **Efforts by the Crypto Tracing Team (CTT)** resulted in the **successful recovery of virtual assets valued at more than $22.8 million** across 1,800 cases, and **aversion of more than $8.8 million in losses** through over 360 victim interventions.

[5] The 550 money mules and 801 SIM card mules are not aggregated because there are individuals who are both money mules and SIM card mules.

- Despite strengthened registration requirements by IMDA and telcos, scammers continued to acquire local SIM cards by exploiting mules and shell companies. From January to December 2025, **the SPF disrupted more than 105,000** mobile lines that were scam-related across all the telcos. This was more than double the number of lines disrupted in 2024. **Notably, the telco with the most number of disrupted local mobile lines was SIMBA with over 39,300 lines.** The SPF, IMDA and telcos will continue to build stronger safeguards and anti-scam measures to prevent the misuse of SIM cards for criminal activities.
- The reduction in cases on social media, messaging and online shopping platforms suggests that **the OCHA Codes of Practice (COP) have been effective**. The COP require designated online service providers to implement systems, processes and measures to meet specific scam-prevention and disruption outcomes.

22. Other **recently implemented and upcoming anti-scam initiatives by other Government agencies** (more details in **Annex G**) include:

- The **Monetary Authority of Singapore (MAS)** has worked with the major retail banks to implement additional friction for large withdrawals from high-balance accounts. MAS is also collaborating with cryptocurrency providers to strengthen anti-scam controls through enhanced surveillance and protective warnings. The major retail banks have phased out SMS one-time passwords for authentication of debit or credit card transactions for digital token users. Additional verification will be implemented for provisioning of cards into mobile wallets. Banks will also be implementing cooling periods for high-risk activities and in-app notifications to verify legitimate bank calls.
- The **Cyber Security Agency of Singapore (CSA)** has implemented multiple initiatives to enhance digital defence capabilities in 2025. CSA launched the National Simulated Scams Exercise (NSSE), a six-month pilot for the Safe App Portal, the sixth national cybersecurity campaign, and concluded its third iteration of the Be Cyber Safe Pop-up and Be Cyber Safe Drama Skit. CSA also continued its collaboration with partners to disseminate cybersecurity and scam tips.
- The **Infocomm Media Development Authority (IMDA)** has continued partnering the SPF and local telcos to strengthen defence against scam calls and SMSes, successfully blocking over 260 million potential scam calls and around 40 million potential scam SMS messages in 2025. On 23 January 2026, IMDA announced that the number of postpaid SIM cards each person can register will be limited to a maximum of 10 across all telcos, effective 28 February 2026, to minimise illicit SIM card use by scammers whilst accommodating legitimate users. A beta version of a self-help postpaid SIM card checker will be launched on 26 February 2026 at

https://go.gov.sg/simcardhowmany, allowing the public to check their registered SIM cards included within the postpaid SIM card limit by logging in with Singpass. All telcos now offer features to block incoming international calls and SMSes, with over 1.1 million subscribers activating overseas call blocking and over 270,000 activating overseas SMS blocking. Additionally, IMDA has worked with telcos to enhance detection capabilities against suspected misuse of local mobile numbers, leading to disruption of around 100,000 mobile lines since mid-2024.

- **GovTech Singapore** has developed anti-scam capabilities through the Scam Analytics and Tactical Intervention System (SATIS) suite, which analyses over 400,000 websites daily and disrupts more than 20,000 malicious websites monthly, alongside SATIS+ which targets other scam enablers. GovTech Singapore also enhanced Singpass' anti-fraud capabilities by using advanced machine learning (ML) models to detect suspicious activities, resulting in 200 suspicious account escalations to SPF in the first two months and the termination of over 4,600 fraudulently created financial accounts in 2025. Additionally, GovTech Singapore's collaboration with the police helped victims of government officials impersonation scams recover $200,000, and supported wider law enforcement efforts including investigations into 32 suspicious Singpass accounts, six arrests for illegal Singpass account sales, and 46 arrests in government impersonation and investment scam operations.
- **Open Government Products (OGP)** has continued to enhance its existing products, via the single SMS Sender ID, 'gov.sg', ScamShield app, and 'Unpacked' mobile immersive scam simulation.
- The **Central Provident Fund Board (CPFB)** launched two new security features in February 2026 to enhance CPF account protection. The Trusted Contact notification service allows CPF members aged 21 and above to appoint up to two trusted individuals who will receive copies of important transaction notifications, providing an additional layer of monitoring without granting them access to account details or transaction capabilities. The CPF Safety Switch is available to members aged 55 and above, enabling immediate account lockdown if scam victimisation is suspected, by disabling online services, stopping withdrawals, and halting disbursements, with deactivation only possible in person or via hotline assistance.

Everyone Plays a Part in Fighting Scams

23. Every member of our community plays a vital role in maintaining Singapore's safety and security.

24. Individuals should take proactive steps to strengthen their protection against fraudulent activities by adopting anti-scam measures. When in doubt, seek advice from reliable sources, call the ScamShield Helpline at 1799, or check the ScamShield application for verification.

25. Criminal syndicates are perpetrating scams in Singapore through local mules. The public must remain vigilant to avoid becoming participants, whether intentionally for monetary rewards or unwittingly through manipulation. They should not allow anyone to utilise their financial accounts such as banking facilities to transfer funds, provide access to their Singpass credentials, or supply them with local SIM cards. Payment accounts, Singpass credentials, and SIM cards are strictly for personal use only. Individuals found guilty of mule-related crimes may face substantial prison sentences, monetary penalties, and caning.

26. In 2025 alone, more than 7,000 money mules and scammers suspected of involvement in scam cases were investigated, and more than 940 have been charged by the SPF to date. The authorities will continue to take strong action against people who commit or facilitate scams.

27. Business entities, especially financial institutions, digital marketplaces and telcos, have a responsibility to prevent, detect and disrupt criminal activities conducted via their services. Implementing anti-scam prevention measures and safeguards will help protect their customers.

28. Given the substantial number of scam cases involving scammers approaching victims through online service platforms such as social media accounts, members of the public are advised to remain vigilant in their online engagements. The Government will sustain its collaboration with online service providers to prevent, intercept and dismantle scam operations.

29. The Government will continue to strengthen safeguards and initiatives that make it difficult for scammers to target Singaporeans. Additionally, the Government will continue to deliver anti-scam public education programmes to equip citizens with essential knowledge, capabilities and resources to defend themselves against scams.

30. Please see **Annex A** for comments by Mr Goh Pei Ming, Minister of State, Ministry of Home Affairs & Ministry of Social and Family Development.

PUBLIC AFFAIRS DEPARTMENT
SINGAPORE POLICE FORCE
25 FEBRUARY 2026 @ 3PM

Annex A

Quote by Minister of State (MOS) for Home Affairs and Social and Family Development

"The decrease in both scam cases and losses between 2024 and 2025 reflects the effectiveness of our anti-scam measures and the close collaboration between the Government, private sector, the community and individuals. However, the fight is far from over. Scams remain the most prevalent crime type in Singapore, and the overall numbers remain high. Scammers continue to adapt their techniques and exploit new vulnerabilities. We therefore must remain vigilant and not let our guard down. The Government will double down on our efforts and continue to rally both international and local partners to disrupt the scam lifecycle. At the same time, prevention starts with each of us. Stay alert and adopt anti-scam protective measures to safeguard yourselves and your loves ones from scams. When in doubt, call 1799 to check if you are being scammed."

- MOS Goh Pei Ming

Annex B

Top 5 Cryptocurrencies Lost to Scams in 2025

(Based on estimated value in Singapore dollars)

Cryptocurrency	Cryptocurrency units lost	Estimated value in Singapore dollars (approximate)
Tether	90,819,092.91	$117.7M
Ethereum	6,785.20	$26.1M
Bitcoin	176.16	$23.2M
USD Coin	9,748,784.21	$12.6M
XRP	463,004.28	$1.3M

Annex C

Top 10 Scam Types in Singapore
(Based on number of reported cases)

Types of Scams	Cases reported		Total amount lost (approximate)		Average amount lost in 2025
	2025	2024	2025	2024	
E-commerce Scams	6,703	11,665	$16.7M	$17.5M	$2,503
Phishing Scams	6,264	8,552	$39.9M	$59.4M	$6,384
Job Scams	5,575	9,043	$123.5M	$156.2M	$22,163
Investment Scams	5,462	6,814	$336.2M	$320.7M	$61,559
Government Officials Impersonation Scams	3,363	1,504	$242.9M	$151.3M	$72,229
Fake Friend Call Scams	1,551	4,179	$4.7M	$13.6M	$3,056
Sexual Services Scams	1,150	1,162	$3.9M	$4.1M	$3,464
Insurance Services Scams	1,003	-	$25.2M	-	$25,125
Loan Scams	935	1,154	$7.0M	$6.0M	$7,515
Internet Love Scams	917	852	$24.9M	$27.6M	$27,202
Top 10 scams	**32,923**	**44,925**	**$825.3M**	**$756.9M**	**$25,069**

Note: Total scam losses may not tally due to the rounding of figures.

Annex D

Background Information on Common or Notable Scam Variants

Government Officials Impersonation Scams

- The majority of government officials impersonation scam victims were aged 65 and above, comprising 34.0% of victims for this scam type. Phone calls and WhatsApp were the most common channels used by government officials impersonation scammers to contact potential victims.

- Government officials impersonation scams typically involve scammers impersonating local government officers (e.g. SPF, Immigration & Checkpoints Authority (ICA), MAS), bank or financial institution representatives (e.g. Unionpay, NTUC), or China government officials (e.g. China Police). Two notable variants emerged in 2025:

    - **Impersonation of bank or financial institution representatives and local government officials through calls (91.7% of cases)** – Victims would receive unsolicited calls from scammers posing as representatives from banks or financial institutions, who cite suspicious transactions on credit cards or insurance policies. When victims deny involvement, they are transferred to fake government officials who accuse them of money laundering. Scammers then instruct victims to transfer money to "safety accounts" or hand over cash for "investigation purposes".

    - **Impersonation of China government officials (e.g. China Police) and local government officials through calls (8.3% of cases)** – Victims receive calls from individuals impersonating ICA officers, airline or telco representatives claiming their details were used fraudulently. When victims deny involvement, they are transferred to another scammer claiming to be a China government official (e.g. China Police), who demand money transfers or cash handovers for "investigation or bail purposes".

- Previously, the SPF observed that scammers may instruct victims to hand over cash, gold bars or other valuable possessions (e.g. jewellery and luxury watches) to scam mules in-person. In some cases, victims were told by scammers to leave such items at specified locations for collection by scam mules. The SPF has since observed new trends in monetary transfers by victims. On the pretext of investigation, victims were instructed to:

    - Transfer funds from bank accounts to Payment Service Provider (e.g. YouTrip) accounts controlled by scammers via PayNow.

- Effect cryptocurrency transfers by creating a new cryptocurrency account, fund the crypto accounts through fiat money transfers from victims' bank accounts before purchasing cryptocurrency, and transferring the cryptocurrency to scammer-controlled cryptocurrency accounts.

- Members of the public should **never** transfer monies, hand monies or other valuables to any unknown persons or persons whose identity you did not verify. **Never** place monies or valuables at a physical location to facilitate subsequent collection.
- Singapore Government officials will never ask members of the public to do the following over a phone call:
  - Ask you to transfer money;
  - Ask you to disclose banking log-in details;
  - Ask you to install mobile apps from unofficial app stores;
  - Transfer your call to the Police.

Investment Scams

- The majority of investment scam victims were aged 30 to 49, making up 34.6% of victims for this scam type. The most common platforms which scammers used to contact investment scam victims were Telegram and Facebook.

- Victims of investment scams came across "investment opportunities" through recommendations from online friends, from their own internet searches/online advertisements, or were added into chatgroups or channels via messaging platforms by scammers purportedly for "investment opportunities". Some victims also received unsolicited messages from scammers offering "investment opportunities". Once they were duped or had been enticed by the false testimonies, victims would either follow the scammers' instructions to transfer monies to specified bank accounts or make payments via their bank cards for the purpose of investing.

- The SPF is concerned that investment scam victims are losing large sums of money via cryptocurrency transfers. Of cases involving cryptocurrency transactions in 2025, investment scams accounted for 38.4%. In these cases, scammers directed victims to create new cryptocurrency accounts for "investing". Victims are told to fund their cryptocurrency accounts with money from their bank accounts and buy cryptocurrency. Victims then transfer the cryptocurrency to scammer-controlled cryptocurrency accounts for investing. In some cases, victims also shared their cryptocurrency account login credentials and seed phrase with scammers for the purpose of "investing". This allowed scammers to gain access and drain cryptocurrency from the account.

- The SPF also observed new tactics, where:

    - Scammers asked victims to download shell investment apps from official app stores. These apps promote fraudulent investment products such as fake cryptocurrency, forex, and stock-trading products, and show fictitious investment progress and returns. These give victims a false sense of assurance that the investment is growing, thereby luring victims into pumping even more money into the investment.

    - The SPF has also observed investment scam victims handing over cash and valuables to scam mules. This is similar to what is observed in government official impersonation scams.

- Victims would discover that they had been scammed only when they experience difficulties in withdrawing their investment returns despite transferring increasingly large sums of "fees" or" "taxes" incurred for the "investment".

- In some instances, victims would receive initial small investment returns. This leads them to believe that the "investments" were genuine and entice them to invest more money by transferring larger sums of monies or cryptocurrencies to scammers.

- Members of the public are strongly advised to be cautious when responding to investment advertisements and when making investment decisions. You should only deal with regulated entities and representatives listed on the Financial Institutions Directory and Financial Institution Representatives Register (FIRR) on MAS' website. Verify the identity of the person promoting the investment by meeting him/her in person at the financial institution's premises, matching the name on his/her official ID against the FIRR, and checking his/her appearance against the official ID. Investors should also look out for red flags when considering investment "opportunities", such as guaranteed or high returns at little or no risk, or pressure to act urgently citing time-limited offers.

Phishing Scams

- The majority of phishing scam victims were aged 30 to 49, comprising 37.7% of victims for this scam type. Facebook and TikTok were the most common channels used by phishing scammers to contact potential victims.

- Phishing scams involve emails, text messages, calls, or advertisements from scammers posing as government officials, financial institutions or businesses. Victims would be tricked into revealing sensitive information such as banking credentials and/or debit or credit card information after clicking malicious links or via phone calls. Upon acquiring the victims' information, scammers would

perform unauthorised transactions on the victims' bank accounts or debit/credit cards.

- In the phishing scam variants, victims would discover that they had been scammed when they found unauthorised transactions made from their bank accounts or debit/credit cards. Some phishing scam variants include the following:

    - Victims usually encounter enticing deals (e.g. heavily discounted transport cards, food-related advertisements) on social media platforms (e.g. Facebook, TikTok, Instagram) that lead them to fraudulent phishing links. Victims would unknowingly submit their card details and authentication (OTP/Digital Token) to scammers, to complete the seemingly legitimate purchases.

    - In 2025, there were 2,670 cases where social media advertisements were used to lure victims into clicking on phishing links, with total amount lost amounting to $4.6 million. The compromised card credentials are then misused in three ways:

        a. Addition to scammer-controlled mobile wallets (e.g. Apple Pay, Google Pay, Samsung Pay) for both in-store Near Field Communication (NFC) purchases and online transactions, particularly on e-commerce and cryptocurrency platforms.

        b. Direct use of card details for online purchase.

        c. Linking to payment services and e-wallets (e.g. Grab, YouTrip, Revolut) for unauthorised top-ups and transactions.

    - Victims would receive unsolicited phone or in-app calls allegedly from government officials such as the SPF, Ministry of Manpower, or the MAS. Scammers would claim that there were issues with victims' bank accounts or that they require the victims' details for purposes of investigation or further verification. Victims would then be convinced to disclose their banking credentials, debit/credit card details, personal details, and/or OTPs/perform digital authentication.

    - Victims would post a listing to sell items on online shopping platforms (e.g. Facebook marketplace, Carousell). Scammers would approach the victims via the in-app messenger or email under the guise of an interested buyer and claim that they have already settled the payment and/or delivery for the item. Scammers would then send victim phishing links impersonating the relevant payment/delivery entities (e.g. Carousell, Lalamove), claiming the victims can receive the proceeds of the sales via the link. Victims would unknowingly relinquish their

bank/card details and authentication (OTP/Digital Token) to scammers. Scammers would then perform unauthorised transactions on the victims' bank accounts or debit/credit cards.

- Members of the public are advised to be prudent when making online payments and to visit only reliable websites for online shopping. You should opt for SMS notifications to be sent to your mobile phone for any charges incurred on your credit or debit cards, and regularly check your bank statements and alert the bank immediately should there be any discrepancies or unauthorised charges. When making payment online, buyers should read the notifications sent and be clear of what you are approving, before providing OTP or approve digital tokens.

E-commerce Scams

- E-commerce scams saw a significant decrease in the number of cases reported in 2025, by 42.5% to 6,703 cases, from 11,665 cases in 2024. The total amount lost to e-commerce scams also decreased, by 4.6% to about $16.7 million in 2025, from about $17.5 million in 2024.

- The majority of e-commerce scam victims were aged 30 to 49, making up 43.8% of victims for this scam type. The most common platforms which scammers used to contact e-commerce scam victims were Carousell and Facebook.

- E-commerce scams typically involve the sale of goods and services without physical meet-ups. Generally, victims would come across attractive deals on online marketplaces or social media platforms but would fail to receive the goods or services after making payment. In some cases, the victims could also be sellers who did not receive payment after delivering the goods or services to scammers pretending to be buyers. The scammers sometimes provided victims with fake screenshots as "proof of payment".

- Pokémon trading cards were the most common item involved in e-commerce scams, with related cases accounting for 13.6% of the total e-commerce scam cases in 2025, as compared to only 1.0% in 2024. Victims typically come across listings of Pokémon trading cards on Carousell. After expressing interest in the product or pre-order, victims are instructed to make payment or an initial deposit via PayNow or bank transfers. Victims only realise that they were scammed when they fail to receive the products, or when the sellers become uncontactable.

Job Scams

- There was a marked decrease in the number of job scams reported in 2025 – down 38.4% to 5,575 cases, from 9,043 cases in 2024. The total amount lost to job scams also fell by 20.9%, to about $123.5 million in the 2025, compared to $156.2 million in 2024. However, job scams still accounted for the third-highest total losses among all scam types.

- The majority of job scam victims were aged 30 to 49, making up 42.7% of victims for this scam type. The most common platforms used by scammers to contact victims were WhatsApp and Facebook.

- Job scams typically involve victims being offered online jobs that can be performed from home. Victims encounter these "job opportunities" through social media platforms such as Facebook, TikTok, and Instagram or through their own internet searches. Scammers also reach out via messaging platforms such as WhatsApp and Telegram, often adding victims to chat groups or channels. Victims are asked to perform simple tasks for a commission, such as booking or reviewing hotels, restaurants, or products; making advance purchases through orders; completing surveys; "boosting" cryptocurrency values; improving product ratings for online merchants, rating mobile apps to raise their rankings; or liking and following social media posts or accounts. Initially, victims receive small commissions, but once convinced they could earn more, scammers introduced higher-paying tasks. Victims are required to create accounts on scam websites and transfer increasingly large sums of monies to bank accounts or crypto wallets controlled by scammers. Victims would realise they have been scammed only when their commissions stop, withdrawals fail, or scammers disappear.

- In 2025, a notable job scam variant involved victims being persuaded to start online businesses. They were asked to register accounts on scam websites/ applications. When orders were received, victims had to use their own money to purchase the items, with the promise of earning commissions once the orders were delivered. Initially, commissions were paid as promised, but over time, the orders required increasingly larger sums. Victims were then told of issues that required additional payments before funds could be withdrawn. This variant was highly convincing, as victims saw their online balances grow, prompting them to invest more in hopes of higher returns.

- In other cases, scammers would befriend victims online and ask for assistance in their part-time jobs or offer opportunities to earn money. Victims would be provided legitimate e-commerce websites and asked to screenshot specific products and make advance payments to fake "business accounts" to receive commissions with promised refunds. This process would be repeated several times, beginning with low-cost items, before progressing to more expensive ones. Victims would initially receive commissions and refunds, but the

scammers would eventually claim to have encountered issues and stop "paying" victims before becoming uncontactable.

Business Email Compromise Scams

- There is a slight increase in Business Email Compromise scam cases by 2.4% to 377 cases in 2025, from 368 cases in 2024. Although the amount lost to business email compromise scams recorded a significant decrease of 60.1% to $35.3 million in 2025, from $88.5 million in 2024.

- Emails were the most common channel used by scammers to contact victims.

- Through email spoofing, compromised email accounts, or other methods, scammers impersonate business entities (e.g. supplier, vendor, client) or persons within organisations (e.g. senior executives, management, staff) and deceive victims into diverting payment to fraudulent bank accounts or fulfilling monetary requests. A prominent variant within the business email compromise scam (business dealings) is detailed below.

    - Victims would receive emails purportedly from known business entities/contacts (e.g. supplier, vendor, client), informing about a change in bank account details for payment. Victims then make payments to the "updated" bank accounts. Victims realised that the emails were spoofed or compromised, when they received late payment notice from the real business entities or when they checked with the real business entities.

    - Typical prime targets are employees who correspond with other business entities. Consumers may also receive such fraudulent emails, although such instances are rare. In some cases, scammers send out fake invoices with actual company details (e.g. address, letterhead, signature, company stamp).

- Two relatively new and unique narratives were identified within business email compromise scams.

    - Business dealings involving a new business venture – Scammers impersonate senior executives (such as a CEO or Chief Financial Officer) through email, WhatsApp messages, or phone calls to notify the victim of a confidential business opportunity, such as a merger and acquisition or a new project. The victim may be instructed to communicate with a 'credible' representative, such as a lawyer, to facilitate the transaction. In some instances, digital manipulation techniques are used, including via Zoom meetings, to enhance the scam's credibility. Confidentiality and secrecy are emphasised, and the

victim may be required to sign a non-disclosure agreement (NDA) to dissuade him/her from consulting colleagues or other senior executives. Ultimately, the victim is asked to transfer funds for the deal to overseas or local bank accounts.

- Payment diversion involving food delivery merchant-partners – Scammers impersonate as merchant-partners of food delivery platforms such as Grab, Deliveroo & Foodpanda to request changes to their payment bank account details (for account crediting) on such platforms. The targeted staff of these platforms would then update the bank accounts in their systems and victims' earnings are credited to the "new" scammer-controlled bank accounts. The targeted staff realised that the emails were spoofed or compromised when these actual food delivery merchant-partners informed that they did not receive their earnings/payment.

- Businesses are advised to educate their employees on this scam type, especially those who are responsible for making fund transfers, to adopt the following preventive measures:

  - Be mindful of any sudden fund transfer instructions or change in payment bank account details. Always verify the authenticity of individuals giving such instructions.
  - Always verify the authenticity of any information sent through unsolicited messages or calls from unknown numbers.
  - Never disclose confidential/personal information or send money to any unknown persons.

Annex E

Top Contact Methods for Scams

Social Media Platforms

- In 2025, while social media platforms were the most common means by which scammers contacted victims, there was a decrease in the number of scam cases by 30.3% in 2025. In particular, 51.9% were contacted through Facebook, 26.0% were contacted through TikTok, and 14.2% through Instagram.

- Significant decreases were seen in the number of scam cases perpetrated via Meta platforms. Facebook & Facebook related platforms saw a 39.6% decrease while Instagram saw a 44.9% decrease. However, TikTok bucked this trend with cases rising by 37.8% in 2025.

Messaging Platforms

- Similarly, the number of scam cases where scammers contacted victims via messaging platforms decreased by 38.2% in 2025. In particular, 53.5% were contacted through WhatsApp, 37.9% were contacted through Telegram and 4.2% were contacted through Facebook Messenger. The number of scam cases perpetrated on Telegram and WhatsApp also decreased in 2025, with Telegram and WhatsApp cases falling by 44.7% and 32.9% respectively.

Phone Calls

- Phone calls remain a contact method of concern. There was however a 18.7% decrease in the number of scam cases perpetrated via this platform in 2025.

Online Shopping Platforms

- The number of scam cases where scammers contacted victims via online shopping platforms decreased significantly in 2025. Carousell saw a 24.6% reduction in cases, whilst cases on Facebook Marketplace fell 23.5%. Shopee experienced the most substantial decline, with cases dropping 60.4%.

Annex F

SPF's Efforts to Fight Scams and Cybercrime

Enforcement

Strengthening legislative levers

Introduction of caning for scams and scams-related offences

The Criminal Law (Miscellaneous Amendments) Bill was passed on 4 November 2025. Caning for scams and scams-related offences was operationalised on 30 December 2025. Scammers, as well as members and recruiters of scam syndicates will face mandatory caning of at least six strokes and up to 24 strokes. Scam mules who facilitate scams by giving away payment accounts, laundering scam proceeds (including money, gold and other valuables), providing SIM cards and/or providing Singpass credentials may be liable for caning of up to 12 strokes.

Operationalisation of the Protection from Scams Act

2. The Protection from Scams Act was operationalised on 1 July 2025. Since then, the SPF has issued 12 Restriction Orders to banks to restrict the banking facilities of scam victims who remained deeply entrenched despite Police engagement (as at 1 February 2026).

Operationalisation of the Facility Restriction Framework

3. The Facility Restriction Framework for scam mules was operationalised on 1 October 2025. Under the framework, scam mules may face restrictions on banking services that could be used to move scam monies (including digital banking, ATM services and card-based transactions), subscription to new mobile lines, and access to existing Corppass accounts or use of Singpass to register for high-risk services that could be exploited for scams. Restrictions on Corppass and Singpass will take effect at a later phase. 550 money mules, 801 telco mules, and 51 corporate entities have been placed under restrictions (as at 9 February 2026) since the framework was operationalised.

Law enforcement interventions and operations

Efforts by Crypto Tracing Team (CTT)

4. Since its operationalisation in March 2025, the CTT followed up on over 1,800 cases involving the dissipation of virtual assets associated with scams, some involving complex obfuscation techniques such as layering and cross-chain bridging. Leveraging advanced blockchain analytics and a network of 78 industry partners, the

team successfully recovered virtual assets valued at approximately $22.8 million, preventing scammers from accessing these illicit gains. A key milestone in 2025 was the breakthrough collaboration with the Digital Assets Association (DAA), culminating in the joint organisation of the Anti-Scam Forum 2025. This partnership represents a shift toward deeper public-private integration, facilitating direct knowledge-sharing between law enforcement and industry leaders. In 2025, the CTT's efforts resulted in over 380 successful interventions that helped victims avert potential losses of over $8.8 million.

Enforcement operations against scammers and money mules

5. In 2025, the ASCom, together with the Scam Strike Teams (SSTs) in the seven Police Land Divisions, conducted 26 island-wide anti-scam enforcement operations, leading to the investigation of more than 7,000 money mules and scammers, suspected to be involved in scam cases involving losses of over $214 million. The SPF has charged more than 940 scammers and money mules in court, including more than 530 of them under the amended laws of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) and the Computer Misuse Act (CMA).

Enforcement operations to combat scams with high losses

6. To combat scams with high losses, particularly government officials impersonation scams, investment scams and job scams, the ASCom together with the SSTs in the seven Police Land Divisions, conducted a series of targeted operations to disrupt and dismantle the scammers' mule account network, infrastructure and communication channels used to contact victims. In 2025, the SPF conducted eight operations, which resulted in the freezing of more than 2,550 bank accounts involving over $10.4 million in suspected scam proceeds, terminated more than 9,000 phone lines and 6,000 online social media enablers.

Enforcement operations against the misuse of SIM cards

7. Since the operationalisation of the offences targeting the misuse of SIM cards under the Miscellaneous Offences Act on 1 January 2025, the SPF has continued enforcement efforts against those who abuse local SIM cards to perpetrate scams. In 2025, the ASCom along with the seven Police Land Divisions conducted eight operations, which resulted in the termination of over 14,300 mobile lines, arrest of 160 persons and investigation of another 220 persons for their suspected involvement in providing fraudulently registered postpaid SIM cards for monetary gains.

Partnerships to disrupt online criminal content and activities and enforce against scams

8. In 2025, the SPF disrupted more than 115,800 mobile lines, more than 87,700 WhatsApp lines, more than 48,800 online monikers and advertisements, and more than 76,000 websites, of which the majority of disruptions were scam-related. This is a significant **increase** in disruptions as compared to 2024, and was done through collaborations with other government agencies such as the HTX (Home Team Science & Technology Agency), GovTech Singapore and IMDA, as well as major industry stakeholders such as Meta, Carousell, Google and the telco companies.

Disrupted asset	2024	2025	% increase
Mobile lines	> 57,700	> 115,800	> 100%
WhatsApp lines	> 40,500	> 87,700	> 116%
Online monikers and advertisements	> 33,600	> 48,800	>45%
Websites	> 44,900	> 76,000	> 69%

9. The ASCom partners over 180 institutions, including financial institutions, card security groups, fintech companies, cryptocurrency houses, remittance service providers, INTERPOL and overseas law enforcement agencies from jurisdictions such as Hong Kong SAR and Malaysia, to facilitate the swift freezing of accounts and recovery of funds and mitigate victim losses. This is achieved through establishing direct communication channels with these partners. In 2025, the ASCom froze more than 15,000 bank accounts based on reports referred to the ASC and successfully recovered more than $117.7 million fiat currency scam losses. Another $22.8 million in cryptocurrency scam losses was recovered, making up a total recovery of about $140.5 million.

Collaboration with foreign law enforcement agencies

10. Online scams are predominantly carried out by perpetrators based overseas, creating significant investigative and prosecutorial challenges. SPF maintains its commitment to strengthening international partnerships to address the cross-border nature of these crimes, improving asset recovery mechanisms and deepening collaborative enforcement efforts.

Takedown of scam syndicates through collaboration with overseas law enforcement agencies

11. In 2025, the close collaboration between the ASCom and overseas law enforcement agencies resulted in the successful takedown of 17 transnational scam syndicates. These operations targeted diverse criminal enterprises including a fake

friend call syndicate, three suspected money laundering cells, five government officials impersonation scam call centre, and one NFC phishing syndicate. The SPF also conducted a joint operation against gold/cash mules and six syndicates hosting Gateways and Simpools, which target government officials impersonation scams. The coordinated efforts resulted in the arrest of over 47 overseas-based suspects and 194 subjects arrested/traced in Singapore, involving losses of over $52 million.

International cooperation for asset recovery

12. Since the formalisation of "FRONTIER+" in October 2024, involving the anti-scam units of six jurisdictions, namely Singapore, Hong Kong SAR, Thailand, the Republic of Korea, the Republic of Maldives and Malaysia, this initiative has been expanded to a total of 13 jurisdictions in 2025, with Australia, Macao SAR, Canada, Indonesia, Brunei, South Africa and Dubai joining the network last year.

13. Leveraging this platform, several member jurisdictions have conducted two iterations of Operation FRONTIER+ in 2025, namely Singapore, Malaysia, Hong Kong SAR, Macao SAR, Republic of Korea, Republic of Maldives and Thailand, resulting in more than 35,600 money mules interviewed and 2,100 subjects arrested across all jurisdictions, and approximately $28.2 million seized from over 36,000 frozen bank accounts.

Engagement

Project A.S.T.R.O. – Leveraging mass distribution of SMSes to alert scam victims

14. To enhance intervention efforts, ASCom leveraged technology to identify and alert potential scam victims. Through Project A.S.T.R.O. (Automation of Scam-fighting Tactics & Reaching Out), ASCom and its partner banks streamlined information sharing workflows and sent SMSes to scam victims. Many victims remained unaware of the deception until receiving the SMS alerts, prompting them to halt further transfers. In 2025, ASCom worked with partner banks to conduct six operations, sending over 32,800 SMSes to alert more than 26,000 victims. This proactive victim-centric approach averted over $267.5 million of potential losses.

Proactive interventions with potential scam victims

15. The ASCom and the Community Policing Units of the Police Land Divisions regularly conduct joint proactive interventions with potential scam victims. These victims were referred by the financial institutions as they had attempted monetary transfers observed to be suspicious. In 2025, 1,266 such interventions were conducted, averting more than $72.2 million of potential losses.

Government-Industry Collaboration Initiatives

16. The SPF regularly reviews online service providers who should be designated under OCHA based on four broad categories, the extent and impact of the harm relating to the specified offence groups; the reach and projected reach in Singapore of the online service; the designs and nature of the online service; and any other relevant factors.

17. In this regard, TikTok was designated in September 2025 and subject to the COP for Online Communication Services. An example of a measure they have put in place is a fast-track channel with the SPF to facilitate the receipt of reports on scams and/or malicious cyber activities. COP requirements serve as upstream measures to prevent and disrupt scams which use social media, messaging and online shopping platforms as contact methods to reach victims. This helps make the online environment on these platforms less conducive to scam activity and enhances online safety.

18. For instance, Meta has applied user verification measures using Government-issued identification for all Facebook Advertisements and on a risk-based approach for Facebook Pages. With the implementation of these user verification measures, scam cases on Facebook decreased by about 38% from July to September 2025 compared to the same period in 2024.

19. In addition to the COP, Implementation Directives (ID) under OCHA were issued to selected online service providers to tackle specific scam types, concerns and emerging scam trends:

- In September 2025, Meta was directed to strengthen their measures against the increased incidence of scammers exploiting Facebook to perpetrate impersonation scams using videos or images of key Government Office Holders.
- In January 2026, a second ID was issued, directing Meta to extend the measures to Government Office Holders that were not covered in the previous ID, and other individuals whom the SPF assesses are at high risk of being impersonated, as well as implement facial recognition measures on notable Facebook users in Singapore.
- In November 2025, IDs were issued to Apple and Google to implement measures to prevent the spoofing of “gov.sg” and Government agency names on their messaging platforms.

20. The SPF is currently reviewing Meta, Apple and Google’s compliance with these IDs.

21. OCHA has also enabled the SPF to issue directions to online service providers to disrupt scam content or scam accounts hosted online. This limits the reach of online criminal activities and reduces Singapore users' exposure to such harms, including online activity preparatory to the commission of scams. Online service providers have acted on all directions issued, generally within a 24-hour timeframe. This represents a significant improvement in the speed of disrupting criminal activities prior to or during the earlier period of OCHA taking effect. For example, Telegram, which had previously not responded to requests to disrupt online activities with criminal nexus, has now acted on all directions issued to them.

22. Moving forward, the SPF is reviewing the existing OCHA COP to enhance requirements and issuing new OCHA COP for advertising and messaging services. These will be announced in due course.

Public Education

23. The SPF has continued its public education efforts to encourage public adoption of anti-scam measures and promote public awareness on emerging and common scam types, through media campaigns, ground engagements and close partnerships with industry and community stakeholders to co-create and amplify anti-scam initiatives.

Encouraging adoption of protective measures and actions

Increased adoption of the ScamShield Suite of anti-scam resources

24. The **ScamShield app** has over 1.53 million downloads, 2.11 million user checks and 832,000 user reports. The **24/7 ScamShield helpline** has received over 220,000 calls and online chats since its launch and currently receives around 500 to 700 calls daily. Of the calls received, around 85% were enquiries if something is a scam, with the helpline operators assisting callers to avert scams. The **ScamShield Alert social channels** have over 97,800 subscribers, and the **ScamShield website** has garnered over 3.4 million visitors since its launch.

25. The ScamShield Helpline's Interactive Voice Response System (IVRS) now supports navigation in all four official languages. Operators will converse in the callers' preferred languages when possible or transfer calls to suitable operators, though this may not always be feasible during peak periods or night shifts with limited staff.

"I can ACT against Scams" campaign

26. The “I can ACT against scams” campaign achieved strong engagement with nearly 7 in 10 surveyed individuals having seen campaign materials. The “Add” phase reached 63% overall, whilst the “Check” phase improved to 69% reach. Survey results showed 90% found the materials easy to understand, 84% found them relevant, and 82% were motivated to adopt anti-scam behaviours, such as using ScamShield services. Steady increase in ScamShield Suite usage demonstrated the campaign’s effectiveness in driving actual proactive adoption. SPF will continue to utilise this campaign in 2026.

Raising awareness on scam types and latest scam variants

27. In July 2025, SPF collaborated with the Ministry of Finance to disseminate anti-scam advisories warning the public about fake SG60 voucher advertisements on social media and phishing websites. SPF partnered with Ticketmaster to alert the public about concert ticket scams related to BLACKPINK’s Deadline World Tour Concert in November 2025. These targeted advisories helped protect consumers from specific scam threats during high-profile events.

Rallying the community to fight against scams and targeted public education efforts

Tapping on the networks of government, community and industry partners to amplify anti-scam messaging

28. The SPF collaborates with the Ministry of Manpower and NGOs to educate migrant workers and domestic workers on scam prevention through talks, courses, and materials in their native languages. These resources are shared with employers and dormitory operators to reinforce worker vigilance. Regular anti-scam engagements are conducted at dormitories, recreation centres, and areas frequented by migrant workers such as Little India and Peninsular Plaza.

Anti-scam roadshows for the public

29. The "We can ACT against scams" roadshow, held on 8 and 9 November 2025, was the Government's first full-scale anti-scam roadshow emphasising empowerment and shared responsibility in fighting scams. Featuring innovative experiential elements, games, and onsite adoption of anti-scam measures, the event was supported by over 16 partners from Government, industry and community, including Bamboo Builders, InTune Music, Aidha, Google and Virage. About 7,500 visitors actively engaged in activities that led them to adopt anti-scam protective measures, including downloading the ScamShield app, joining the ScamShield Alert WhatsApp channel, and completing SPEO's scam vulnerability checklist.

30. Members of the public can continue to look forward to learning about scams at more anti-scam roadshows in 2026, starting with the SaferSG Together Roadshows in March 2026.

E-commerce Marketplace Transaction Safety Rating

31. The E-commerce Marketplace Transaction Safety Rating (TSR) was launched in May 2022 to raise consumer awareness of the extent to which different e-commerce marketplaces have put in place safety features to protect their users from scams.

32. MHA encourages all e-commerce marketplaces to put in place the recommended safeguards, specifically user verification against Government-issued documentation and secure payment options. These measures have proven to be effective in combatting scams. Several e-commerce marketplaces which have implemented the recommended safety features under the TSR (i.e. Amazon, Lazada, Shopee, TikTok Shop) have seen significantly fewer e-commerce scams than other platforms (i.e. Carousell, Facebook Marketplace). Members of the public are encouraged to be more vigilant when transacting on e-commerce marketplaces that do not have these recommended safety features and thus have a lower rating.

Annex G

Whole of Government's Efforts to Fight Scams and Cybercrime

Anti-scam measures by the Monetary Authority of Singapore (MAS)

Improved Authentication and Verification

Major retail banks have phased out SMS one-time passwords for authentication of debit or credit card transactions for digital token users and implemented additional verification for provisioning of cards into mobile wallets. These measures have made it more difficult for a scammer to perform fraudulent card transactions or provision a customer's card into his own mobile wallet.

Money Lock

2. The usage of Money Lock continues to grow. As at 31 December 2025, at least 479,000 customers have locked up close to $44 billion of savings. Banks will continue to encourage their customers to use this service to limit potential losses should a customer's digital banking access be compromised.

Additional Friction for High-Risk Transactions

3. In October 2025, MAS worked with major retail banks on additional friction for transactions that drain large sums from accounts with significant balances.

4. Major retail banks will progressively introduce additional cooling periods for high-risk activities, such as increasing transaction limits or changing contact details, to provide potential victims an opportunity to re-assess their actions. In-app notifications will also be introduced to help customers verify that an incoming call is indeed from the bank.

5. Overall, these measures will introduce more friction and could impact legitimate transactions. While banks will do their best to minimise the inconvenience and give time for customers to get used to the new measures, there will be some trade-off of convenience for greater security in the ongoing fight against scams.

6. In response to the trend of scammers exploiting cryptocurrency platforms, MAS is also working with digital payment token (i.e., cryptocurrency) service providers to strengthen their anti-scam controls. Measures include stepping up fraud surveillance to detect mule accounts, and introducing friction and anti-scam warnings to safeguard victims from losses through their cryptocurrency accounts.

Anti-scam measures by the Cyber Security Agency of Singapore (CSA)

National Simulated Scams Exercise

7. On 1 February 2026, CSA, with the support of the Ministry of Home Affairs, launched a pilot run of the National Simulated Scams Exercise (NSSE), as part of the Government's public education effort to combat scams. Through robocalls simulating Government Officials Impersonation Scam calls, participants will be able to gain a better understanding of how scams typically work and learn practical steps to protect themselves in a safe environment. The NSSE will be conducted from 1 March to 31 August 2026.

Safe App Portal

8. In October 2025, CSA launched a six-month pilot for the Safe App Portal. The Portal is an online tool that provides actionable safety and security insights on mobile apps to help developers build more secure apps by addressing security weaknesses earlier in the development process. In doing so, they strengthen the baseline security posture of their mobile apps. Developers can conduct an app scan to which generates a security assessment report, which are namely code security issues, uncommon permission requests, and code security issues. Since its inception, the Portal has analysed over 225 unique apps.

"Stop and Check" Cybersecurity Campaign

9. CSA launched the sixth national cybersecurity campaign in September 2025 with the tagline "Stop and Check", to remind the public to take a cognitive break when presented with unsolicited messages and check with official sources before responding. The campaign also promotes three cyber tips, i.e. "Enable 2FA and Using Strong Passphrases", "Update Software Promptly", and "Add ScamShield and Anti-Virus Apps". The campaign is supported by physical roadshows and pop-ups across Singapore throughout 2026. The first pop up would be at CIMB Plaza in end March 2026.

10. CSA concluded its third iteration of the Be Cyber Safe Pop-up and Be Cyber Safe Drama Skit in 2025 which aims to provide an interactive and fun way for students to learn about key cyber threats and ways they can stay safe online. Since its launch in October 2023, the Pop-up has travelled to 177 schools and community spaces while the drama skit has completed 163 shows since it was rolled out in January 2024. A new edition of the drama skit was rolled out in January 2026.

11. To reach out to seniors, CSA continued its collaboration with Singapore Press Holdings (SPH) and Ngee Ann Polytechnic on the 'Youths Help Seniors Go Digital' workshops, with accompanying advertorials providing cybersecurity and scam tips running in vernacular publications. CSA also received strong support from public and

private sector partners such as SPF, People's Association (PA), IMDA, Central Provident Fund Board (CPFB), SAFRA and major local banks to co-develop and disseminate content on scam trends and good cyber hygiene practices.

Anti-scam measures by the Government Technology Agency of Singapore (GovTech Singapore)

SATIS Suite of Scam Detection Tools

12. GovTech Singapore continues to collaborate with SPF and HTX to enhance the Scam Analytics and Tactical Intervention System (SATIS) suite of scam detection tools. SATIS leverages artificial intelligence and machine learning to swiftly triage, assess and disrupt scam-related websites. Powered by GovTech Singapore's proprietary AI/ML classifier, the recursive Machine-Learning Scam Evaluator (rMSE), SATIS enables the authorities to automatically analyse over 400,000 websites daily. Additional enhancements have also enabled the disruption of over almost double the number of malicious websites disrupted every month (>20,000). Beyond actively monitoring for scam websites, SATIS employs advanced techniques to discover additional scam websites based on previously blocked sites. Identified scam websites are automatically sent to GovTech Singapore's partners such as Google Web Risk for disruption. A similar system called SATIS+ disrupts other scam enablers such as mobile numbers, online monikers and payment channels.

Partnership with Global Signals Exchange

13. GovTech Singapore is the first government agency to join the Global Signal Exchange (GSE). In partnership with the SPF, GovTech Singapore sends scam signals-including scam-tainted websites through the GSE to strengthen detection and disruption efforts worldwide.

Strengthening Anti-Fraud Capabilities to Protect Singpass Accounts

14. In 2025, GovTech Singapore, enhanced signals, and deployed advanced machine learning (ML) models that enable 24/7 monitoring and detection of suspicious activities. These enhancements provides enhanced intelligence, improves operational efficiency, and streamlines anti-fraud operations.

15. Within the first two months of deploying advanced ML models, GovTech Singapore escalated 200 suspicious accounts to the SPF, which contributed to the disruption of multiple money mule operations. In 2025, over 4,600 financial accounts that were fraudulently created using Myinfo were terminated.

16. Notably, GovTech Singapore's collaboration with the SPF helped victims of government officials impersonation scams recover significant sums totalling $200,000. The team's efforts also supported wider law enforcement successes, resulting in investigations into 32 suspicious Singpass accounts, six arrests tied to the illegal sale of Singpass accounts, and 46 arrests in SPF-led operations targeting government officials impersonation and investment scams.

Anti-scam measures by the Open Government Products (OGP)

Single SMS Sender ID, 'gov.sg'

17. Since the implementation of single SMS Sender ID, 'gov.sg', for all government agencies, 289 million SMSes have been sent through the platform, and 93% of the public now recognises the gov.sg SMS channel. The platform has expanded to serve 84,299 agency users, attaining an 88.3% positive satisfaction score. Since its implementation, there have been zero scam SMSes sent from the gov.sg ID.

ScamShield app

18. The Government has continued to expand the capabilities of the ScamShield app. In August 2025, push notifications were introduced to close the feedback loop for users. Once a reported number is verified as a scam by the authorities, users receive a push notification from the ScamShield app to inform them of the update, strengthening trust in the reporting process and reinforcing transparency. In addition, users can now submit reports for suspicious emails they receive directly through the app.

19. The app user base has grown by 61.8%, from 944,000 to 1.53 million users. A total of 439,480 activated users have used the "Check for Scams" or "Report a Scam" feature at least once and have rated the app an average of 4.67/5 for in-app satisfaction.

'Unpacked' mobile immersive scam simulation

20. 'Unpacked' is an immersive, mobile-first simulation that allows users experience a scam firsthand to better understand how it unfolds. Since its inception in February 2025, 'Unpacked' has hosted more than 15,924 unique visitors.

Anti-scam measures by the Infocomm Media Development Authority (IMDA)

21. IMDA continues to partner SPF and local telcos to implement measures that strengthen our defence against scam calls and SMSes. Through these efforts, over

260 million potential scam calls and around 40 million potential scam SMS messages were successfully blocked in 2025.

22. On 23 January 2026, IMDA announced that in consultation with SPF, the number of postpaid SIM cards each person can register will be limited to a maximum of 10 across all telcos, effective 28 February 2026. The limit aims to minimise illicit SIM card use and purchases by scammers, whilst accommodating legitimate users who require multiple SIM cards for family or business purposes. This follows earlier tightening of SIM card limits in April 2014 and April 2024 and is the latest in the series of anti-scam measures put in place by IMDA and the telcos to protect the public against scams.

Public can use a self-help SIM card checker to enquire on the number of postpaid SIM cards that are counted as part of the postpaid SIM 10-card limit

23. IMDA, in collaboration with GovTech Singapore, will launch a self-help postpaid SIM card checker as part of a trial for the public to check on the number of postpaid SIM cards under their name and identification document and counted under the limit.

24. The beta version of the self-help tool will be live from 26 February 2026, at 9am. The public can participate in the trial by visiting https://go.gov.sg/simcardhowmany and logging in with their Singpass. An email notification will be sent to the registered email, showing the total number of postpaid SIM cards counted under the 10-card limit. As postpaid SIM cards subscribed by individuals under corporate individual subscription (CIS) plans and data-only SIM cards are not counted towards the limit, this information will not be reflected under the SIM card checker. Members of public who spot discrepancies or suspect that their postpaid SIM cards were fraudulently registered should report to their telcos and ScamShield.

25. For more information on the self-help SIM card checker, please visit https://www.imda.gov.sg/how-we-can-help/anti-scam-measures.

Public can activate features to block all incoming international calls and SMSes

26. Today, all telcos in Singapore offer the features to block incoming international calls and SMSes on mobile and residential fixed lines. To date, over 1.1 million subscribers have activated the feature to block overseas calls and over 270,000 subscribers have activated the feature to block overseas SMSes.

27. Subscribers are encouraged to activate the features to prevent the incidence of receiving scam calls and SMSes from overseas numbers if they do not expect to get any overseas calls or SMSes. Subscribers can also check in with their respective telcos for more information on how to activate the features.

Proactive detection and blocking of local scam numbers

28. To further protect the public against scam calls, IMDA has been working with telcos to enhance their capability to detect and act against the suspected misuse of local mobile numbers based on suspicious traits. Since mid-2024, such efforts have led to disruption of around 100,000 mobile lines.

Anti-scam measures by the Central Provident Fund Board (CPFB)

29. On 2 February 2026, CPFB launched the Trusted Contact notification service and the CPF Safety Switch. Both initiatives aim to provide members with additional ways to safeguard their CPF accounts.

Trusted Contact notification service

30. With the new Trusted Contact notification service, CPF members aged 21 and above will have the option to appoint up to two Trusted Contacts who would receive a copy of the same notifications for important transactions[6]. This **optional** service provides members with an additional safeguard by enabling someone they trust, such as a family member, to help spot suspicious transactions and intervene promptly.

31. Trusted Contacts cannot view their appointer's CPF account details beyond the brief information included in the notifications and cannot transact on the appointer's behalf. They serve only as an additional pair of eyes to monitor key account activity and have no legal obligations or liabilities. This design limits potential misuse as existing withdrawal safeguards remain in place to protect members.

CPF Safety Switch

32. The CPF Safety Switch is a protective measure designed to immediately cease any unintended monetary outflows and prevent informational loss. Available to members aged 55 and above, the CPF Safety Switch allows members to immediately secure their CPF accounts if they suspect that they have fallen victim to a scam.

33. CPF members can call the CPF hotline at 1800-227-1188 to activate the CPF Safety Switch, which disables access to CPF online services on the CPF website and mobile app, stop in-progress withdrawals and halt all disbursements to the member's registered bank account. For added security, the CPF Safety Switch can only be deactivated in person at a CPF Service Centre or via the CPF hotline during operating

[6] Important transactions refer to CPF lump sum withdrawals for immediate retirement needs and updates to daily withdrawal limit, bank account details and contact information.

hours with the assistance of a CPFB officer. Members who do not intend to make withdrawals in the short term and wish to take a precautionary approach to safeguard their CPF account savings against potential scams can consider activating the **CPF Withdrawal Lock** instead[7].

34. CPF members can check their account settings, such as contact details and registered bank account, via the CPF website and follow prompts to review their account settings where relevant. As part of staying vigilant against scams, members should also familiarise themselves with CPFB's official communication channels:

- Calls will only be made from 6227 1188. CPFB will **never** call you via WhatsApp or any other messaging apps.

- WhatsApp messages to CPF members will be from "CPF Board Text Us" or "CPF Board", with the blue verified tick.

- SMSes will only be sent from "gov.sg" sender ID.

- Sender's email address will end with @cpf.gov.sg or @e.cpf.gov.sg. Check that the email address is spelt correctly.

35. More information on CPFB's anti-scam measures can be found at www.cpf.gov.sg/antiscamtips.

[7] For more information on the differences between CPF Safety Switch and CPF Withdrawal Lock, members may visit cpf.gov.sg/switchvslock.