SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Mid-Year Scam and Cybercrime Brief 2026

Key Highlights of the Scams Situation

The scam situation in Singapore improved further in the first half of 2026, continuing the downward trend since 2025.

- In the first half of 2026, scam cases fell by 14.4%, while losses fell by 17.9%. Cases involving losses of S$100,000 or more also fell by 24.5%. This reflects strong partnerships and enforcement measures to:

  - **Prevent and block scammers** from reaching victims. Measures included (i) Implementation Directives issued to Apple, Google and Meta to combat impersonation scams, (ii) implementation of the facility restriction framework, and (iii) enhancements to the Scam Analytics and Tactical Intervention System (SATIS) to scale the proactive disruption of scam websites.

  - **Detect and report scams.** The Singapore Police Force (SPF) continued to work closely with service providers to disrupt scams. In the first half of 2026, SPF disrupted 47,500 scam-related mobile lines, 37,500 WhatsApp lines, 31,600 online monikers and 52,200 malicious websites.

  - **Take enforcement action and recover scam losses.** In the first half of 2026, more than 2,900 money mules and scammers were investigated, with at least 470 charged. Convicted offenders sentenced to caning received between 1 and 3 strokes, with an average sentence of 26 months' imprisonment.

  - **Educate the public.** Efforts included the National Simulated Scams Exercise, anti-scam roadshows, and the ScamShield suite of anti-scam resources to raise awareness and encourage the public to adopt anti-scam measures.

This notwithstanding, scams remain the dominant crime type in Singapore and online platforms remain scammers' preferred method of approach. Elderly victims remain vulnerable to higher average losses compared to other age groups.

- Investment, phishing, job and government officials impersonation scams were among the top five scam types both in terms of case numbers and losses.

- Online platforms continue to be used as a first approach for majority (89.0%) of scam cases. The three Meta platforms alone accounted for 34.1% of total scam cases. Carousell is the only designated online service registering an increase in scam cases in the first half of 2026 compared to the same period in 2025.

- Elderly victims sustained the highest average losses among all age groups.

To advance our fight against scams, we will strengthen scam disruption, tighten anti-scam measures on designated online services, and deter against their non-compliance.

- The National Scams List (NSL) facilitates data sharing between the Police and service providers to scale up and speed up scam disruption. NSL trials with the banking sector have allowed participating banks to identify and disrupt unreported scam accounts. The Ministry of Home Affairs (MHA) has proposed legislation to support the expansion of such data sharing initiatives with digital payment token service providers, banks, online service providers and telecommunication companies.

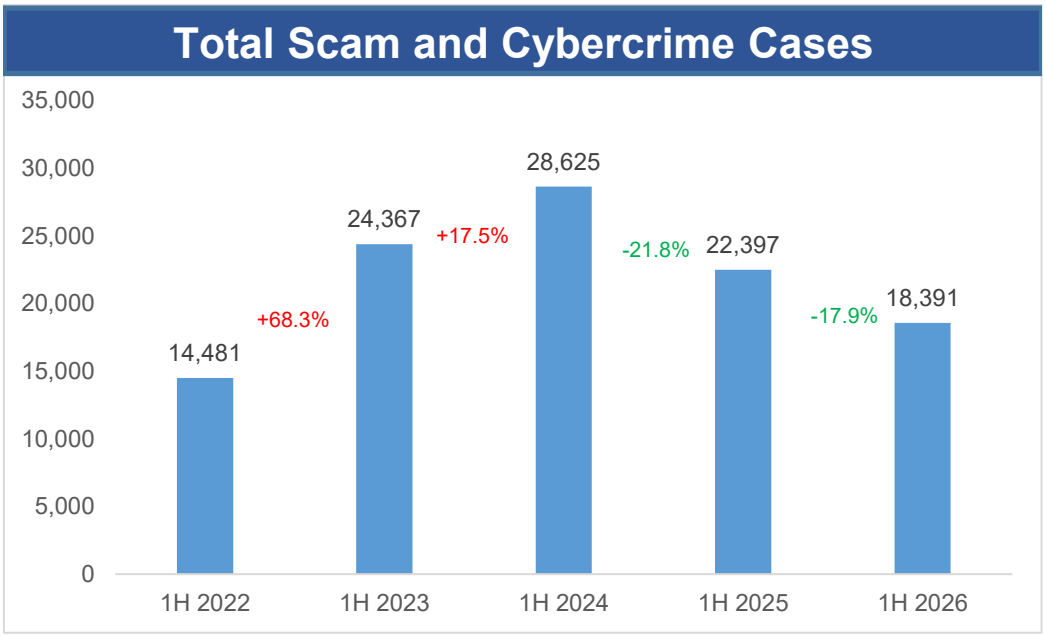
- Codes of Practice (COPs) were issued on 17 August 2026 to designated online service providers to significantly tighten anti-scam requirements, and proactively disrupt scams and malicious cyberactivities affecting people in Singapore.

- MHA and SPF have proposed legislative amendments to empower the Competent Authority to impose penalties of up to S$10 million for non-compliance with the COPs and Implementation Directives issued under the Online Criminal Harms Act (OCHA).

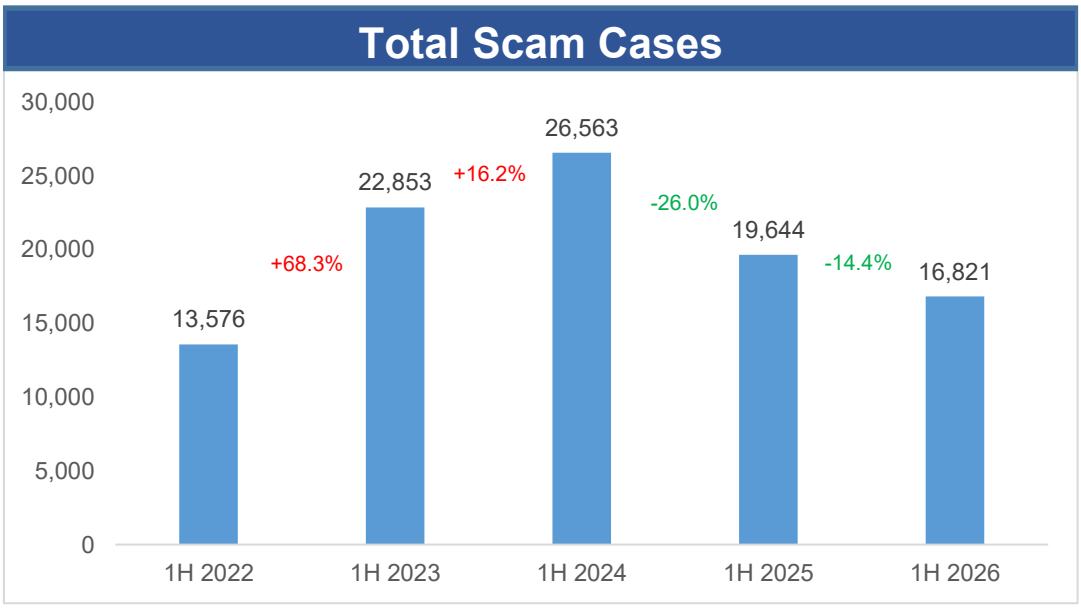
- The Government and service providers have leveraged technological solutions to combat scams. The Government Technology Agency of Singapore (GovTech Singapore) has introduced passkeys to combat phishing scams. Major retail banks have introduced notifications through their bank applications to signal legitimate bank calls. The Government is also taking steps to improve the identifiability of legitimate government communications by introducing a single recognisable number prefix for government agencies to use when calling members of the public, which SPF will pilot later this year. The Government will also consider tagging calls from Government agencies with recognisable caller names, similar to the gov.sg SMS Sender ID.

Overall Scam and Cybercrime Situation for January to June 2026

The overall scam and cybercrime situation **improved further in the first half of 2026**, continuing the downward trend since 2025. From January to June 2026, the **number of scam and cybercrime cases fell by 17.9% to 18,391 cases**, compared with 22,397 cases in the same period in 2025.

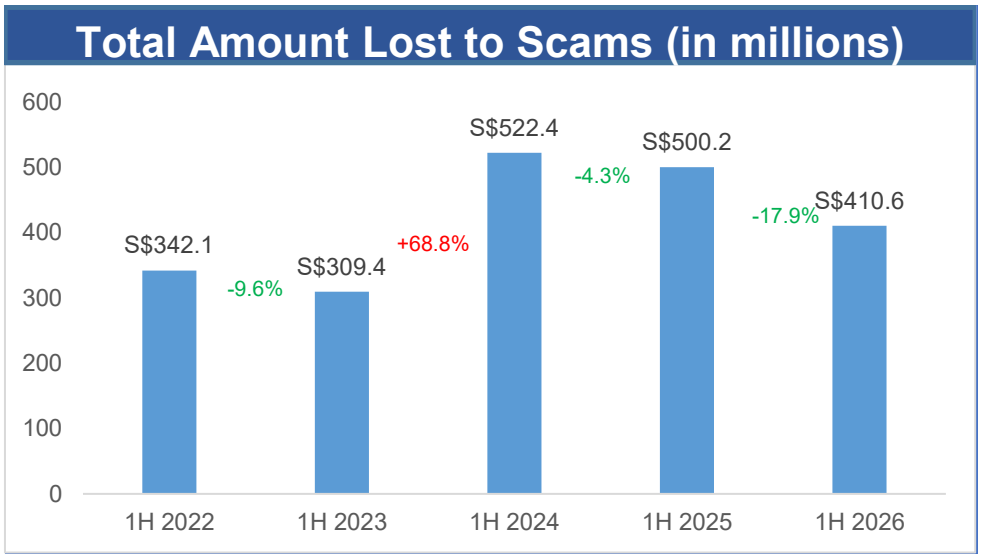


2. Scams accounted for 91.5% of these 18,391 cases. The **total number of scam cases fell by 14.4% to 16,821 cases in the first half of 2026**, from 19,644 cases in the same period last year.



3. The **amount lost to scams also fell by 17.9% to about S$410.6 million in the first half of 2026**, from about S$500.2 million in the same period last year. While

the scam situation has improved, the high number of cases and losses remains a concern, and **tackling scams continues to be a national priority**.



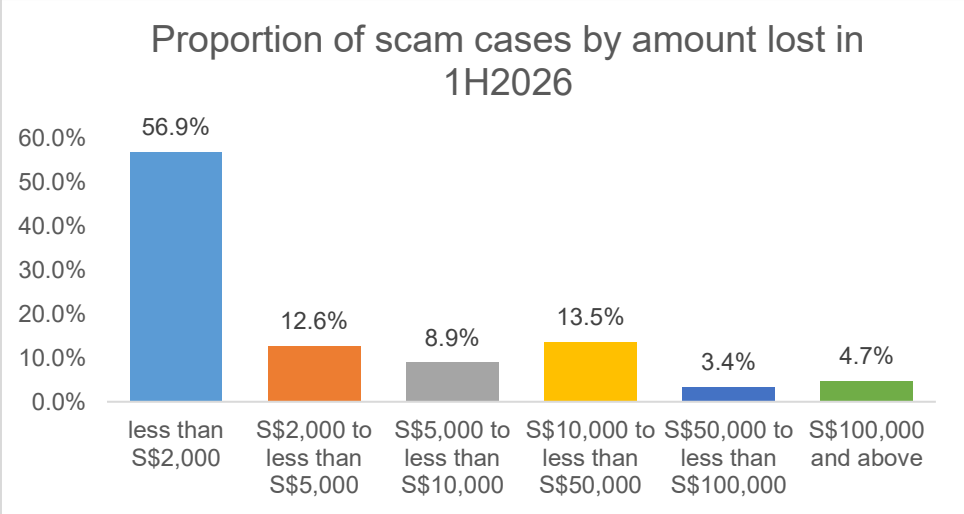
4. In particular, the number of **insurance services scams, fake friend call scams and phishing scams fell significantly** in the first half of 2026 compared with the same period in 2025. Total losses from **government officials impersonation scams, job scams and phishing scams** also fell significantly.

5. The decrease in both scam cases and scam losses is encouraging and reflects the collective efforts of the Government, industry partners and the community to combat scams. We will continue to strengthen our anti-scam measures to stay ahead of evolving scam threats.

6. In the first half of 2026, the Anti-Scam Centre (ASC) **successfully recovered more than S$97.7 million of scam losses**[1] **, which included over S$89.7 million in fiat currencies and over S$8 million in cryptocurrency.** Additionally, through proactive interventions with victims at various stages of being scammed, ASC and its partners helped victims **prevent at least S$127.1 million in potential losses, which included over S$115.4 million in fiat currencies and at least S$11.7million in cryptocurrency.**

7. T**he majority of scam cases, about 69.5%, involved losses of less than S$5,000**, while 4.7% of scam cases involved losses of at least S$100,000. **The median loss per case fell by 19.8% to S$1,350 in the first half of 2026, from S$1,682 in the same period in 2025.**

[1] The amount of scam losses *recovered* refers to funds in the bank accounts and cryptocurrency wallets of scammers or mules, scammed from victims in cases reported to the Anti-Scam Centre (ASC), that have been frozen by the SPF. It does not refer to monies *returned* to scam victims.

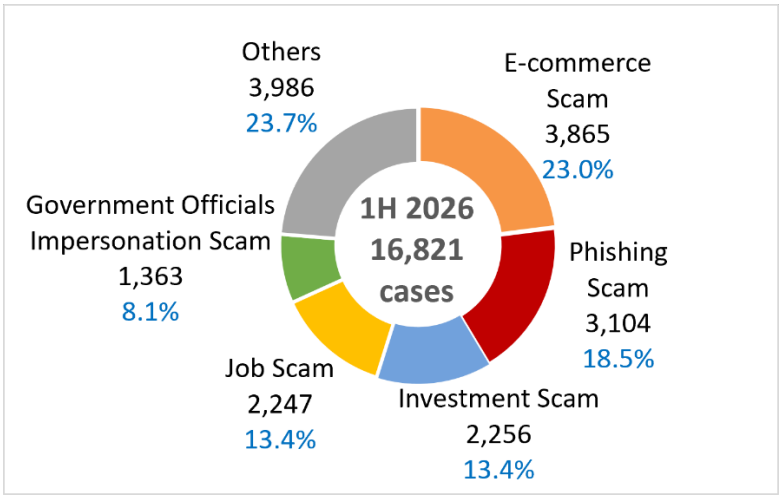


8. The percentage of reported scams involving **self-effected transfers** rose to 80.8% in the first half of 2026, from 78.8% in the same period last year. Scams involving self-effected transfers remain high and form the majority of reported scams. In most cases, scammers did not gain direct control of victims' accounts, but manipulated victims into making monetary transactions through deception and social engineering. SPF urges the public to exercise caution when making fund transfers, including verifying the legitimacy of requests before making any transfers.

Scam and Cybercrime Types of Concern

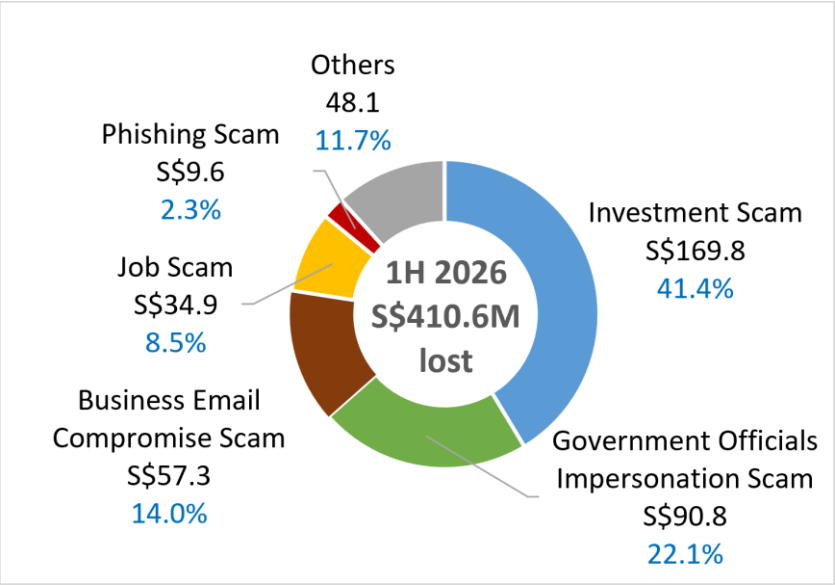
9. In terms of case numbers, **e-commerce scams, phishing scams, investment scams, job scams and government officials impersonation scams** were the top five scam types in the first half of 2026.

Breakdown of scam types by number of cases



10. In terms of the amount lost, **investment scams, government officials impersonation scams, business email compromise scams, job scams and phishing scams** were the top five scam types in the first half of 2026.

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



11. **Cryptocurrency losses[2] continued to form a sizeable percentage of scam losses, accounting for about S$65.5 million, or about 16.0% of total scam losses in the first half of 2026**. Nevertheless, this is a decrease of 43.0% from S$114.9 million during the same period in 2025. This suggests that the cryptocurrency-related measures put in place, such as the formation of the Cryptocurrency Tracing Team in the Cyber Command and the public education efforts highlighting this scam trend may have made an impact. Scammers leverage cryptocurrency as transactions are irreversible and difficult to trace, making asset recovery extremely challenging. **Tether, Ethereum, and USD Coin** were the top cryptocurrencies in terms of amount lost (details in **Annex A**) and accounted for about 95.3% of total cryptocurrency scam losses.

12. The key scam types of concern in the first half of 2026 were:

a) E-Commerce Scams

i. E-Commerce scams recorded the **highest number of reported cases** among all scam types, with an increase of 19.3% to 3,865 cases in the first half of 2026, from 3,240 during the same period in 2025.

ii. The amount lost to e-commerce scam cases **increased** by 18.9% to about S$8.3 million in the first half of 2026, from about S$7.0 million during the same period in 2025.

[2]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. It also does not include cases where victims claimed to have incurred cryptocurrency losses but are unable to provide details of the cryptocurrency transactions.

iii. Pokémon trading cards remained the top item involved in e-commerce scams, with related cases increasing by 116.8% to 605 cases in the first half of 2026, from 279 cases during the same period last year. This accounted for 15.7% of the total reported e-commerce scam cases. Total losses also surged by 172.4% to S$1.2 million in the first half of 2026, from about S$472,000 during the same period in 2025. This increase was largely driven by the rise of the pre-order trend. Victims typically came across listings of Pokémon trading cards or other popular collectibles and fan merchandise (e.g. K-pop lightsticks) on online platforms such as Carousell. To secure the product, scammers persuaded victims to transfer monies as a "deposit" or full payment upfront, with the promised date of delivery usually months away. Victims only realised that they had been scammed when they failed to receive the products by the promised date, or when they came across online posts from other buyers who had been scammed by the same seller.

b) Investment Scams

i. Investment scams recorded the **highest amount loss** amongst all scam types, at S$169.8 million in the first half of 2026. This is a slight decrease of 5.1% from S$178.9 million during the same period in 2025.

ii. The number of investment scams reported remained the **third highest** among all scam types, despite a decrease of 16.2% to 2,256 cases in the first half of 2026, from 2,692 cases during the same period in 2025.

iii. The SPF observed a new trend where scammers, impersonating entities such as National University of Singapore (NUS) and MooMoo to lend credibility to their ruse, would post online advertisements offering free investment tips or strategies. Victims who expressed interest by leaving their contact details would be contacted by scammers and invited into WhatsApp chatgroups masquerading as "investment learning communities" or redirected upon clicking the advertisements to contact scammers via a phone number and invited to join these chat groups. Within these chat groups, scammers posing as mentors would provide seemingly reliable investment tips and stock picks. Other scammers posing as members would attest to the “good advice” given by “mentors”, further enticing victims to seek out “mentors” to invest.

c) Government Officials Impersonation Scams

i. Government officials impersonation scams recorded the **second highest loss** among all scam types in the first half of 2026, despite a decrease in both the number of cases reported and the amount lost.

ii. The amount lost to this scam type fell by 31.7% to S$90.8 million in the first half of 2026, from S$132.9 million during the first half of 2025.

iii. The SPF has observed a continuing trend of monetary transfers via ATM cash deposits and the physical handover of cash and valuables to scammers.

iv. The SPF observed a new trend where scammers would impersonate entities such as Singtel, YouTrip and Prudential. In these cases, victims were subsequently transferred to scammers claiming to be government officials from the Ministry of Law (MinLaw), Monetary Authority of Singapore (MAS) or the SPF. Victims would then be pressured into transferring monies to accounts controlled by scammers.

d) Social Media Impersonation Scams

i. Social media impersonation scams recorded a **significant increase** of 71.3% in amount loss to S$3.9 million in the first half of 2026, from S$2.2 million during the same period in 2025.This increase was driven by a single case that amounted to about S$2.1 million losses in cryptocurrency.

ii. The number of cases reported also **increased** by 47.9% to 587 cases, from 397 cases during the same period in 2025.

iii. A notable social media impersonation scam variant involves scammers approaching victims who are contacts of compromised WhatsApp accounts. In the first half of 2026, there were 391 reported cases, accounting for 66.6% of social media impersonation scam cases. Scammers would cite various reasons such as the need for an emergency loan or issues with a bank transfer, to deceive victims into transferring monies to bank accounts or Payment Service Provider accounts (e.g. Liquid Pay, YouTrip) controlled by scammers. Victims may be asked to perform additional transfers after completing initial transfers. Victims typically realised that they had been scammed only after verifying with the actual owners of the impersonated WhatsApp accounts.

e) Business Email Compromise Scams

i. Business email compromise scams recorded a **significant increase** of 193.1% in **the amount lost** to S$57.3 million in the first half of 2026, from S$19.5 million during the same period in 2025.

ii. The number of business email compromise scams reported **rose** by 67.9% to 262 in the first half of 2026, from 156 during the same period

in 2025. Through email spoofing, compromised email accounts and use of digital manipulation, scammers impersonate business entities (e.g. suppliers, vendors, clients) or individuals within organisations (e.g. senior executives, management, staff), and deceive victims into diverting payments to fraudulent bank accounts or fulfilling monetary requests.

f) Phishing scams

i. Notwithstanding the decrease in messaging platforms as a contact method for scammers in the first half of 2026, the SPF has observed an ongoing trend of phishing cases involving messages delivered via Apple iMessage. In these cases, scammers impersonate courier companies and send messages from email addresses containing random alphanumeric strings or overseas numbers, claiming that a parcel could not be delivered due to an invalid delivery address. Victims are directed to phishing websites resembling legitimate courier platforms and asked to provide their payment card details or internet banking credentials and authorise the transaction using their digital tokens under the pretext of paying a small re-delivery fee. In some cases, after victims were tricked into providing their OTPs, their cards were added to Google Pay or Apple Pay or their bank accounts were logged in from unfamiliar devices. Victims would only discover that they had been scammed after noticing unauthorised transactions made to their bank accounts.

ii. Members of the public are reminded to exercise vigilance when receiving unsolicited messages, avoid clicking on embedded links, and verify delivery matters directly through the courier's official website or mobile application.

13. Details of the top 10 scam types in Singapore can be found in **Annex B.**

14. A background of the other common or notable scam variants is at **Annex C**.

Top Contact Methods

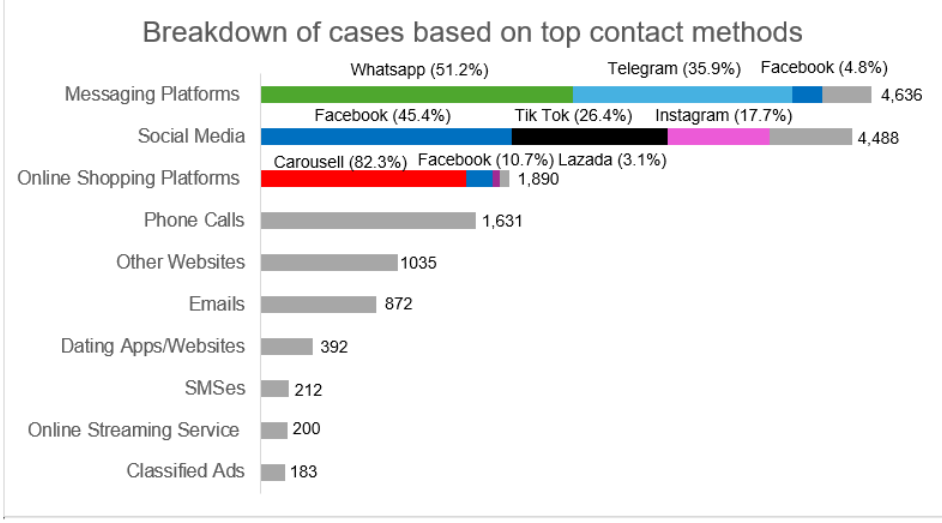
15. **Messaging platforms (27.6%), social media (26.7%), online shopping platforms (11.2%) and phone calls (9.7%)** were the top contact methods used by scammers to reach out to victims.

16. While messaging platforms, social media and phone calls remain the top contact methods for scammers, there has been a decrease in reported scam cases involving these contact methods. Scam cases involving designated online service providers (DOSPs) under OCHA have decreased by 14.1%, continuing the downward

trend from the same period in 2025. For example, cases on TikTok have decreased by 16.2% to 1,244 in the first half of 2026, from 1,485 during the same period in 2025.

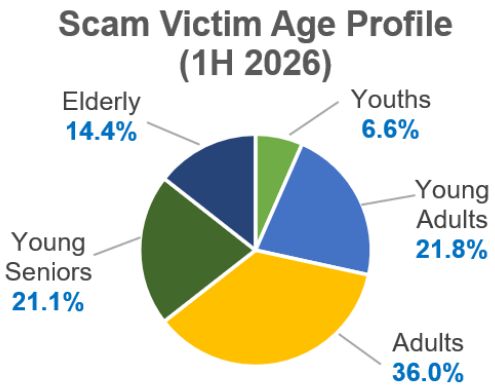
- **Three products from Meta (Facebook, WhatsApp, Instagram) remain of particular concern, as they made up a significant proportion (34.1%) of total cases reported across all platforms exploited by scammers to contact victims.** Cases on Carousell rose by 17.1% to 1,555 in the first half of 2026, from 1,328 during the same period in 2025.

- More details of the platforms commonly used by scammers can be found in **Annex D**.



Scam Victim Profile

17. **In the first half of 2026, 64.4% of scam victims were youths, young adults, and adults aged below 50.** There was a fall in the proportion of elderly scam victims to 14.4% in the first half of 2026, from 15.0% during the same period in 2025. **Nevertheless, the average amount lost per elderly victim has risen to $42,347 in the first half of 2026, from S$35,374 in the same period in 2025. This remained the highest among the various age groups**. More details in **Annex E**.



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

18. The SPF continues to work closely with other Government agencies and private sector stakeholders to strengthen scam intervention measures to minimise victims' losses, and share information to prevent scams. The SPF also strengthened local and international partnerships through the Anti-Scam Conference 2026, held in Singapore from 11 to 13 May 2026 under the theme "United Against Scams". The conference brought together representatives from over 20 countries, international organisations, industry partners and local stakeholders to share operational insights, exchange best practices, and strengthen partnerships to better detect, disrupt, and investigate scams. At the opening ceremony, Mr Goh Pei Ming, Senior Minister of State for Ministry of Home Affairs & Ministry of Social and Family Development, announced that the SPF would form a new Cyber Command to bring together and scale up SPF's counter-scam and cybercrime capabilities to better protect Singaporeans from crime in the cyberspace. The Cyber Command was established on 3 July 2026.

Some of the **recently implemented key anti-scam initiatives** include (more details at **Annex F**):

Prevent and block scams

- While multiple factors contribute to the improving scam situation, the decrease in scam cases involving DOSPs demonstrates the importance of upstream safeguards in reducing scammers' abilities to target Singapore users. However, scammers have continued to adapt their tactics and exploit new technologies and platform features, including messaging applications, online advertisements and video conferencing. To address these risks, the OCHA Office has developed and issued three **COPs** for Online Messaging and Conferencing Services, Social Media services and e-Commerce Services on 17 August 2026. These COPs require designated online services that pose significant risk to Singapore users to implement additional safeguards against scams, building on the earlier COPs introduced in June 2024. Further details of the COP requirements can be accessed at this link: SPF | Issuance Of Codes Of Practice Under The Online Criminal Harms Act .
- MAS worked with the Association of Banks in Singapore to **discontinue the PayNow nickname feature** for retail customers on 6 June 2026 to prevent scammers from exploiting the nickname feature to masquerade as legitimate individuals or organisations. In addition, major retail banks have progressively introduced notifications through their bank apps, triggered at the start of outbound calls to customers, so that customers can verify whether an incoming call claiming to be from the bank is legitimate.

- The **Facility Restriction Framework** was expanded in 2026 to include restrictions on new Digital Token Payment account registrations from 24 April 2026, and on the use of Singpass to register for high-risk services such as bank accounts, mobile lines, and corporate entities from 1 July 2026.
- From 1 July 2026, GovTech Singapore introduced **passkeys as a new, password-free login method for Singpass**, designed to strengthen protection against phishing scams. To log in, users select the passkey option on the Singpass login page and verify their identity using biometrics (fingerprint or facial recognition) or their six-digit Singpass app passcode.
- The Infocomm Media Development Authority (IMDA) implemented the **postpaid SIM card limit of 10 cards per subscriber** across all telcos in February 2026, to minimise the illicit SIM cards use by scammers. The public can visit https://go.gov.sg/simcardhowmany, a self-help SIM card checker developed by GovTech Singapore, in collaboration with IMDA, to check the number of postpaid SIM cards that are counted within the 10-card limit, under their name. In addition, the Government uses analytics to proactively detect and disrupt fraudulently registered phone lines.
- SPF is working with OGP and MDDI to introduce a single, easily recognisable prefix number which SPF officers will use to call members of the public. This will be piloted with SPF later this year.

Detect and report scams

- CSA has been supporting SPF by providing **specialised technical malware analysis** to better understand the technical aspects of scam campaigns. In 2026, CSA analysed two malicious Android Application Kit (APK) samples associated with a scam campaign impersonating a local business. The analysis assessed that the malware was likely distributed as a malware-as-a-service model, where threat actors make minor customisations to readily available malware kits before deployment. CSA shared its technical findings with SPF to provide insights into the malware's behaviour.
- The SPF has been working with private sector partners to take down scam operations before more victims are harmed. In a trial under the NSL initiative, the SPF shared scam-linked account numbers and account holder details with selected participating banks. For every scam-linked account shared by SPF, participating banks were able to identify and disrupt at least one additional account that was previously unreported.
- In the first half of 2026, the SPF disrupted more than 47,500 mobile lines that were scam-related across all telecommunication companies. Notably, **SIMBA and StarHub had the highest number of disrupted local mobile lines, with 11,491 and 12,481** lines affected respectively. **Of the StarHub lines, 11,032**

(88%) were registered under eight Telecom, a sub-brand of StarHub. The SPF will continue to take tough enforcement actions against errant retailers who distribute SIM cards that facilitate scams.

Enforce against scams and recover lost monies

- In the first half of 2026 alone, more than 2,900 money mules and scammers suspected of involvement in scam cases were investigated, and at least 470 have been charged by the SPF.
- Since caning was introduced for scam-related offences on 30 December 2025, convicted offenders where caning was meted out have received between **1 and 3 strokes** of the cane and an average sentence of 26 months' imprisonment.
- Scams are predominantly carried out by perpetrators based overseas. To address this, SPF works with international partners to conduct cross-border enforcement operations.
    - In the first half of the 2026, SPF participated in Operation First Light, a global anti-fraud operation coordinated by INTERPOL across 97 countries, where Singapore's efforts contributed to 1,938 arrests, 4,065 bank accounts frozen and approximately S$59 million in illicit assets intercepted.
    - To strengthen cross border enforcement efforts, FRONTIER+ was established on 21 October 2024. The network has been expanded to cover 14 jurisdictions, with the inclusion of the United States in the first half of 2026. Leveraging this platform, several member jurisdictions have conducted Operation FRONTIER+ III in the first half of 2026, namely Singapore, Malaysia, Hong Kong SAR, Macao SAR, Republic of Korea, Indonesia, Republic of Maldives, Thailand, Brunei and Canada, resulting in more than 7,500 subjects investigated, and 3,000 subjects arrested across all jurisdictions, and approximately S$207 million seized from over 101,000 frozen bank accounts.

Public Education

- The six-month pilot run of the National Simulated Scams Exercise, which is held from 1 March to 31 August 2026, is part of the Government's public education effort to combat scams. The exercise involves the use of robo-callers simulating scammers and closely references real-life scam scripts used in Government Officials Impersonation Scam calls. Close to about 5,000 people have participated in the exercise so far and learnt practical steps to protect themselves from scams.
- The E-commerce Scam Situation Report (ESSR) replaces the E-commerce Marketplace Transaction Safety Ratings (TSR), offering a more comprehensive assessment of e-commerce scam risks. Unlike the TSR, which primarily focused on the safety features of e-commerce platforms, the ESSR provides a

broader overview of the e-commerce scam situation and ranks the top 10 platforms according to reported scam losses and cases. This enables members of the public to better assess potential risks and exercise greater caution when transacting on higher-risk platforms. For more details, please refer to **Annex G**.

19. Beyond the measures above, MHA has proposed a series of legislative amendments under the Scams (Countermeasures) and other Matters Bill to:

a. Enable and safeguard scam-related information exchange between the Police and service providers;

b. Strengthen application of the Facility Restriction Framework to restrict the provision of services to identified persons;

c. Introduce new offences to deter the misuse of online accounts;

d. Enhance the Online Criminal Harms Act (OCHA); and

e. Enhance the effectiveness of Police operations.

More details can be found in MHA's press release accessible at First reading of the Scams (Countermeasures) and Other Matters Bill | Ministry of Home Affairs

Everyone Plays a Part in Fighting Scams

20. Everyone plays a vital role in keeping Singapore safe and secure and must remain vigilant, as scammers will evolve their methods and tactics. Individuals should take proactive steps to strengthen their protection against fraudulent activities by adopting anti-scam measures. When in doubt, they should seek advice from reliable sources, call the ScamShield Helpline at 1799, or use the ScamShield application for verification.

21. Criminal syndicates continue to perpetrate scams in Singapore through local and foreign mules. The public must remain vigilant to avoid becoming unwitting participants. This includes allowing fraudsters to use their financial accounts such as banking facilities to transfer illicit funds, providing access to their Singpass credentials, or supplying criminals 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.

22. Business entities, especially financial institutions, digital marketplaces and telecommunications providers, 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.

23. The Government remains committed to strengthening safeguards and initiatives that make it increasingly difficult for scammers to exploit Singaporeans. The Government will also continue to deliver comprehensive anti-scam public education programmes, as well as equip citizens with essential knowledge, capabilities and resources to protect themselves against scams.

PUBLIC AFFAIRS DEPARTMENT
SINGAPORE POLICE FORCE
26 AUGUST 2026 @ 3PM

Annex A

Top 5 Cryptocurrencies Lost to Scams in the first half of 2026

(Based on estimated value in Singapore dollars)

Cryptocurrency	Cryptocurrency units lost	Estimated value in Singapore dollars (approximate)
Tether	35,978,662.91	S$46.1M
Ethereum	3,561.31	S$10.2M
USD Coin	4,761,265.14	S$6.1M
Bitcoin	15.23	S$1.4M
XRP	202,330.14	S$332K

Annex B

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

Types of Scams	Cases reported		Total amount lost in Singapore Dollars (approximate)		Average amount lost in 1H 2026
	1H 2026	1H 2025	1H 2026	1H 2025	
E-commerce Scams	3,865	3,240	S$8.3M	S$7.0M	S$2,160
Phishing Scams	3,104	3,772	S$9.6M	S$30.0M	S$3,108
Investment Scams	2,256	2,692	S$169.8M	S$178.9M	S$75,267
Job Scams	2,247	2,717	S$34.9M	S$64.0M	S$15,534
Government Officials Impersonation Scams	1,363	1,772	S$90.8M	S$132.9M	S$66,643
Social Media Impersonation Scams	587	397	S$3.9M	S$2.2M	S$6,698
Sexual Services Scams	478	538	S$1.5M	S$1.6M	S$3,156
Loan Scams	384	456	S$2.1M	S$3.3M	S$5,518
Internet Love Scams	373	428	S$8.4M	S$12.2M	S$22,709
Fake Friend Call Scams	353	1,052	S$818K	S$3.0M	S$2,319
Top 10 scams	**15,010**	**17,064**	**S$330.3M**	**S$435.5M**	**S$22,011**

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

Annex C

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 40.8% 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.

- In the first half of 2026, the SPF received at least 30 reports where scammers impersonating goverment officials exploited Voice over Internet Protocol (VoIP) to contact victims.

- Government officials impersonation scams typically involve scammers first impersonating as bank, telecommunication companies (telcos) or financial institution representatives (e.g. Unionpay, NTUC, Prudential), and victims were subsequently transferred to scammers claiming to be government officers (e.g. MAS, MinLaw, SPF) or foreign law enforcement to pressure victims into performing money transfers. The notable variants include:

    - **Impersonation of bank, telcos or financial institution representatives and local government officials through calls (94.2% of cases)** – Victims typically receive unsolicited calls from scammers impersonating representatives from banks, telecommunication companies or financial institutions (e.g. Unionpay, NTUC, Prudential), who cite suspicious credit card transactions or new phone lines signups; outstanding bills. When victims deny involvement, they are transferred to scammers impersonating government officials (e.g. MAS, MinLaw, SPF), who accuse them of money laundering. Scammers then instruct victims to transfer money to purported "safety accounts" designated by the Government. In many cases, victims were also instructed to hand over cash and valuables for "investigation purposes".

    - **Impersonation of foreign and local government officials through calls (5.8% of cases)** – Victims receive calls from individuals impersonating Immigration & Checkpoints Authority (ICA) officers, airline or telco representatives who claim that victims' details were misused. Victims are transferred to another scammer claiming to be a foreign law enforcement officer, who then demand money for "investigation or bail purposes".

- The Police would like to highlight continuing trends observed in monetary transfers where victims were instructed to:
    - Transfer money or make cash deposits via ATMs to scammer-controlled bank accounts.
    - Hand over cash, gold and/or to purchase luxury watches to scam mules.
    - Hand over ATM/bank cards to scam mules and disclose card's PIN number to scammers. Victims subsequently discover cash withdrawals or money transfers out from their bank accounts.

Investment Scams

- Victims of investment scams were typically exposed to "investment opportunities" through various online channels. This includes recommendations from online acquaintances, their own internet searches, online advertisements, unsolicited messages or calls from scammers or being added into "investment" chatgroups or channels on messaging platforms by scammers.
- The Police have observed a new trend where scammers would post online advertisements offering free investment tips or strategies, impersonating entities such as NUS and MooMoo to lend credibility to their ruse. Victims who expressed interest by leaving their contact details would be contacted by scammers and invited into WhatsApp chatgroups masquerading as "investment learning communities" or redirected upon clicking the advertisements to contact scammers via a phone number and invited to join these chat groups. Within these chat groups, scammers posing as mentors would provide seemingly reliable investment tips and stock picks. Scammers posing as members would attest to the "good advice" given by "mentors", further enticing victims to seek out "mentors" to invest.
- Once convinced, scammers would instruct victims to transfer funds to specified bank accounts or cryptocurrency wallets, or make payments via their bank cards. The Police also observed another concerning trend where victims would hand over large amount of cash and valuables to scam mules under the belief that they were making legitimate investment.
- In some cases, victims were instructed to create investment accounts through fraudulent investment websites or through fake investment applications downloaded from official app stores. These websites or applications may claim affiliation with legitimate entities, shell companies, or fictitious organisations. Such interfaces display fictitious investment progress and returns to give victims a false sense of assurance that the investment is growing, thereby luring victims into depositing progressively larger sums of money for "investment".
- Although some victims initially received small returns on their investments, victims would typically discover that they had been scammed after encountering difficulties in withdrawing large sum investment returns, were subjected to

repeated demands for additional “fees” or “taxes” to process their withdrawal or were alerted by banks or the Police.

E-Commerce Scams

- The majority of e-commerce scam victims were aged 30 to 49, making up 41.3% of victims for this scam type. The most common platforms which scammers used to contact e-commerce scam victims were Carousell and Telegram.
- 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".

Social Media Impersonation Scams

- The majority of social media impersonation scam victims were aged 50 to 64, making up 35.5% of victims for this scam type. The most common platforms used by scammers to contact victims were WhatsApp and Facebook.
- Social media impersonation scams typically involve scammers impersonating acquaintances (e.g. friends, family members, colleagues) on social media (e.g. Facebook, Instagram) and/or communications platforms (e.g. WhatsApp, Telegram, WeChat) to deceive victims into providing OTPs, bank-related details (e.g. login credentials, card information), personal information (e.g. mobile no.) and/or transferring monies to scammers. Asides monetary losses, victims may lose access to their social media and/or communications accounts.

Business Email Compromise Scams

- 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 involved victims receiving emails purportedly from known business entities/contacts (e.g. supplier, vendor, client), informing or requesting a change in bank account details for payment. In some instances, victims would receive fraudulent invoices with actual company details (e.g. address, letterhead, signature, company stamp), instructing them to transfer payment to specified bank accounts. Victims then proceeded to make payments to the fraudulent “updated” bank accounts. Victims would realise that the emails were

spoofed or compromised, when they received late payment notices from or upon verification with the real business entities.

- Another variant involved victims receiving fraudulent emails purportedly from their CEOs or supervisors to purchase gift cards. In some cases, scammers would request victims' personal mobile numbers to continue communication via WhatsApp, before instructing them to purchase gift cards for work-related purposes such as staff incentives or gifts for clients. The gift cards purchased were predominantly Razer Gold gift cards, which were largely bought in person at physical retail outlets such as 7-Eleven. Scammers would then instruct victims to scratch and provide the redemption codes behind the cards. Victims would only realise that the emails were spoofed or compromised after checking with their bosses / colleagues.
- 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.

Phishing Scams

- The majority of phishing scam victims were aged 30 to 49, comprising 40.8% of victims for this scam type.
- Phishing scams typically involve emails, text messages or calls from scammers posing as government officials, financial institutions or businesses. Victims would be tricked into providing 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. Victims would discover that they had been scammed when they found unauthorised transactions made from their bank accounts or debit/credit cards.

Job Scams

- There was a decrease in the number of job scams reported in the first half of 2026, by 17.3% to 2,247 cases, from 2,717 cases in the first half of 2025. The total amount lost to job scams in the first half of 2026 also saw a decrease by 45.5% to about $34.9 million in the first half of 2026, from about $64.0 million

during the same period last year. Job scams ranked fourth in terms of total amount lost in the first half of 2026 among all scam types.

- The majority of job scam victims were aged 30 to 49, making up 38.6% of victims for this scam type. WhatsApp and Facebook were the most common platforms which scammers used to contact victims.
- Job scams typically involve victims being offered online jobs that can be done from home. Victims may come across these “job opportunities” on social media platforms such as Facebook, TikTok and Instagram, through internet searches, or via messaging platforms such as WhatsApp and Telegram. In some cases, they would also be added to chat groups or channels promoting such jobs. Victims were usually asked to complete simple tasks for a commission, such as booking hotels and travel orders, rating or reviewing restaurants, online product listings or mobile apps, making advance purchases, completing surveys, or liking and following social media posts or accounts. While victims would initially receive small commissions, they were eventually asked to pay more to complete additional tasks or unlock higher earnings. They would realise that they had been scammed when they failed to receive their commission, could not withdraw their monies, or when the scammers became uncontactable.
- In the first half of 2026, online tasks continued to be a major variant of job scam reports. Separately, social media boosting emerged as a notable growing variant and should be closely monitored. While its case volume remained lower than online tasks variant, the sharp increase suggests that scammers may be making greater use of social media-related tasks, such as asking victims to like, follow, share or boost posts, accounts, product listings or online merchants in return for commissions.

Annex D

Top Contact Methods

Messaging Platforms

- In the first half of 2026, while messaging platforms were the most common means by which scammers contacted victims, there was a slight **decrease** in the number of scam cases by 2.0% to 4,636 in the first half of 2026, from 4,731 during the same period in 2025. The number of scam cases perpetrated on WeChat, WhatsApp and Telegram also **decreased** in the first half of 2026, with WeChat cases falling by 33.0%, WhatsApp cases falling by 6.6%, and Telegram cases falling by 2.1%.

Social Media Platforms

- The number of scam cases where scammers contacted victims via social media platforms **decreased** by 23.7% to 4,488 in the first half of 2026, from 5,883 in the same period in 2025. In particular, 45.4% were contacted through Facebook, 26.4% were contacted through TikTok, and 17.7% through Instagram.

- Significant decreases were seen in the number of scam cases perpetrated via Meta platforms. Facebook saw a 35.9% decrease, TikTok saw a 16.2% decrease and Instagram saw a 10.3% decrease.

Online Shopping Platforms

- Online shopping platforms remain a contact method of concern. There was a 1.8% **increase** in the number of scam cases perpetuated via this platform to 1,890 in the first half of 2026, from 1,857 during the same period in 2025. In particular, 82.3% of these cases occurred on Carousell, 10.7% on Facebook Marketplace, and 3.1% on Lazada.

Phone Calls

- Phone calls remain another contact method of concern. There was however a 49.1% decrease in the number of scam cases perpetrated via this platform, to 1,631 in the first half of 2026, from 3,206 during the same period in 2025.

Annex E

Scam Victim Profile

- **Youths, aged 19 and below, made up 6.6% of scam victims.** 45.6% fell prey to e-commerce scams, while 16.1% fell prey to phishing scams and 14.9% fell prey to job scams. Youths most commonly respond to scammers via messaging platforms, online shopping platforms and social media. The average amount lost by youths to scams was S$2,336 per victim.

- **Young adults, aged 20 to 29, made up 21.8% of scam victims.** 36.1% fell prey to e-commerce scams, while 16.1% fell prey to job scams and 16.0% fell prey to phishing scams. Young adults most commonly respond to scammers via messaging platforms, social media and online shopping platforms. The average amount lost by young adults to scams was S$7,498 per victim.

- **Adults, aged 30 to 49, made up 36.0% of scam victims.** 27.0% fell prey to e-commerce scams, while 21.2% fell prey to phishing scams and 14.3% fell prey to job scams. Adults most commonly respond to scammers via social media, messaging platforms and online shopping platforms. The average amount lost by adults to scams was S$17,000 per victim.

- **Young seniors, aged 50 to 64, made up 21.1% of scam victims.** 20.9% fell prey to phishing scams, while 19.7% fell prey to investment scams and 13.6% fell prey to job scams. Young seniors most commonly respond to scammers via social media, messaging platforms and phone calls. The average amount lost by young seniors to scams was S$32,879 per victim.

- **The elderly, aged 65 and above, made up 14.4% of scam victims.** 23.0% fell prey to government officials impersonation scams, while 22.2% fell prey to investment scams and 14.5% fell prey to phishing scams. Elderly most commonly respond to scammers via messaging platforms, social media and phone calls. **The average amount lost by the elderly to scams was S$42,347 per victim, which is the highest across all age groups**.

Annex F

SPF and WOG's Efforts to Fight Scams and Cybercrime

Prevent and block scams

Operationalisation of the Facility Restriction Framework

1. The Facility Restriction Framework for scam mules, which was operationalised on 1 October 2025 by the SPF alongside the MAS, IMDA and GovTech Singapore, has resulted in 1,423 money mules, 1,439 telco mules, and 53 corporate mules being placed under restrictions (as of 30 June 2026). The framework was expanded from 24 April 2026 to include restrictions on the registration of new Digital Token Payment (DPT) accounts, and on 1 July 2026 to include restrictions on the use of Singpass to register for high-risk services that could be exploited for scams such as bank accounts, mobile lines and corporate entities.

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 18 Restriction Orders to banks to restrict the banking facilities of scam victims who remained deeply entrenched despite Police engagement (as at 30 June 2026).

Project A.S.T.R.O (Automation of Scam-fighting Tactics & Reaching Out)

3. In the first half of 2026, ASCom worked with partner banks to conduct three operations, sending over 11,700 SMSes to alert more than 9180 victims. This proactive victim-centric approach averted over S$99.5 million of potential losses.

New and Enhanced OCHA Codes of Practice (COPs)

4. To strengthen safeguards against scams on messaging platforms, the new COP for Online Messaging and Conferencing Services will now be applied to Apple iMessage, Apple Facetime (collectively as Apple), Google Message and Google Meet (collectively as Google).

5. The new COP for Social Media Services strengthens safeguards against scam vectors increasingly exploited by scammers, including online advertisements and other platform functionalities. An example of the safeguard includes prompt removal of published advertisement when there is reason to suspect that the advertisement is in furtherance of a scam. The enhanced COP for e-Commerce services builds upon existing requirements for seller verification and payment protection. Designated online service providers will be required to introduce stronger account holder's consent before permitting logins from new or unrecognised devices. To safeguard against fraudulent

advertisements, designated online service providers are also required to verify that the advertisers are licensed by MAS or other applicable Singapore authorities before they could publish advertisements offering financial services. Further details of the new and enhanced COP requirements can be accessed at this link: SPF | Issuance Of Codes Of Practice Under The Online Criminal Harms Act

Money Lock (MAS)

6. Banks continue to encourage customers to use Money Lock. As at 30 June 2026, about 589,000 customers have locked up close to S$49 billion of savings. Customers are encouraged to use this service to limit potential losses should a customer's digital banking access be compromised.

Strengthen Prevention and Detection of High-Risk Transactions (MAS)

7. Major retail banks have introduced 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. Enhanced fraud surveillance rules to block or hold transactions that drain large sums from customer accounts of significant balances were also introduced since October 2025.

8. MAS is working with GovTech Singapore, SPF and participating banks on a proof-of-value to test whether artificial intelligence models trained on cross-bank and public-private data can improve overall detection of scam transactions.

9. MAS is working with digital payment token service providers (i.e., cryptocurrency service providers) to strengthen their anti-scam controls, such as stepping up fraud surveillance to detect mule accounts and implementing account safeguards to prevent losses through customers' cryptocurrency accounts.

Single SMS Sender ID, 'gov.sg' (OGP)

10. Since the implementation of single SMS Sender ID, 'gov.sg', for all government agencies, 360 million SMSes have been sent through the platform, and 84% of the public recognises the gov.sg SMS channel. The platform is used for 98.5% of agency use cases and has recorded a positive satisfaction score of 79.6% among agency users. To date, there have been zero scam SMSes sent from the gov.sg Sender ID.

SATIS Suite of Scam Detection Tools (GovTech Singapore)

11. GovTech Singapore continues to enhance the Scam Analytics and Tactical Intervention System (SATIS) suite of scam detection tools, in collaboration with SPF and

HTX. 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 600,000 websites daily. Additional enhancements have also enabled the disruption of over almost double the number of malicious websites disrupted every month (>15,000). These disruptions prevent millions of attempted visits to scam sites every month.

12. 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 Safe Browsing for disruption. The SATIS suite has also expanded to disrupt various types of scam enablers such as phone numbers, online monikers (e.g., accounts on Facebook, WhatsApp, Telegram, Carousell), bank accounts, fintech and crypto accounts.

Singpass Introduces Passkeys for Safer, Phishing-resistant Login (GovTech Singapore)

13. From 1 July 2026, GovTech Singapore introduced passkeys as a new, password-free login method for Singpass, designed to strengthen protection against phishing scams. To log in, users select the passkey option on the Singpass login page and verify their identity using biometrics (fingerprint or facial recognition) or their six-digit Singpass app passcode.

14. When users create a passkey in the Singpass app, a unique digital key pair is generated. The private key is stored securely on the user's device, while the corresponding public key is registered with Singpass. During login, the private key on the user's device is verified against the registered public key in Singpass to validate an official login.

15. This verification ensures that passkeys work only on the legitimate Singpass login domain and cannot be used on fake websites. Since the private key never leaves the device and no login credentials such as passwords and OTPs are entered or transmitted, there is nothing for scammers to steal – even if users inadvertently land on a fraudulent website.

16. Passkeys strengthen Singpass' role as a trusted gateway to government and private sector services, while supporting GovTech Singapore's broader efforts to protect users from evolving scam and cyber threats. Existing login methods such as QR login,

Face Verification, and SMS One-Time Passwords remain available to ensure continued accessibility for users.

17. Launched in beta for iPhone (iOS) users on mobile browsers, passkeys will be extended to Android users and desktop logins in subsequent phases. Users who have enabled notifications in their settings will receive a push notification in the Singpass app when the feature becomes available to them.

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

18. IMDA continues to partner SPF and local telcos to implement measures that strengthen our defence against scam calls and SMSes. Through these efforts, over 70 million potential scam calls and over 11 million potential scam SMS messages were successfully blocked in the first half of 2026. Today, all telcos in Singapore offer the features to block incoming international calls and SMSes on mobile and residential fixed lines. To date, over 1.3 million subscribers have activated the feature to block overseas calls and over 270,000 subscribers have activated the feature to block overseas SMSes.

19. 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 (IMDA)

20. 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 170,000 mobile lines.

National Simulated Scams Exercise (Cyber Security Agency of Singapore (CSA))

21. 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 can gain a better understanding of how scams typically work and learn practical steps to protect themselves in a safe environment. The NSSE is being conducted from 1 March to 31 August 2026.

New security features (CPF Board)

22. In the first half of 2026, CPF Board introduced two new security features to provide CPF members with additional ways to safeguard their CPF accounts. The Trusted Contact notification service allows CPF members aged 21 and above to appoint up to two trusted individuals to receive copies of notifications for important transactions, providing an extra pair of eyes to help spot potential scams or unauthorised activities early. The CPF Safety Switch enables members aged 55 and above to immediately secure their CPF accounts if they suspect they have fallen victim to a scam, by disabling access to CPF online services via the CPF website and mobile app,and stopping withdrawals. 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[3].

23. These measures strengthen CPF Board's existing suite of anti-scam safeguards by further supporting members and their trusted contacts in remaining alert to scams and protecting members' CPF savings.

<u>Detect and report scams</u>

ScamShield Suite of anti-scam resources (OGP, National Crime Prevention Council (NCPC), SPF)

24. ScamShield now automatically detects and flags numbers linked to known scam message campaigns, expanding its detection capabilities. Manual scam checks and reports now also cover usernames on online messaging apps, and in collaboration with the SPF, ScamShield's operator dashboard has been improved to better manage reported numbers.

25. The ScamShield app has garnered over 1.61 million downloads, 2.88 million user checks and 1.04 million user reports. The 24/7 ScamShield helpline has received over 310,000 calls since its launch and currently receives around 500 calls daily. Of the calls received, around 84% were enquiries checking if something was a scam, with the helpline operators assisting callers to avert scams. The ScamShield Alert social channels on WhatsApp and Telegram have over 101,000 subscribers, and the ScamShield website has been viewed over 4.7 million times by over 2.6 million users since its launch. The app alerts users to over 1 million scams per year, with 76,000 users checking for scams each month and over 100,000 Android users alerted to at least one scam call or message each month.

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

National Scams List

26. The SPF is stepping up the fight against scams by working with private sector partners to scale up detection and disruption efforts, so that scam operations can be taken down before more victims are harmed. In a recent trial under the NSL initiative, SPF shared scam-linked account numbers and account holder details with selected participating banks. For every scam-linked account shared by the SPF, participating banks were able to identify and disrupt at least 1 additional scam-linked account that was unreported. These are accounts that may otherwise have remained undetected.

Taking Down Scam Infrastructure Across Online Channels

27. The SPF shared scam-linked websites and phone numbers with online platforms such as Meta, leading to the disruption of more than 30,800 scam-tainted accounts and content. In the first half of 2026, the SPF disrupted more than 37,500 WhatsApp lines, over 31,600 online monikers and advertisements, and more than 52,200 scam-related websites. These figures reflect SPF's significantly enhanced capabilities to take down scam infrastructure across online channels. In comparison, the number of mobile lines disrupted stood at more than 47,500, a decrease from the same period last year. This is consistent with the observed trend of scammers shifting their operations away from traditional mobile line-based methods toward online platforms. While telecommunications providers have strengthened their registration measures and enhanced monitoring, the SPF, IMDA and telecommunications companies will continue working closely together to build stronger safeguards and anti-scam measures, preventing the misuse of SIM cards for criminal activities.

Disrupted asset	1H 2025	1H 2026	% change
Mobile lines	> 58,700	> 47,500	> -19%
WhatsApp lines	> 33,300	> 37,500	> 13%
Online monikers and advertisements	> 21,600	> 31,600	> 46%
Websites	> 30,200	>52,200	> 72%

Partnership with Global Signal Exchange (GovTech Singapore)

28. 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, and facilitate tighter industry collaboration. Since joining the GSE, GovTech Singapore has:

- Shared over 180,000 high confidence scam signals through the GSE
- Contributed to the removal of over 80,000 scam enablers, including 30,800 entities and pages associated with fraud and scams from Facebook and Instagram.

Strengthening Trust and Safety Across the Singpass Ecosystem (GovTech Singapore)

29. GovTech Singapore continues to strengthen Singpass' Trust and Safety capabilities to detect threats early, prevent the misuse of digital identities, and preserve trust in the digital ecosystem.

30. This includes using advanced analytics and machine learning to identify suspicious activity, alongside investigations, intelligence-sharing and targeted interventions. Building on the deployment of an advanced machine learning model in 2025, Singpass introduced a second-generation model in 2026. Incorporating new risk signals, the model analyses around three million transactions daily to identify potentially compromised or misused accounts, including those linked to money mule operations and illicit account creation.

31. These capabilities enable Singpass to detect emerging patterns of abuse, intervene earlier, and prevent high-risk accounts from being used to access digital services. They also support broader efforts to protect individuals who may have been deceived or manipulated into surrendering control of their Singpass accounts.

32. Singpass works closely with the Singapore Police Force (SPF) to share relevant intelligence and disrupt scam operations. Intelligence developed through Singpass' analytics contributed to the detection of a job scam syndicate that had misused Singpass accounts, leading to investigations into 20 user accounts and the arrest of five suspects. Under the Facility Restriction Framework, Singpass also works with SPF to restrict access to Singpass and Corppass for high-risk individuals where appropriate. These targeted measures help prevent further misuse of digital credentials and limit the ability of scam syndicates to create or operate accounts for illicit purposes.

33. Together, these measures reflect Singpass' broader Trust and Safety approach: detecting abuse early, protecting users, disrupting malicious actors and preserving trust in Singapore's digital identity ecosystem.

Enforce against scams and recover lost monies

Enhanced penalties for scam-related offences with caning introduced

34. The introduction of caning for scams and scams-related offences took effect on 30 December 2025. Scammers and members or recruiters of scam syndicates will face mandatory caning of at least six strokes and up to 24 strokes. Scam mules who enable scammers 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.

International cooperation for asset recovery

35. Since the formalisation of “FRONTIER+” in October 2024, this initiative has been expanded to 14 jurisdictions, with the United States joining in the first half of 2026. Leveraging this platform, several member jurisdictions have conducted Operation FRONTIER+ III in the first half of 2026, namely Singapore, Malaysia, Hong Kong SAR, Macao SAR, Republic of Korea, Indonesia, Republic of Maldives, Thailand, Brunei and Canada, resulting in more than 7,500 subjects investigated, and 3,000 subjects arrested across all jurisdictions, and approximately S$207 million seized from over 101,000 frozen bank accounts.

Major operations to dismantle scam syndicates

36. The SPF was involved in several major operations in the first half of 2026 to dismantle scam syndicates. Operation Clear Line targeted SIM card abuse islandwide, resulting in 196 subscribers investigated, 86 arrested, and 59 prosecuted — about 50% more prosecutions than in the whole of 2025. Errant retailers were not spared either, with 15 arrested and 12 investigated. Operation Strike Back further disrupted local scam infrastructure across four iterations, freezing 923 mule accounts, seizing S$1.33 million in suspected scam proceeds, terminating 2,912 mobile lines, and disrupting 5,614 online enablers. Singapore also participated in Operation First Light 2026, a global anti-fraud operation coordinated by INTERPOL across 97 countries, where Singapore's efforts contributed to 1,938 arrests, 4,065 bank accounts frozen, and approximately SS$59 million in illicit assets intercepted. These were among the more notable operations in the first half of 2026, with more conducted across the period.

Public Education

Countering scammers' shift towards physical value transfers

37. The SPF works with Ministry of Law, banks, and Precious Stones and Metals Dealers (PSMDs) to sensitise frontline staff, strengthen intervention capabilities, and educate the public, in response to scammers' increasing exploitation of cash, gold, and luxury watches through physical handovers.

Outreach to the elderly

38. The SPF has placed a greater focus on the elderly population segment in 2026, given the increase in elderly scam victimisation and the disproportionate impact of scam types such as government officials impersonation scams and investment scams on elderly. Public education efforts targeted at the elderly have focused on raising awareness on government officials impersonation and investment scams, encouraging the elderly to stop and check whenever they are unsure if something is a scam and promoting the adoption of protective measures such as the ScamShield app, 24/7 ScamShield Helpline (1799), Money Lock and CPF Withdrawal Lock.

39. The SPF has also sought to make anti-scam public education more elderly-friendly and accessible. Public education materials in multiple content formats including jingles, short videos, EDMs and audio clips with bite-sized messages are produced in English and vernacular languages, using larger fonts, clear visuals and simple, action-oriented messages. Elderly are also prominently featured in campaign materials to improve relatability. The materials are also disseminated across a mix of channels preferred by the elderly such as television, radio, newspapers, social media, messaging platforms and out of home displays. The SPF works closely with government agencies such as the Agency for Integrated Care (AIC), the People's Association (PA) and community partners such as the NCPC, Love-Link Services Society and Bamboo Builders to broaden outreach and deliver anti-scam public education through trusted touchpoints frequented by the elderly. These include Active Ageing Centres, ServiceSG Centres, community roadshows, preventive health visits and other community engagement platforms. Through these engagements, the elderly are encouraged to adopt anti-scam protective measures and to check with their loved ones or the 24/7 ScamShield helpline (1799) whenever they are unsure if something is a scam. This whole-of-community approach strengthens awareness, reinforces protective behaviours and enhances upstream scam prevention among the elderly.

Anti-scam roadshows for the public

40. Through the SaferSG roadshows, the SPF brought anti-scam public education directly into the heartlands through in-person engagements with members of public. The roadshows featured experiential elements, interactive games and activities, and

dedicated anti-scam exhibition booths to increase public awareness of scam risks and common scam tactics. Members of the public were also guided on the spot to adopt key protective measures, including downloading the ScamShield app and subscribing to the ScamShield Alert channels to receive the latest information about emerging scam trends. These roadshows also provided opportunities for members of public to engage officers directly, ask questions and reinforce anti-scam knowledge in a practical and accessible manner. SPF will continue to incorporate anti-scam messaging and encourage on-site adoption of protective measures at SaferSG roadshows in the second half of 2026.

Scam advisories

41. Key advisories highlighting emerging and common scam trends were issued across multiple communications channels in the first half of 2026, including digital platforms, mainstream media, out of home displays, community engagements and partner networks. The advisories also reminded members of the public to adopt anti-scam protective measures to enhance their resilience against scams and remain vigilant to evolving scam tactics. They also highlighted the legal consequences and warned potential offenders against selling and sharing bank accounts, Singpass credentials and SIM cards with others, as these are commonly exploited by scammers and syndicates to facilitate criminal activities.

"Stop and Check" Cybersecurity Campaign (CSA)

42. CSA launched the sixth national cybersecurity campaign in September 2025 with the tagline "Stop and Check", to encourage 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". In 2026, CSA also continued to engage members of the public with interactive activities at roadshows and event pop-ups in the Central Business District and heartlands.

43. CSA engaged more than 79,500 students through initiatives under the SG Cyber Safe Students Programme. In 2026, CSA rolled out the fourth edition of the Be Cyber Safe Drama Skit, launched a roving scavenger hunt and conducted a cybersecurity hackathon in schools. CSA will be organising Minecraft bootcamps for students where they can apply their learning in a team hackathon challenge in November. Registration details are available on CSA's website.

44. The SG Cyber Safe Seniors programme reached more than 125,000 seniors since January 2026, through on-ground engagements and partnerships across the public, private and community sectors. These include outreach activities at Active Ageing

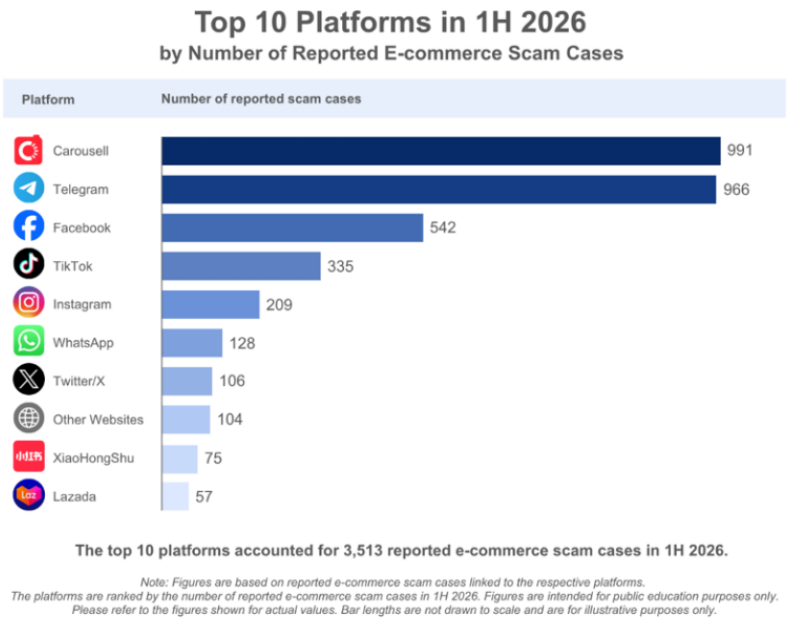
Centres, heartland events, and Be Cyber Safe workshops with community organisations such as Lions Befrienders.

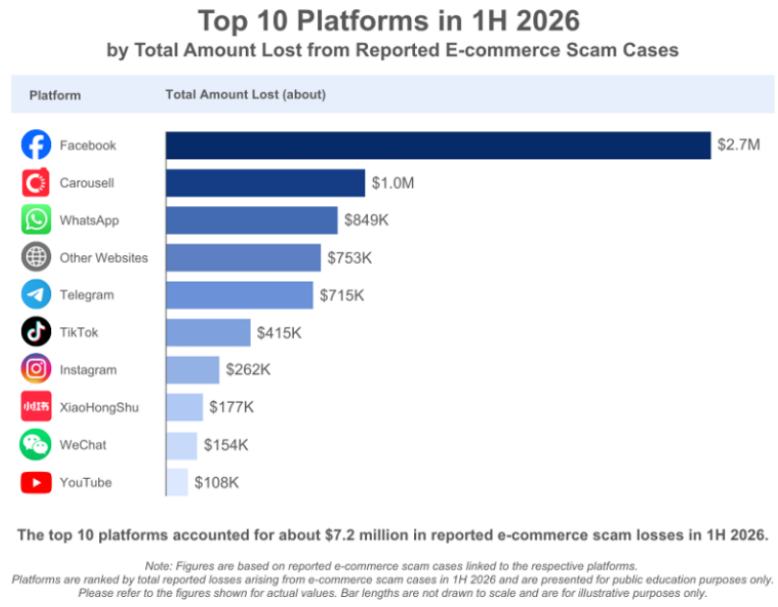
Public education efforts (CPF Board)

45. To raise awareness of its anti-scam safeguards, CPF Board adopts a multi-channel approach for its public education efforts. This includes a multi-phase anti-scam campaign launched in May 2026. Targeted at members aged 50 and above, the campaign aims to help members recognise legitimate CPF communications, stay vigilant against evolving scam tactics, and make use of CPF Board's anti-scam measures. Delivered across digital display panels in community locations, social media platforms and other digital channels, the campaign has been rolled out in English and vernacular languages, to extend its reach among segments that may be more vulnerable to scams.

Annex G

The E-commerce Scam Situation Report





46. Facebook platforms recorded the highest aggregate losses at approximately S$2.7 million and Carousell saw the highest number of cases, with approximately S$1 million lost. WhatsApp and other website platforms also saw relatively high losses despite lower case volumes.

47. To better protect themselves from e-commerce scams, consumers should consider the availability of the following security available when transacting on online

marketplaces. They include: (a) user verification measures that verify users against government-issued records, (b) secure in-platform payment mechanisms that release funds only after delivery is confirmed, and (c) proactive systems that detect and remove suspicious accounts, listings and activities. These measures can provide consumers with greater assurance when transacting online and reduce opportunities for scammers to exploit online marketplaces. Platforms that offer a broader suite of such safeguards generally provide additional layers of protection for users, although the range and extent of safety features vary across platforms.

48. Major e-commerce and social media platforms have progressively introduced measures to strengthen platform safety. For example, Carousell has implemented features such as an escrow-based payment system with trackable delivery, mandatory two-factor authentication for new device logins, and in-platform safeguards that discourage users from moving transactions off-platform. Under the E-Commerce Code, the platform has also piloted enhanced verification measures for higher-risk sellers and strengthened account security controls. Likewise, Facebook (Meta) has introduced various verification measures, including advertiser verification and risk-based verification for selected sellers and pages. These enhancements seek to improve user accountability, raise the cost of fraudulent activity, and reduce opportunities for scammers to operate on online platforms.

49. In parallel, Government agencies and industry partners have strengthened collective efforts to combat scams across the digital ecosystem. Legislative and regulatory measures, including the Online Criminal Harms Act and its accompanying Codes of Practice, require designated online services to implement upstream safeguards to detect, prevent and disrupt scam-related activities. These include requirements relating to user verification, proactive scam detection capabilities, and the timely removal of malicious content and accounts.

50. In addition to upstream measures, platforms are required to remove malicious content and accounts promptly. Enforcement operations have also been scaled-up, resulting in the disruption of tens of thousands of scam-related mobile lines, online accounts and websites in 2025. Together, these platform-level obligations, regulatory requirements and enforcement measures enhanced consumer protection and markedly reduce the pathways scammers can use to reach and exploit potential victims.