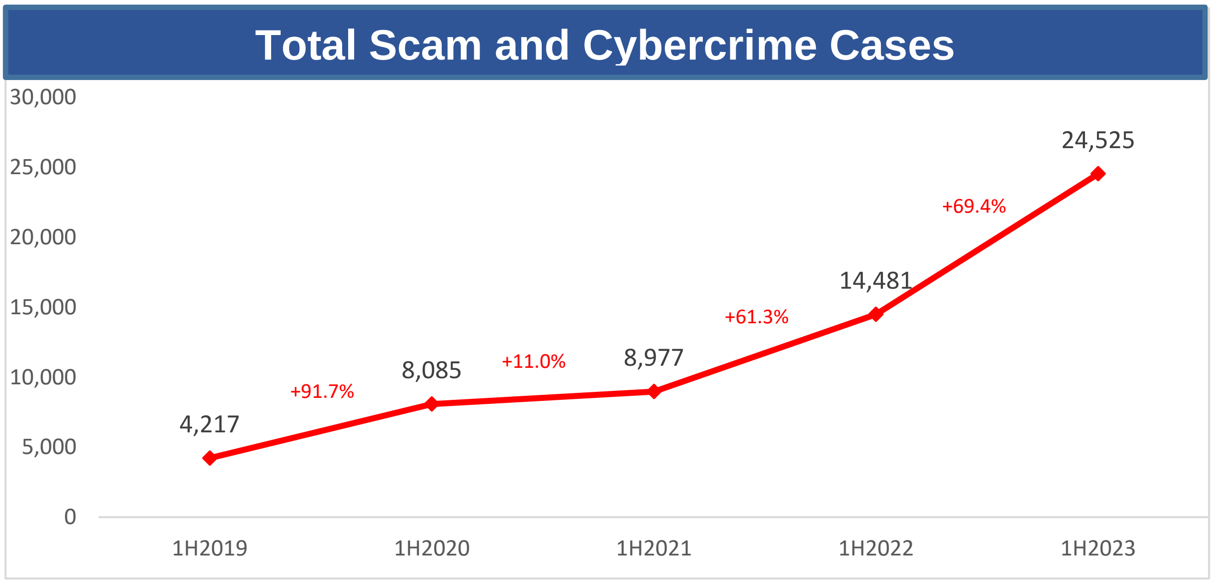
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

POLICE NEWS RELEASE

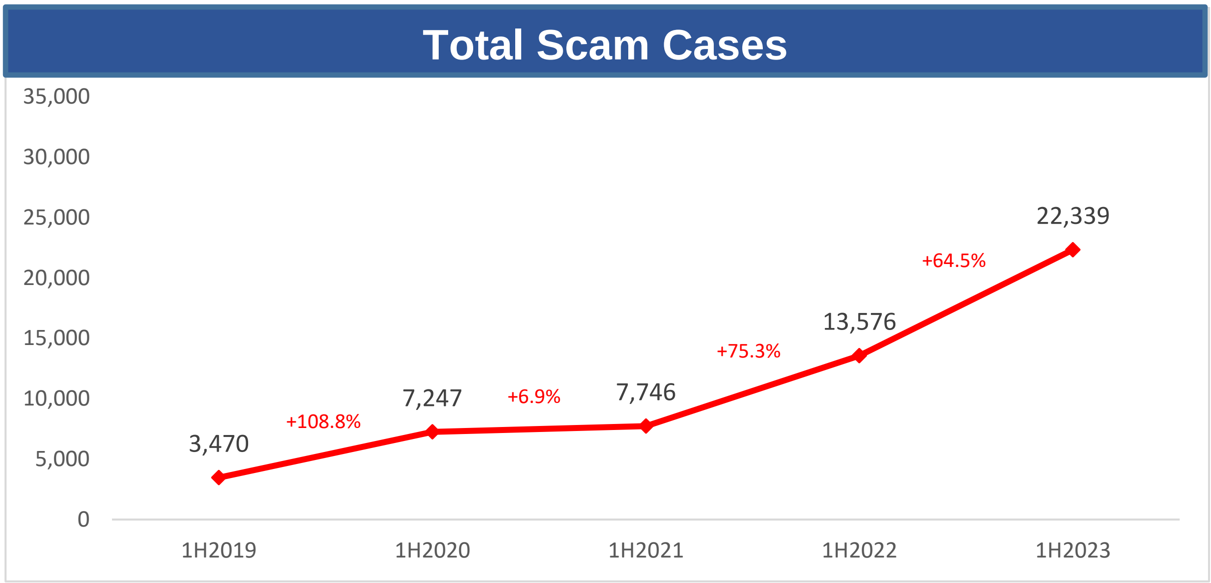
MID-YEAR SCAMS AND CYBERCRIME STATISTICS 2023

Overall Scams and Cybercrime Situation for January to June 2023

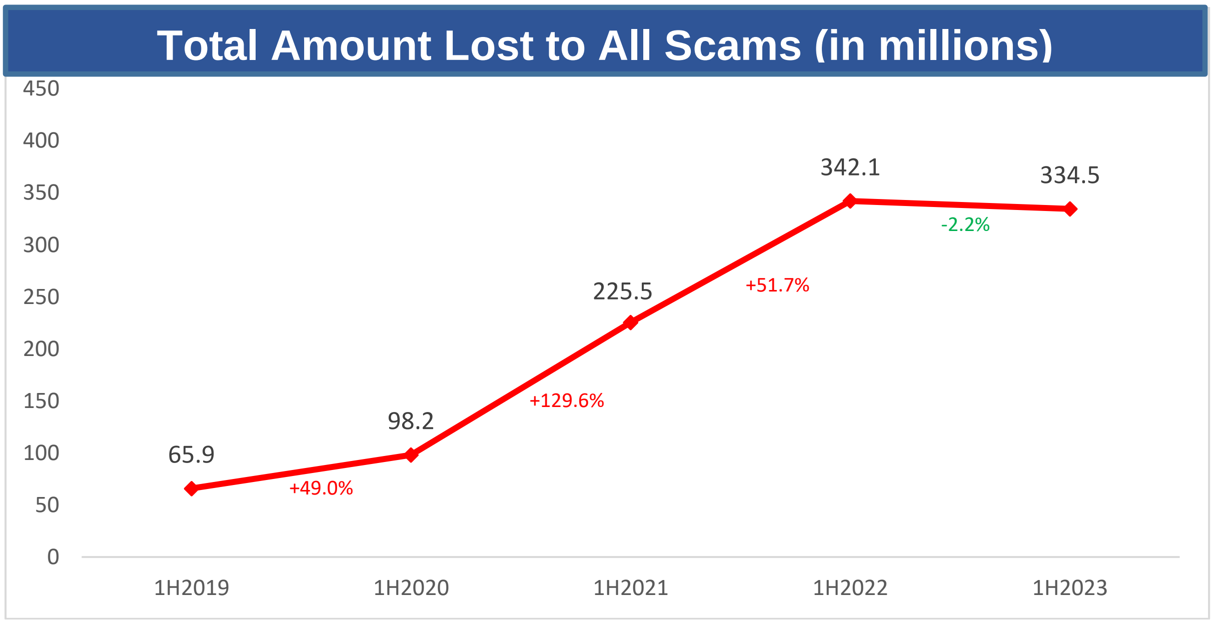
Scams and cybercrime continue to be a key concern. From January to June 2023, the number of scam and cybercrime cases increased by 69.4% to 24,525 cases, compared to 14,481 cases in the same period in 2022.



2. Scams accounted for 91.1% of these 24,525 cases. The total number of scam cases reported increased by 64.5% to 22,339 cases in the first half of 2023, from 13,576 cases in the same period last year.



3. **However, the total amount reported to have been cheated decreased by 2.2% to $334.5 million, from $342.1 million in the same period last year. 55% of the cases have losses less than or equal to $2,000. SPF has been working closely with Government agencies and private sector stakeholders to strengthen scam intervention measures to minimise victims' losses.**



4. Of note, **young adults, aged 20 to 39, made up more than 50% of the total number of scam victims**. The majority of this age group fell prey to job scams, e-commerce scams and phishing scams.

Top Scam and Cybercrime Concerns

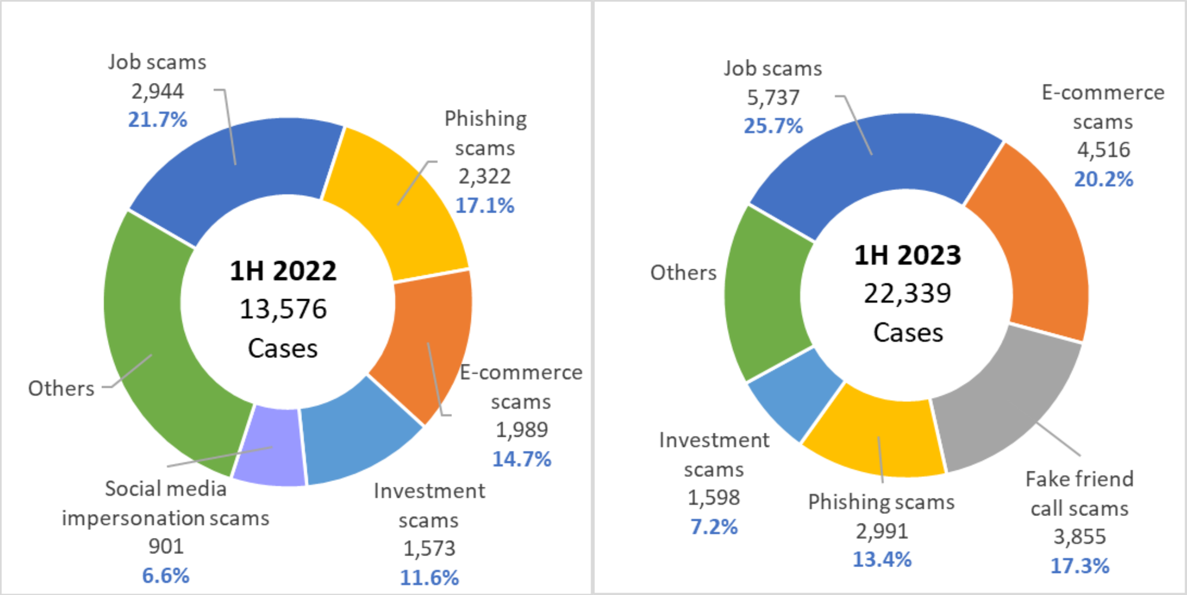
5. **Among the top ten scam types in the first half of 2023, government officials impersonation scams had the highest average losses at about**

$116,000, followed by investment scams at about $60,000. These two scam types involve deception over a period of time, using complex social engineering and deception methods. E-commerce scams and phishing scams had lower average losses, at about $1,600 and $2,400 respectively.

6. **Job scams, e-commerce scams, fake friend call scams, phishing scams and investment scams were the top five scam types in the first half of 2023.** These made up 83.8% of all scam cases reported during that period.

7. Please see **Annex A** for the statistics on the top ten scams.

Breakdown of Scam Types



a) Job scams

i. Job scams recorded the highest number of reported cases amongst all the scam types in the first half of 2023. There were 5,737 cases reported, and the total amount cheated was $79.4 million.

ii. Job scams typically involve victims being offered online jobs that could be performed from home. They would be asked to perform simple tasks such as making advance purchases, liking social media posts, reviewing hotels/restaurants/airlines, completing surveys, ‘boosting’ the value of cryptocurrencies, ‘boosting’ the ratings of product listings for online merchants, or ‘rating’ mobile apps to improve their rankings on app stores. To begin earning commission from these tasks, they may be required to create accounts on fraudulent websites. They would initially be asked to transfer funds to bank accounts provided by the scammers, after which they would receive a small commission. They would then be asked to provide more and more funds, purportedly required for higher earnings. The victims would eventually realise they have been scammed when they fail to receive their commission despite sending huge sums of money, when they are unable to withdraw the monies from their accounts, or when the scammers can no longer be contacted.

iii. The most common platforms which scammers used to contact victims in job scams were WhatsApp and Telegram.

b) E-commerce scams

i. E-commerce scams recorded the second highest number of reported cases amongst all scam types in the first half of 2023. There were 4,516 cases reported and the total amount cheated was $7.3 million.

ii. E-commerce scams involve the sales of goods and services without meet-up. Generally, victims would come across good deals on various online marketplaces or social media platforms, but would fail to receive goods or services after making payments. In some cases, the victims could also be sellers; scammers pretend to be interested buyers, but do not pay them after receiving the goods or services. In such cases, culprits may sometimes provide victims with fake screenshots as “proof” of payment.

iii. The most common platforms where victims encountered e-commerce scammers were Facebook, Carousell, and Telegram. The items commonly involved in the transactions were rental of residential units and electronic goods.

c) Fake friend call scams

i. There were 3,855 fake friend call scams reported in the first half of 2023 and the total amount cheated was $12.6 million.

ii. Fake friend call scams typically involve scammers contacting victims via phone calls, pretending to be the victims’ friend or acquaintance. After establishing contact, the scammers would capitalise on the friendship, and use various reasons to request money from the victims. The victims would end up transferring money to bank accounts belonging to unknown individuals. They would only discover that they had been scammed when they contact their actual friends and realise that their friends had neither contacted them, nor changed their contact number.

iii. Phone calls and WhatsApp were the most common channels used by fake friend call scammers to contact potential victims.

d) Phishing scams

i. There were 2,991 phishing scams reported in the first half of 2023 and the total amount cheated was $7.4 million.

ii. Phishing scams generally involve emails, text messages, calls or advertisements from scammers impersonating officials or trusted entities, to trick victims into revealing details, including their credit card or bank account information. This could be done via voice calls or websites. Thereafter, the scammers would perform unauthorised transactions on the victims' credit card or bank account.

iii. In one of the variants, scammers would impersonate government officials such as the SPF and MOM, and approach victims via calls (mostly WhatsApp voice or video calls). The victims would be convinced by the callers to provide their banking credentials, OTPs and/or personal details. Subsequently, they found unauthorised transactions on their bank account.

iv. In another variant, scammers would act as buyers and claim to be interested in items that victims were selling on Carousell or Facebook. After communicating with the victims via in-app messages and agreeing on the selling price, the scammers would send phishing links or QR codes for the purpose of completing the transaction (i.e., payment of item or scheduling a delivery). The links led the victims to either spoofed bank websites or spoofed delivery company websites where victims were prompted to key in their banking credentials, credit card details and OTPs. They found unauthorised transactions on their bank account/card thereafter.

v. WhatsApp, SMS, Carousell and Facebook were the most common channels used by phishing scammers to contact potential victims.

e) Investment scams

i. There were 1,598 investment scams reported in the first half of 2023 and the total amount cheated was $97.0 million. The number of investment scams reported increased by 1.6% from 1,573 cases reported in the same period last year. The total amount reported to have been cheated decreased by 7.0%, from $104.3 million in the same period last year.

ii. Victims of investment scams usually come across "investment opportunities" through their own internet searches or via recommendations from online friends. They would be enticed by the scammers to invest and asked to transfer money to unknown bank accounts or cryptocurrency wallets for the purposes of their "investments". Victims would generally receive small profits initially and hence be led to believe that the “investments” were genuine, and therefore would be enticed to transfer even more funds. They would also be deceived by the scammers’ use of “investment” websites or apps to display their ‘profits’ and be convinced to invest larger sums. Once larger amounts of money or cryptocurrencies had been transferred to the scammers, the victims would find out that they cannot withdraw their earnings or the scammers would become uncontactable.

iii. Facebook, Instagram and Telegram were the most common platforms used by investment scammers to contact potential victims.

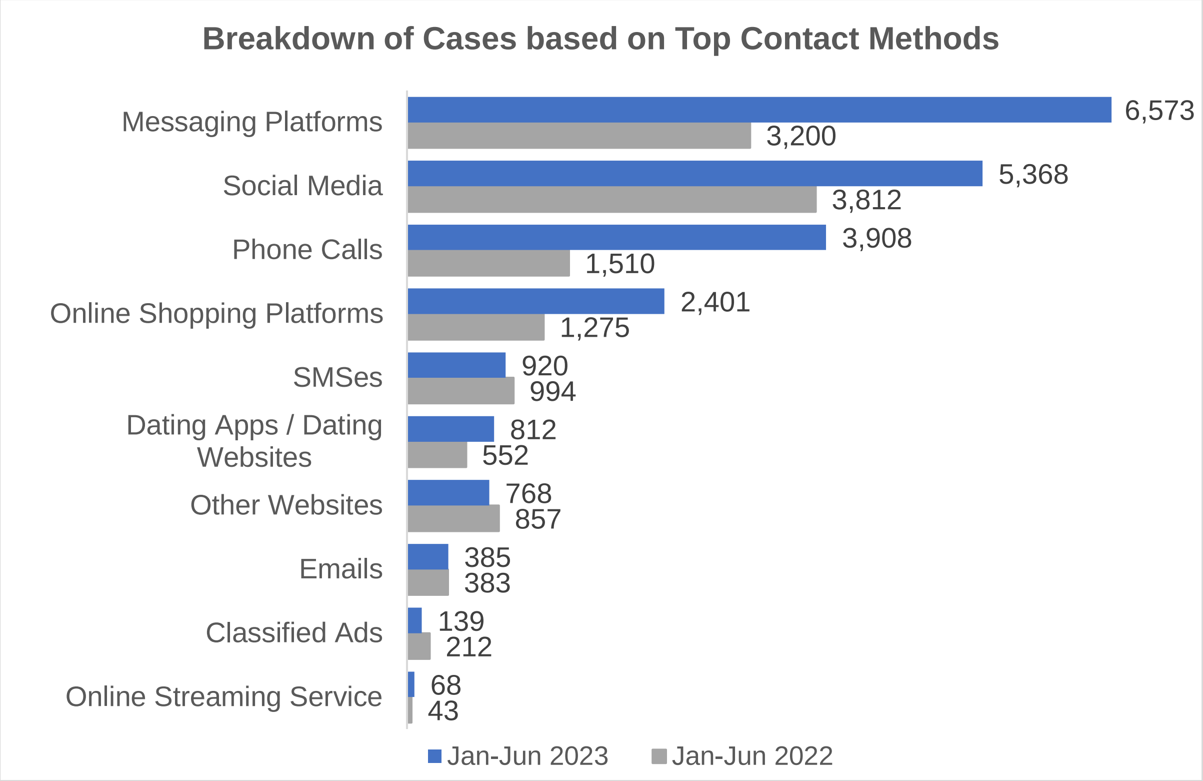
Malware-enabled scams

8. In the first half of 2023, there were more than 750 cases of victims having downloaded malware onto their phones, and the total amount cheated was at least $10 million. 11 of these reports involved unauthorised CPF withdrawals, where at least $218,000 was reported lost.

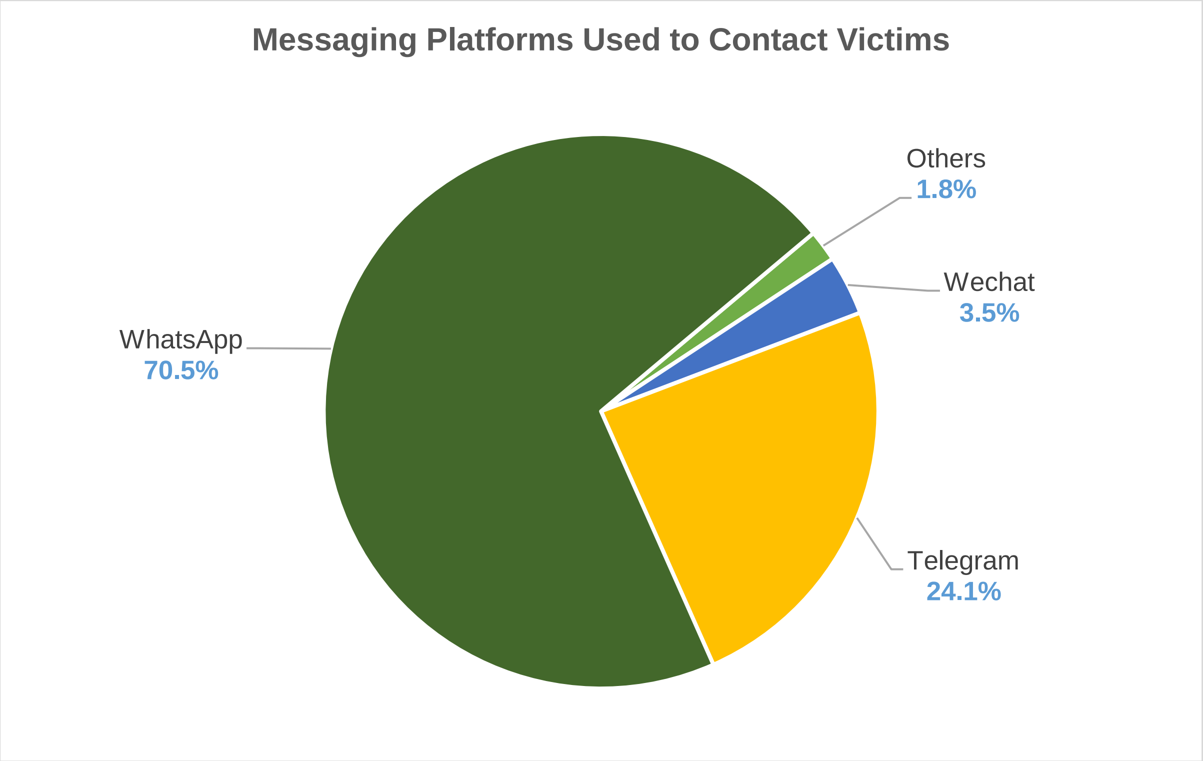
i. Victims generally responded to advertisements for services (e.g., home cleaning, food purchase and pet grooming) on social media platforms such as Facebook and Instagram. Under the pretext of payment for the services, the scammers would send the victims a URL link over WhatsApp, requiring them to download an Android Package Kit (APK) file, an app created for Android’s operating system. After the victims have downloaded the APK file, the scammers would be able to obtain the victims’ internet banking credentials and/or card details. Subsequently, the victims discovered unauthorised transactions on their banking accounts and/or cards.

Top Contact Methods

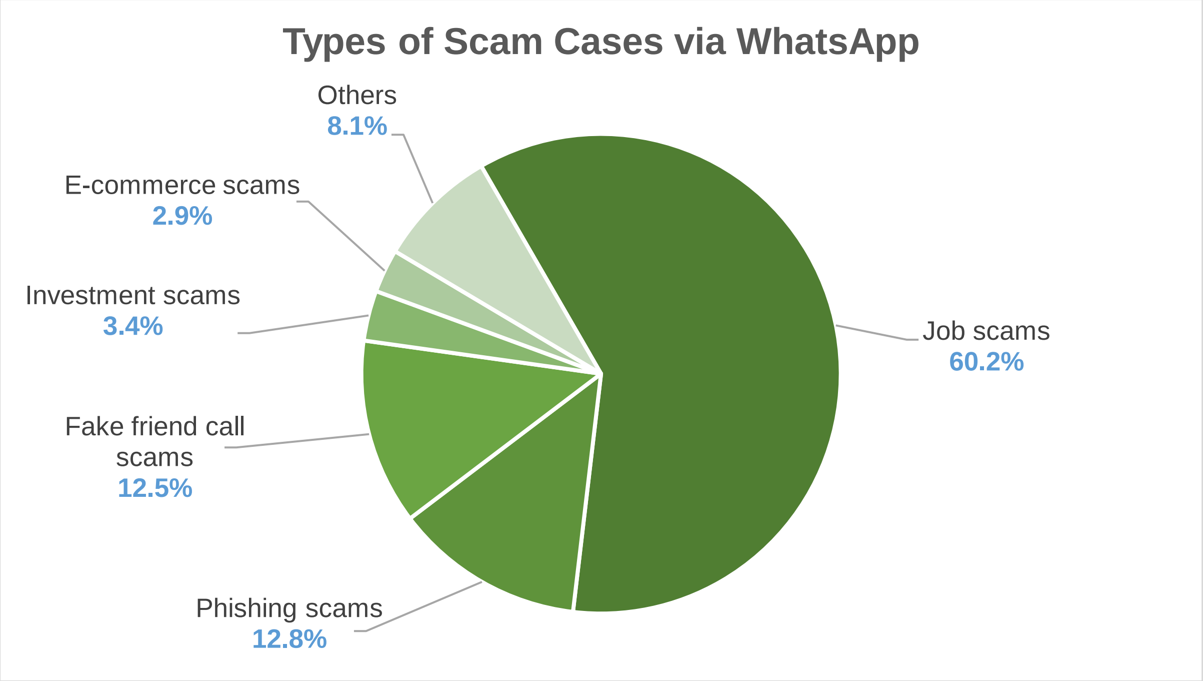
9. Scammers tend to reach out to victims through messaging platforms, social media, phone calls, online shopping platforms and SMSes. These formed the top five approach methods by scammers.



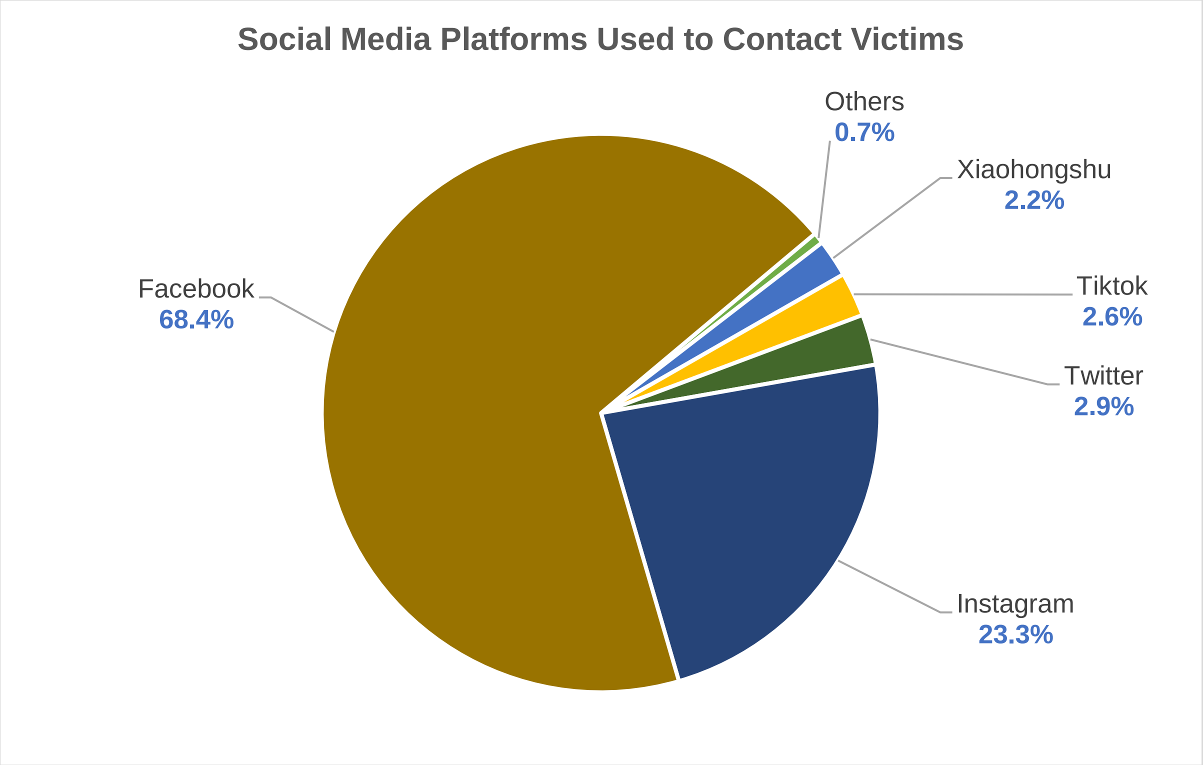
10. In the first half of 2023, 29.4% of scam cases involved contact via messaging platforms compared to 23.6% in the same period last year, with about 70.5% of the cases via WhatsApp, and 24.1% via Telegram.



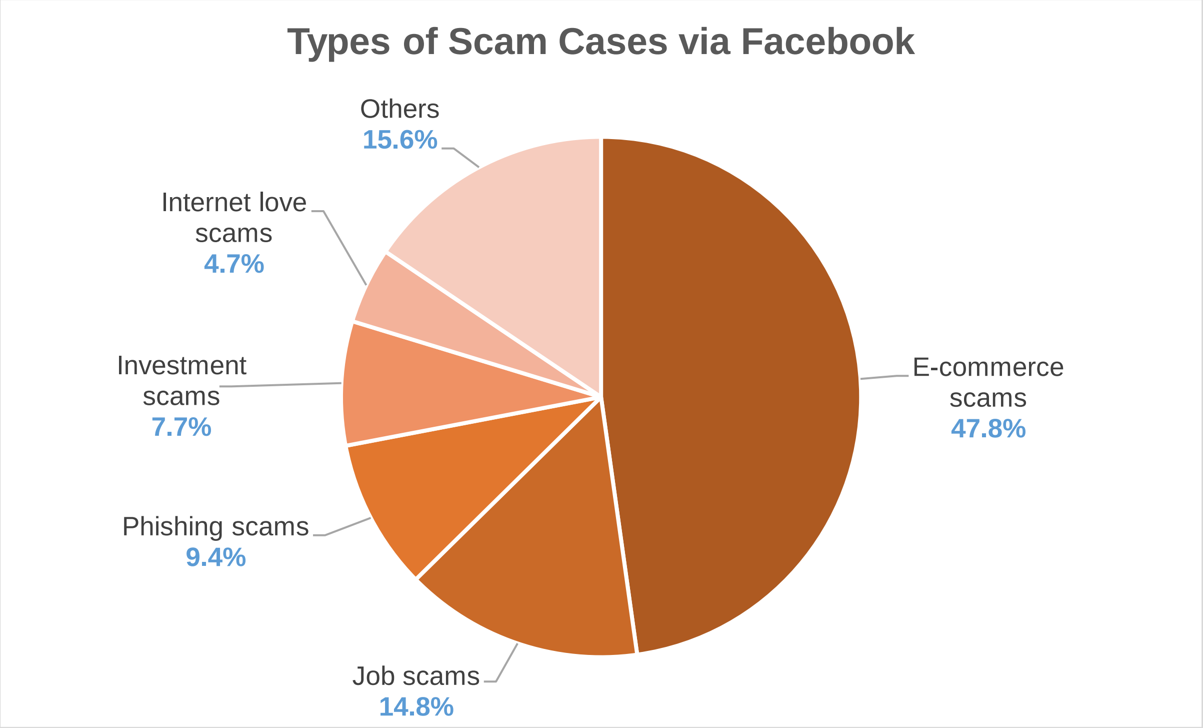
11. Among the scam cases where victims were contacted via WhatsApp, 60.2% were job scams, 12.8% were phishing scams and 12.5% were fake friend call scams.



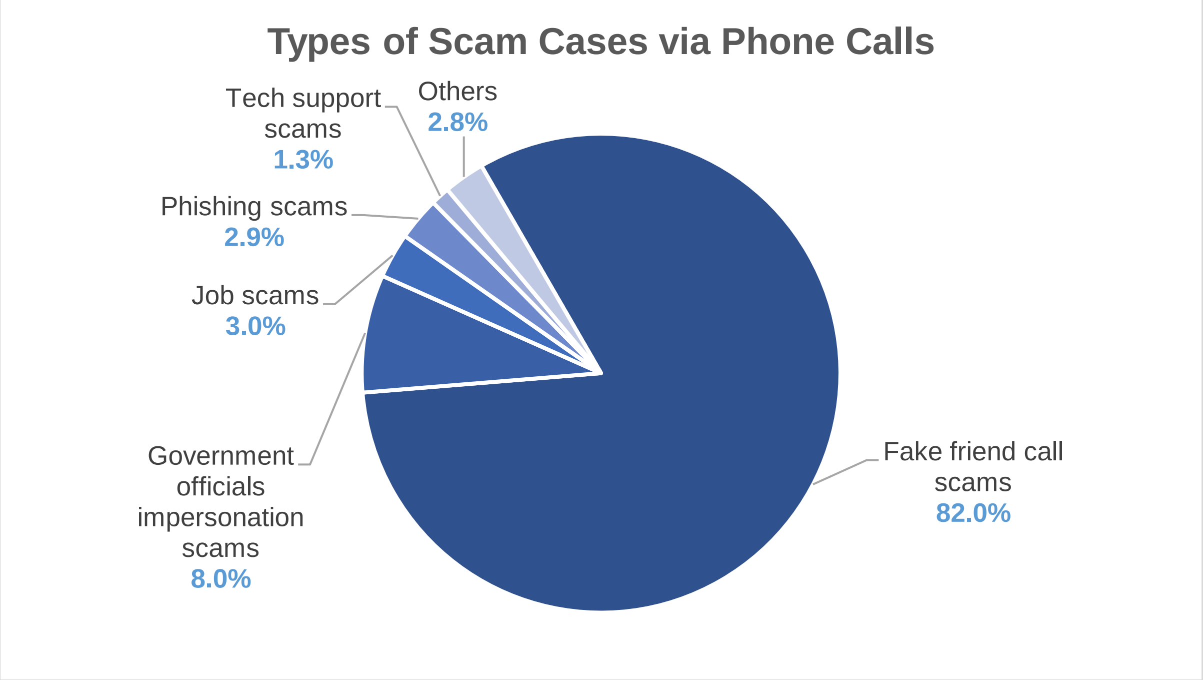
12. In the first half of 2023, 24.0% of scam cases involved contact via social media compared to 28.1% in the same period last year, with about 68.4% on Facebook, and 23.3% on Instagram.



13. Among the scam cases where victims were contacted via Facebook, 47.8% were e-commerce scams, 14.8% were job scams, and 9.4% were phishing scams.



14. In the first half of 2023, 17.5% of scam cases involved contact via phone calls compared to 11.1% in the same period last year. Among the scam cases where victims were contacted via phone calls, 82% were fake friend call scams, 8% were government officials impersonation scams and 3% were job scams.



Scam Victim Profile

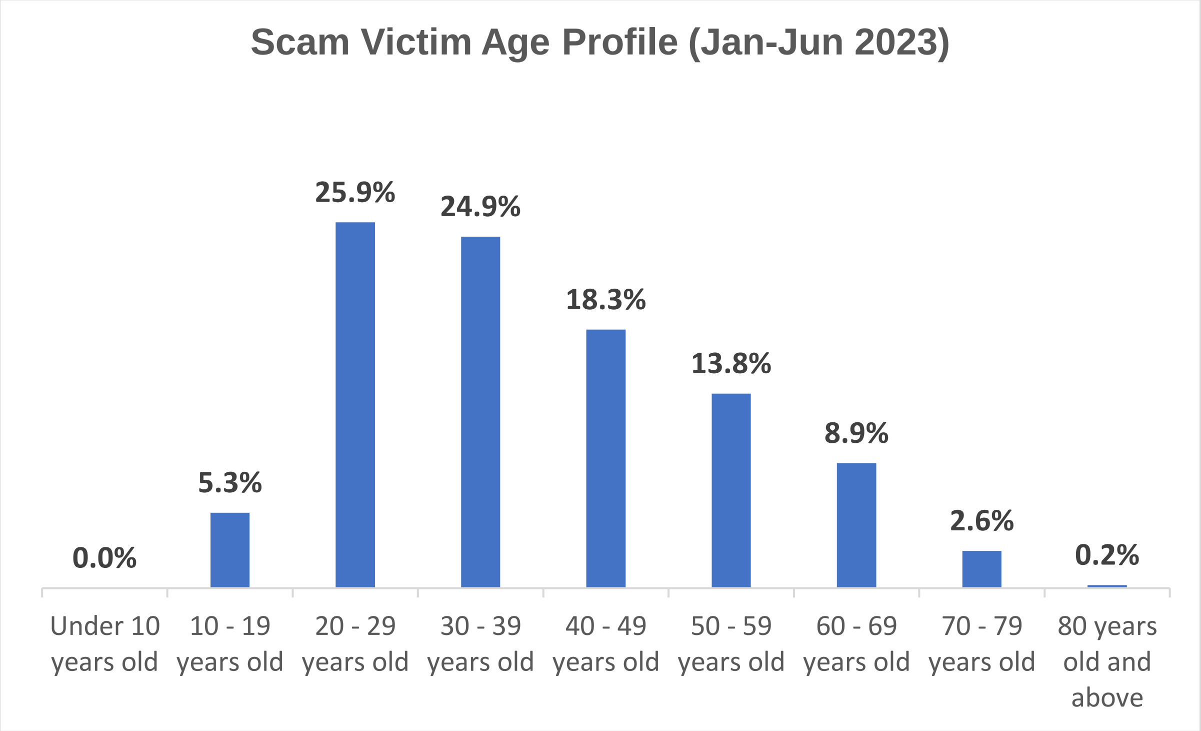
15. Young adults made up more than half of the scam victims in the first half of the year. The breakdown of scam victims by age group is as follow:

a) Youths, aged 10 to 19, made up 5.3% of the total number of scam victims. 30.5% of victims from this age group fell prey to job scams, 28.6% to e-commerce scams and 15.4% to phishing scams. Scammers tend to contact youths via messaging platforms, online shopping platforms and social media.

b) Young adults aged 20 to 39 made up 50.8% of the total number of scam victims. 33.9% of victims from this age group fell prey to job scams, 23.9% to e-commerce scams and 12.6% to phishing scams. Scammers tend to contact young adults via messaging platforms, social media and online shopping platforms.

c) Adults, aged 40 to 59, made up 32.1% of the total number of scam victims. 24.1% of victims from this age group fell prey to fake friend call scams, 19.5% to e-commerce scams and 18.9% to job scams. Scammers tend to contact this victim group via social media, messaging platforms and phone calls.

d) The elderly, aged 60 and above, made up 11.7% of the total number of scam victims. 40.7% of victims from this age group fell prey to fake friend call scams, 12.5% to phishing scams and 10.0% to investment scams. Scammers tend to reach out to the elderly via phone calls, messaging platforms and social media.



Police's Efforts to Fight Scams and Cybercrimes

Enforcement

a) Harnessing strong public-private partnership

16. Since its operationalisation in March 2022, the Anti-Scam Command (ASCom) has expanded its partnerships to more than 90 institutions, comprising local and foreign banks, credit/debit card security groups, fintech companies, cryptocurrency houses and remittance service providers in Singapore, to facilitate the swift freezing of accounts and recovery of funds to reduce victim losses. This is achieved through establishing direct communications channels and close working relationships with these partners. In the first half of 2023, the ASCom froze more than 9,000 bank accounts based on reports referred to the Anti-Scam Centre (ASC) and recovered about $50.8 million.

17. Another milestone was the co-location of staff from six banks and the Government Technology Agency (GovTech) within the ASCom. This enables SPF to leverage Singpass' fraud analytics capabilities to identify and flag unusual activities in Singpass accounts. It also facilitates swifter freezing of bank accounts and faster sharing of information with the banks, which facilitates timely and successful victim interventions. In the first half of 2023, the ASCom worked with the co-located bank staff to identify more than 800 unsuspecting scam victims. Through engagement with the victims, potential losses of more than $5 million were averted.

b) Other law enforcement interventions

18. The ASC also works closely with other stakeholders such as the local telecommunication companies and e-commerce platforms to act against conduits used for scams. In the first half of 2023, more than 3,700 mobile lines and more than 10,300 WhatsApp lines which were believed to be used in scams, were submitted for termination. Additionally, more than 1,500 online monikers and advertisements involved in suspected scams were removed.

19. From March to May 2023, SPF conducted two island-wide operations targeting eight handphone shops and 16 handphone shop owners and assistants. They had allegedly helped scammers exploit registered prepaid SIM cards as an anonymous channel of communications for illicit activities such as unlicensed moneylending, scams, and vice. More than 110 phone subscribers were investigated for their suspected involvement in such fraudulent registration of SIM cards. The two operations also resulted in the termination of more than 1,900 phone lines.

20. SPF also uses analytic tools to identify and block scam websites. In the first half of 2023, SPF blocked over 11,000 scam websites.

21. From January to June 2023, there were 11 malware-enabled scam cases involving unauthorised CPF withdrawals of at least $218,000. The ASCom's swift

action led to the recovery of about $88,000 of the CPF monies, bringing down the net loss to about $130,000.

22. The Police continue to take tough anti-scam enforcement actions against local scammers and money mules. In the first half of 2023, the ASCom, together with the Scam Strike Teams in the seven Police Land Divisions, conducted 12 island wide anti-scam enforcement operations, leading to the investigation of more than 4,700 money mules and scammers.

23. Additionally, the Smart Nation and Digital Government Office (SNDGO) and the Ministry of Home Affairs introduced amendments to the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) and Computer Misuse Act (CMA). The amendments, which will take effect at the end of 2023, will empower SPF to act more effectively against money mules and those who abuse Singpass to perpetrate scams and other crimes.

Engagement

a) ***Proactive and technology-enabled intervention for scam victims***

24. The ASCom focuses on upstream interventions to identify and alert victims, and leverages technology to strengthen its sense-making capabilities. The ASCom works with OCBC, UOB and DBS banks, to automate information-sharing, information-processing and the mass distribution of SMS alerts to scam victims. Many of these victims only realised that they had fallen prey to scams after receiving SMS alerts from the Police advising them to immediately cease any further monetary transfers. Through three joint operations, more than 6,900 SMSes were sent to alert more than 5,700 victims. This proactive victim-centric approach averted over $39 million of potential losses.

International Cooperation and Partnerships

a) Collaboration with foreign law enforcement agencies

25. The vast majority of online scams are perpetrated by scammers based outside Singapore. A common modus operandi by these syndicates is to move the scammed monies between multiple bank accounts, including to overseas bank accounts. Such cases are difficult to investigate and prosecute, and once the scammed funds have been transferred out of Singapore, the chances of recovery are extremely low. The success of our efforts to solve these cases depends on the level of cooperation from overseas law enforcement agencies, as well as their ability to track down the scammers in their jurisdiction. SPF works closely with foreign counterparts and

partners such as the Royal Malaysia Police and INTERPOL, to exchange information and conduct joint investigations and operations against transnational scams.

26. In the first half of 2023, the collaboration between SPF and overseas law enforcement agencies led to the successful take-down of nine scam syndicates comprising four fake friend call scam syndicates, three job scam syndicates, one phishing scam syndicate and one internet love scam syndicate. More than 42 persons based overseas, who were responsible for more than 580 cases in Singapore, were arrested.

27. In March 2023, SPF successfully extradited three individuals from Malaysia and charged them in court for cheating offences. They are believed to be involved in a fake friend call scam syndicate targeting Singaporeans. Preliminary investigations revealed that the syndicate is believed to be involved in more than 40 cases, with total losses of more than $250,000.

28. In June 2023, SPF successfully extradited another three individuals from Malaysia and charged them with money laundering offences. They are believed to be responsible for laundering scam proceeds linked to more than 50 police reports of investment scams, job scams, e-commerce scams, and government official impersonation scams in Singapore, and involving losses amounting to more than $2.9 million. They are believed to have procured Singapore bank accounts through various chat platforms such as Telegram and Facebook, to launder the syndicate's scam proceeds.

b) Partnerships with other countries

29. In June 2023, the SPF partnered the International Security Cooperation Directorate (DCIS) of the French Embassy in Singapore to organise the inaugural Regional Anti-Scam Conference in Singapore. The conference, aimed at building networks and fostering strong regional cooperation through case sharing and identifying best practices in cyber-scams investigations and assets recovery, was attended by more than 500 local and foreign enforcement representatives from police organisations, government agencies, and industry.

30. Since January 2023, the SPF has hosted 14 visits to the ASC from overseas law agencies such as Hong Kong Police Force, UK National Crime Agency, Maldives Police Service, Dubai Police and Korea National Police Agency.

Education

a) Continued public education efforts

31. To educate the public, the SPF engages the community through:

a. Broad-based programmes such as the ‘I Can *ACT* against Scams’ campaign and timely dissemination of communications on the latest/trending scam variants;

b. Partnering with industrial and community partners to roll out tailored programmes and outreach for different groups e.g. youths, elderly, migrant workers, financial service users, digital platform users and community stakeholders; and

c. Engagement events such as Conversation on Safeguarding the Community with Actionable Measures Against Scams (C-SCAMS)

32. The SPF and the National Crime Prevention Council (NCPC) proactively disseminate information and advisories on scams and successful prosecutions. For example, NCPC’s ‘CrimeWatch’ programme features a regular ‘Scam Alert’ segment which highlights scams of concern and provides prevention tips to viewers. NCPC also regularly shares scam prevention tips and advisories with the public through various social media and messaging platforms.

33. SPF has launched an e-Shoppers on Watch interest group under the Cyber category of the Community Watch Scheme (CWS). This interest group harnesses the community to share relevant scam information they come across with SPF and share scam-related advisories from SPF with their loved ones. As of 30 June 2023, there are more than 4,700 CWS members in the e-Shoppers on Watch interest group.

34. In April 2023, SPF collaborated with Gardenia Singapore to launch a two-month anti-scam campaign. During this period, scam awareness messages were prominently displayed on the overbands of Gardenia bread loaves. By participating in the campaign’s anti-scam quizzes, consumers deepened their understanding and awareness about scams. In addition, since December 2022, SPF has collaborated with two major coffeeshop chains, BGain and S-11, to roll out the ‘A Coffee Cup To Fight Scams’ initiative across 30 coffeeshops island-wide. Anti-scam advisories were printed on the cups to remind consumers on how to protect themselves and their loved ones from scams. SPF will continue to work with stakeholders to increase scam awareness and better safeguard our community.

E-commerce Marketplace Transaction Safety Ratings (“TSR”)

35. The E-commerce Marketplace TSR was launched in May 2022 to educate consumers on the extent to which different e-commerce marketplaces have put in place safety features to protect them from scams, and what consumers should look

out for when transacting online (e.g. strong verification measures to ascertain users' identities, secured payment options). [1]

36. In the May 2023 TSR, **Facebook Marketplace continued to be rated the lowest (one tick), as the platform has not implemented the recommended safeguards, such as user verification measures, and has had a significant number of e-commerce scams reported against it** (1,138 cases in 2022, or 23.9% of total number of e-commerce scams). We encourage consumers to transact only with the marketplaces with better ratings to safeguard themselves against e-commerce scams.

Rating	E-Commerce Marketplace
✓ ✓ ✓ ✓	Amazon, Lazada, Qoo10
✓ ✓ ✓	Shopee
✓ ✓	Carousell
✓	Facebook Marketplace

37. The TSR can be found on the Ministry of Home Affairs (MHA)'s website.

WOG Efforts to Fight Scams

ScamShield mobile application by NCPC and GovTech

38. The ScamShield mobile application (app) is jointly developed by the National Crime Prevention Council (NCPC) and Open Government Products (OGP). The app identifies and filters out scam messages and blocks calls from phone numbers that are verified as scam-related. Since the inception of the ScamShield app on iOS and Android, there have been more than 630,000 downloads, more than 7.7 million SMSes have been reported, and over 86,000 phone numbers believed to be used for scam calls have been blocked.

39. With scams increasingly migrating to third party platforms such as WhatsApp, NCPC, together with OGP and SPF, soft-launched the ScamShield Bot on WhatsApp – a chatbot that verifies potential scam communications using crowd-sourced information and makes it easier for users to share scam details with the authorities. This soft launch in July 2023 offered the product to be trialed by members of the public and for the developer to gather user-feedback and monitor the app's utilization. The ScamShield Bot will be made available to the general public by end 2023.

[1] Major e-commerce marketplaces are assessed based on safety features that MHA has identified to be critical in safeguarding consumers against e-commerce scams. These safety features include (a) measures to ascertain user authenticity (e.g. verification of identifies against Government-issued identification), (b) measures to improve transaction safety (e.g. secured payment options), (c) availability of loss remediation channels for consumers, as well as (d) effectiveness of their anti-scam measures. These safety features are based on the anti-scam guidelines in the Technical Reference 76, a set of industry standards for e-retailers published by the Singapore Standards Council. E-commerce marketplaces that adopt all the critical safety features will score a maximum of four ticks.

Anti-scam measures by the SNDGG

40. GovTech, part of the Smart Nation and Digital Government Group (SNDGG), has enhanced Singpass' security measures to protect users against the threat of scams. For example, in response to the recent malware-related scams involving unauthorised withdrawals of CPF monies, GovTech and CPF Board introduced additional authentication measures to increase the protection for CPF members.

41. SNDGG regularly engages citizens through webinars and hybrid sessions via the #SmartNationTogether platform to educate them on the importance of staying vigilant, keeping their Singpass safe and how they can use available tools like ScamShield to help combat scams. SNDGG also reaches out to seniors to help them navigate technology safely, through its Smart Nation Ambassadors' engagement and collaborative efforts with partners like the Infocomm Media Development Authority (IMDA), CSA, SPF, National Library Board and Retired & Senior Volunteer Programme Singapore. The Smart Nation Builder, a roving exhibition with interactive game stations, is deployed at various locations for the public to learn more about various digital government initiatives and how to transact safely online. In addition, a permanent interactive cybersecurity exhibit at the Smart National PlayScape showcase, located at the Science Centre Singapore, aims to educate visitors on the importance of cyber safety against evolving cyber threats.

Anti-scam measures by the Monetary Authority of Singapore

42. In addition to the two rounds of anti-scam measures introduced in 2022, the Association of Banks in Singapore's Standing Committee on Fraud continues to improve the suite of measures to tackle digital banking scams as they evolve. The Monetary Authority of Singapore and banks are according high priority to anti-scam efforts, and are working to progressively introduce additional measures to combat malware-related scams. For instance, OCBC's recent security measure deals with the danger of downloading apps that are not from the official app stores. Such apps may contain malware and can result in confidential data, such as banking credentials, being stolen. While there may be some measure of added inconvenience for customers, these additional anti-malware measures are necessary to protect customers from malware-related scams.

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

43. The SPF and CSA have disseminated key anti-scam messages through multiple platforms, such as outreach events, social media, press releases, and island-wide digital display panels at HDB lift lobbies. SPF and CSA are working with agencies to send targeted messages to vulnerable groups, such as the Ministry of Education for students, Agency for Integrated Care for the elderly, and Ministry of Manpower for migrant workers. More information on cybersecurity and anti-scam tips can be found on SPF and CSA's websites.

44. CSA, SPF and IMDA collaborated on the SG Cyber Safe Seniors Programme, to raise awareness of cybersecurity and encourage adoption of good cyber hygiene practices among seniors. Since July 2021, the programme had reached out to 91,000 seniors, through roadshows, community pop-ups, webinars, and one-to-one sessions at Digital Hubs.

45. On 30 September 2023, CSA, in consultation with the Ministry of Communications and Information, will be launching its fifth national cybersecurity campaign, themed "The Unseen Enemy". The campaign will highlight the "unseen" yet pervasive nature of cyber threats. Through roadshows, corporate partnerships and publicity on social media and out-of-home platforms, the new campaign will encourage the adoption of good cyber hygiene habits, especially CSA's four "Cyber Tips" that members of the public can adopt to stay cyber-secure and scam-safe.

46. The SPF and CSA have also worked with corporate partners such as e-commerce platforms Carousell, Shopee and Qoo10 to amplify public education messages on malware scams, by leveraging their consumer networks and reach of their websites and in-app platforms.

Retention of the "Likely-SCAM" label by the Infocomm Media Development Authority

47. IMDA implemented the full Singapore SMS Sender ID Registry (SSIR) regime on 31 January 2023. Under the full SSIR regime, non-registered SMS Sender-IDs have a "Likely-SCAM" label attached to them, to alert consumers to exercise caution when dealing with them.

48. Currently, there are over 3,600 merchants (who account for ~96% of SMSes with alphanumeric sender IDs) registered with SSIR, up from 198 merchants in October 2022 when the SSIR regime was first announced. The SSIR regime has been successful in reducing the number of SMS scam cases, with a decline of 70% in the three months after implementation of full SSIR (360 cases), compared to the three months before (1,200 cases).

49. The public has reacted positively to this initiative. In a survey on SSIR, 4 in 5 agreed that the "Likely-SCAM" label made them more cautious about whether the SMS is real or fake, and 92% would choose to delete or ignore the SMSes that are labelled "Likely-SCAM".[2]

[2] SSIR Likely-SCAM Online Study conducted by MCI in Jun 2023 with more than 1,000 Singapore residents aged 15 and above to understand public responses to the "Likely-SCAM" label.

50. Moving forward, the “Likely-SCAM” label will be retained as it serves a useful function as a “spam filter and spam bin” that raises consumer alertness and gets them to exercise caution.

51. IMDA would like to urge organisations to register with SSIR, if they have not done so.

Business Operators and the Community Play a Key Role in Fighting Crime

52. Everyone has a part to play in keeping Singapore safe and secure. Business operators, particularly banks, online marketplaces and telcos, have a responsibility to prevent, deter and detect crimes committed through their platforms. Putting in place anti-scam measures and precautions will help keep their customers safe.

PUBLIC AFFAIRS DEPARTMENT
SINGAPORE POLICE FORCE
13 SEPTEMBER 2023 @ 4PM

Annex A

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

Types of Scams	Cases Reported		Total Amount Cheated (at least)		Average Amount Cheated in First Half of 2023
	Jan - Jun 2023	Jan - Jun 2022	Jan - Jun 2023	Jan -Jun 2022	
Job scams	5,737	2,944	$79.4M	$51.6M	$13,851
E-commerce scams	4,516	1,989	$7.3M	$7.5M	$1,635
Fake friend call scams	3,855	633	$12.6M	$3.1M	$3,279
Phishing scams	2,991	2,322	$7.4M	$7.2M	$2,478
Investment scams	1,598	1,573	$97.0M	$104.3M	$60,704
Social media impersonation scams	524	901	$4.6M	$1.9M	$8,791
Internet love scams	446	443	$25.9M	$20.3M	$58,117
Loan scams	427	545	$2.7M	$4.0M	$6,377
Government officials impersonation scams	369	320	$42.8M	$37.9M	$116,048
Credit-for-sex scams	361	314	$1.3M	$930K	$3,754
Top 10 scams	**20,824**	**11,984**	**$281.3M**	**$239.0M**	

Note: Total amount cheated may not tally due to rounding.