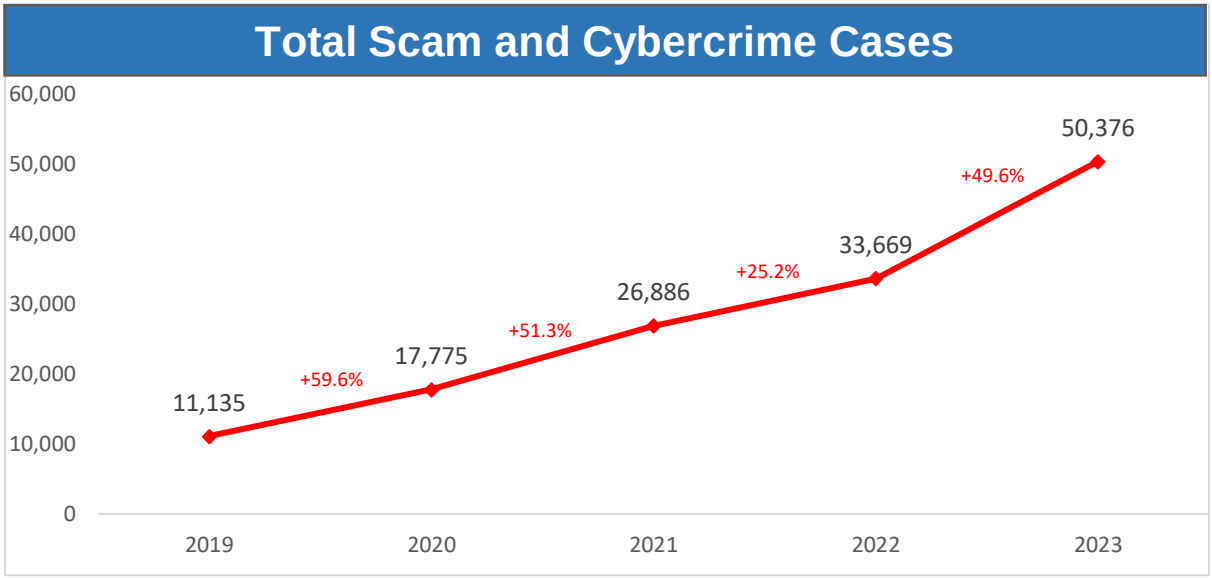
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

Annual Scams and Cybercrime Brief 2023

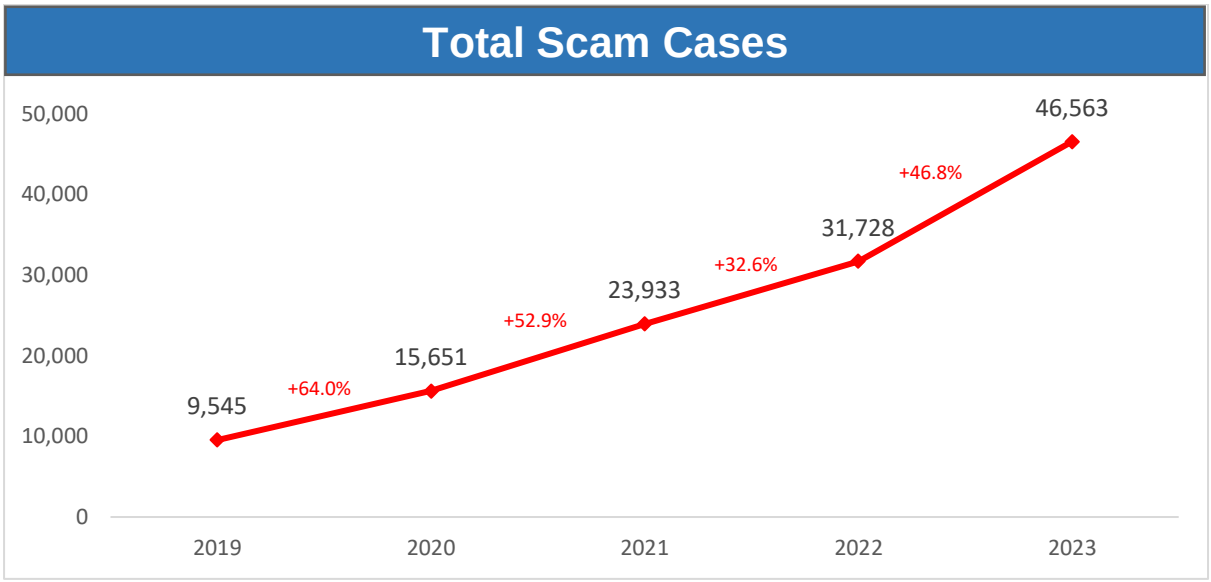
Overall Scams and Cybercrime Situation in 2023

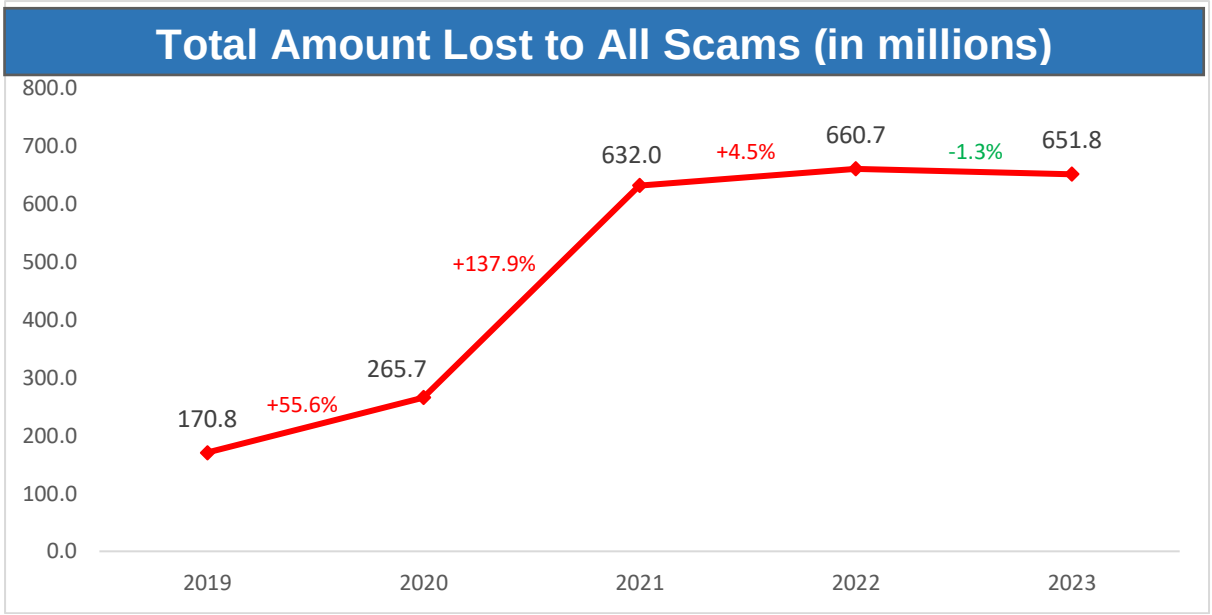
Scams and cybercrime continue to be a key concern. The number of scam and cybercrime cases increased by 49.6% to 50,376 in 2023, compared to 33,669 cases in 2022.



2. Scams, including malware-enabled scams, accounted for 92.4% of these 50,376 cases. The total number of scam cases increased by 46.8% to 46,563 in 2023, from 31,728 cases in 2022.

3. Despite the increase in the number of scams cases, **the total amount lost registered a slight decrease of 1.3% to $651.8 million in 2023, from $660.7 million in 2022.** While this is the first time that the total amount lost to scams had dropped in the last five years, it remains very significant.





4. **The average amount lost to each of the top five scam types, i.e. job scams, e-commerce scams, fake friend call scams, phishing scams, and investment scams, has generally decreased**. Overall, the average amount lost per scam case for all reported scam cases has also decreased, by about 32.8% from $20,824 in 2022 to $13,999 in 2023. 55.6% of scam cases have losses less than or equal to $2,000.

5. The slight improvement in losses may be due in part to the proactive and coordinated efforts by the Singapore Police Force (SPF), the Infocomm Media Development Authority (IMDA), Cyber Security Agency of Singapore (CSA), Smart Nation Group (SNG), Monetary Authority of Singapore (MAS), and private sector stakeholders to prevent scams and stop or mitigate losses during ongoing scams, as well as to raise public awareness on measures that individuals can take to avoid being scammed.

6. However, the amount lost to scams involving the use of social engineering and deception to induce victims to transfer monies to scammers, continues to be high. We

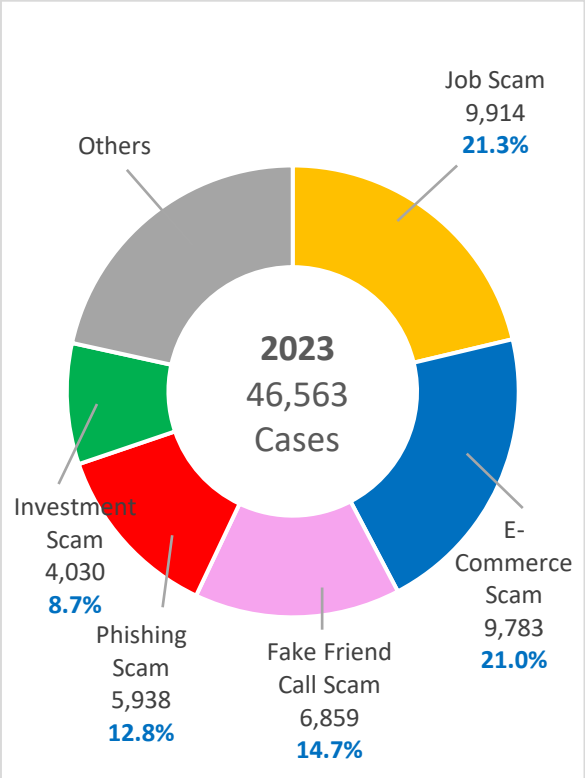
are also concerned about the sharp increase in number of scams that were perpetuated through social media and messaging platforms such as Facebook, Instagram, WhatsApp and Telegram.

7. Individual vigilance remains crucial. By staying informed and exercising caution, every individual can better protect themselves and each other against scams.

Top Scam Concerns

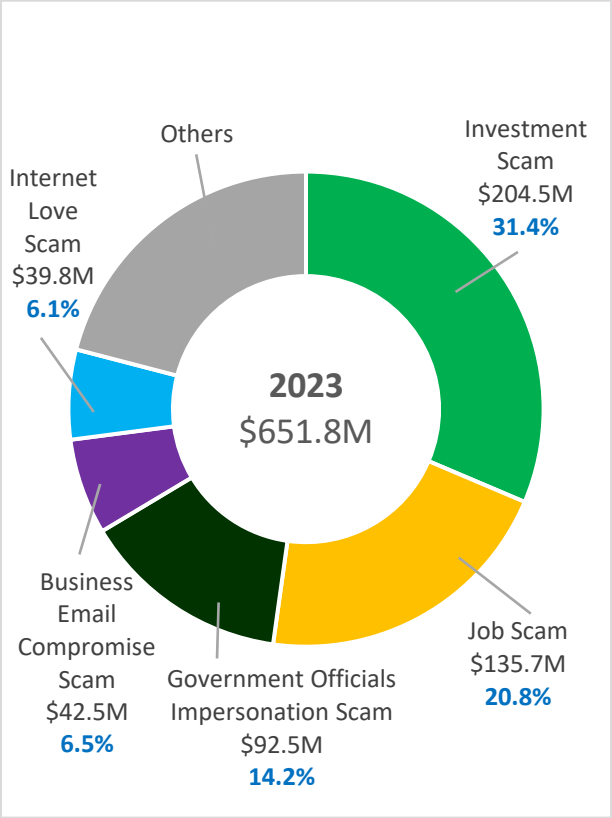
8. **Job scams, e-commerce scams, fake friend call scams, phishing scams, and investment scams** were the top five scam types in 2023. These made up 85.5% of the top ten scam types reported in 2023, and about 78.4% of all scam types.

Breakdown of scam types by number of cases



9. Among the top ten scam types in 2023 (see **Annex A**), **government officials impersonation scams had the highest average losses at about $103,600 per case, followed by investment scams at about $50,700 per case**. These two scam types involve deception and social engineering conducted over a period of time, using an array of complex scam methods.

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



a) Job scams

i. Job scams recorded the highest number of reported cases amongst all the scam types in 2023. There were 9,914 cases reported in 2023, compared to 6,492 cases in 2022, an increase of 52.7%. The total amount lost from job scams increased by 15.6% to at least $135.7 million in 2023, from at least $117.4 million in 2022. The average amount lost per job scam case decreased by 24.3% to $13,692 in 2023, from $18,089 in 2022.

ii. Job scams typically involve victims being offered online jobs that could be performed from home. They would be asked to perform tasks for a commission, such as making advance purchases, liking social media posts, reviewing hotels/restaurants/airlines, completing surveys, "boosting" value of cryptocurrencies, "boosting" ratings of product listings for online merchants, or "rating" mobile apps to improve their rankings on app stores. Another "job" offered to victims entails transfer of funds to bank accounts provided by the scammers, for a small commission. The scammers would subsequently request higher amount of funds to be transferred, for purportedly higher earnings. The victims would eventually realise that they had been scammed when they failed to receive their commission, when they were unable to withdraw the monies from the bank accounts, or when the scammers could no longer be contacted.

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

iv. The majority of job scam victims were aged 30 to 49, making up 45.4% of victims for this scam type. The most common platforms which scammers used to contact job scam victims were WhatsApp and Telegram.

b) <u>E-commerce scams</u>

i. E-commerce scams recorded the second highest number of reported cases amongst all scam types for 2023. There were 9,783 cases reported in 2023, compared to 4,762 cases in 2022, an increase of 105.4%. The total amount lost from e-commerce scams decreased by 34.7% to at least $13.9 million in 2023, from at least $21.3 million in 2022. The average amount lost per e-commerce scam case decreased by 68.2% to $1,428 in 2023, from $4,491 in 2022.

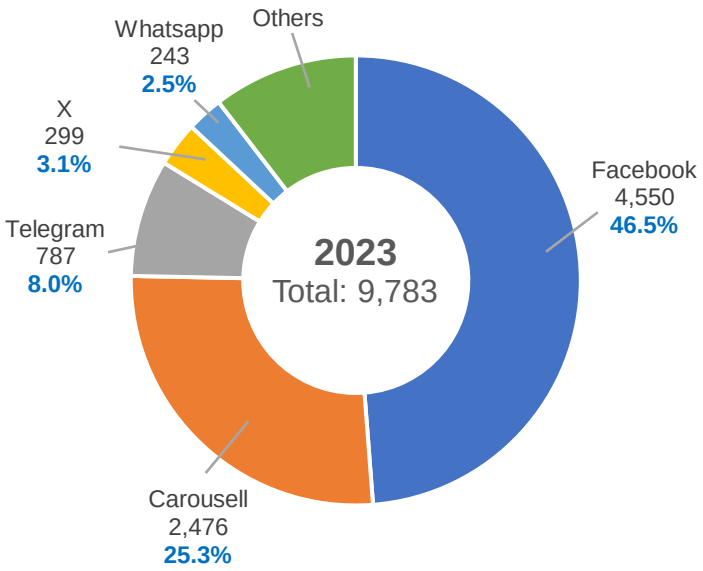
ii. E-commerce scams involve the sales of goods and services without physical meet-ups. Generally, victims would come across attractive deals on online marketplaces or social media platforms but would fail to receive the goods or services after making payment. In some cases, the victims were sellers 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".

iii. A new variant of e-commerce scams which emerged in 2023 involved freecycling, where victims came across posts offering free giveaways or the sale of items at discounted prices on social media platforms. Victims suffered financial losses when scammers requested goodwill deposits, reservation fees, or payment for delivery.

iv. The items commonly featured in e-commerce scam cases were rental of residences, electronic goods, and concert tickets.

v. The majority of e-commerce scam victims were aged 30 to 49, making up 49.3% of victims for this scam type. The most common platforms on which e-commerce scams were conducted included Facebook, Carousell and Telegram. The breakdown of e-commerce scams on the various platforms are as follows:

Top five digital platforms used in e-commerce scams in 2023



c) Fake friend call scams

i. There were 6,859 fake friend call scam cases in 2023, compared to 2,106 cases in 2022, an increase of 225.7%. The total amount lost from fake friend call scams increased by 162.5% to at least $23.1 million in 2023, from at least $8.8 million in 2022. The average amount lost per fake friend call scam decreased by 19.7% to $3,373 in 2023, from $4,201 in 2022.

ii. Fake friend call scams typically involve scammers contacting victims via phone calls or WhatsApp, pretending to be their acquaintance. During the conversation, the scammers would claim that they had lost their mobile phone and changed phone number. After establishing rapport, the scammers would capitalise on the perceived friendship and seek money from the victims for various reasons. The common reasons offered by scammers for these “loans” were to pay contractors for renovation fees, pay for costs relating to the opening of new businesses, or pay vendors/suppliers. The victims would transfer money via PayNow to bank accounts belonging to unknown persons. They would discover that they had been scammed when they contacted their actual acquaintance and realised that they had neither changed their contact number nor contacted them.

iii. The majority of fake friend call scam victims were aged 50 to 64, making up 37.5% of victims for this scam type. 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 5,938 phishing scam cases reported in 2023, compared to 7,097 cases in 2022, a decrease of 16.3%. The total amount lost from phishing scams also decreased, by 13.9% to at least $14.2 million in 2023, from at least $16.5 million in 2022. The average amount lost per phishing scam case increased slightly by 2.4% to $2,394 in 2023, from $2,338 in 2022.

ii. Phishing scams involve emails, messages, calls, or advertisements by scammers posing as government officials, financial institutions or businesses. Victims would be tricked into revealing sensitive information such as usernames, passwords, banking credentials and/or debit or credit card information by 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.

iii. Some phishing scam variants include the following actions by scammers:

- Posing as interested buyers through marketplace platforms – Scammers would pose as potential buyers and approach victims by expressing interest in items listed for sale on online marketplace platforms such as Carousell. Victims would receive malicious URL links or QR codes via email or in-app messaging under the pretext of receiving payment for items or to pay for courier services to facilitate the delivery of the items. Upon clicking on the malicious links, victims were led to spoofed bank or delivery company websites where victims were prompted to key in their banking credentials, debit/credit card details and One-Time-Passwords (OTPs).

- Impersonation of government officials through calls – Victims would receive unsolicited phone or in-app calls allegedly from government officials such as the SPF and the Ministry of Manpower (MOM). Scammers would claim that there were issues with victims' bank accounts and required further verification. Victims would then be convinced to disclose their banking credentials, debit/credit card details, OTPs and/or personal details.

- Impersonation of banks through spoofed SMSes – Victims would receive unsolicited SMSes from both overseas and local numbers, or short codes impersonating banks. The spoofed SMSes "warned" victims of possible unauthorised transactions in their bank or credit card accounts, and instructed them to click on embedded links for verification or to stop the transactions. Victims were then directed to spoofed banking websites after clicking on the embedded links and

were misled into providing their banking credentials, debit/credit card details or OTPs that allowed scammers to perform unauthorised transactions.

In these variants, victims would discover that they had been scammed when they found unauthorised transactions made from their bank accounts or debit/credit cards.

iv. The majority of phishing scam victims were aged 30 to 49, making up 47.8% of victims for this scam type. Carousell, SMSes and Facebook were the most common channels used by phishing scammers to contact potential victims.

e) Investment scams

i. There were 4,030 investment scam cases reported in 2023, compared to 3,108 cases in 2022, an increase of 29.7%. The total amount lost to investment scams increased by 3.1% to at least $204.5 million in 2023, from at least $198.3 million in 2022. Among the top ten scam types, investment scam recorded the highest amount lost, even though the average amount lost per investment scam case had decreased by 20.5% to $50,754 in 2023 from $63,834 in 2022.

ii. Victims of investment scams usually came across “investment opportunities” through their own internet searches or via recommendations from online friends. Once they were duped or had been enticed by the false testimonies, they transferred funds to specified bank accounts or cryptocurrency wallets or made payments via their bank cards for their “investments”. In some cases, the victims would receive initial small “profits” which led them to believe that their “investments” were genuine, enticing them to invest more money by transferring larger amounts of monies or cryptocurrencies to the scammers. The victims might also be deceived by the scammers’ use of “investment” websites or apps to display their “profits” and be convinced to invest more monies. After larger amounts of monies or cryptocurrencies were transferred to the scammers for their “investment”, they would experience difficulties withdrawing their earnings from their “investments” and only then realise that they had been scammed.

iii. There has been an upward trend in cases featuring victims who were added into chatgroups or channels via messaging platforms such as WhatsApp and Telegram, purportedly for “investment opportunities”. In these chatgroups or channels, the victims were presented with multiple claims from other members who had “profited” from their investments, convincing the victims of the authenticity of the investments. Tempted by the promised returns, the victims would contact the scammers. They would then share personal information with the scammers to “set up accounts” and transfer funds for “investment”. Before receiving the earnings from their “investments”, the victims were instructed by the scammers to transfer monies for various “fees” incurred for the

"investment". The victims would realise that they had been scammed when they were unable to withdraw their "profits" despite paying the incurred "fees" for the "investments".

iv. The majority of investment scam victims were aged 30 to 49, making up 45.1% of victims for this scam type. Facebook, Telegram and Instagram were the most common platforms used by investment scammers to contact potential victims.

Malware-enabled scams

10. In 2023, there were about 1,899 cases of victims having downloaded malware onto their phones, and the total amount lost was at least $34.1 million. The average amount lost per malware-enabled scam case was about $17,960.

i. The 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 victims a file or URL link over WhatsApp, requiring them to download an Android Package Kit (APK) file, an app created for the Android operating system. These APK files contained malware which targeted the victims' devices. After the victims downloaded the APK file, the scammers might instruct the victims to make payment by providing their banking credentials and/or card details in spoofed websites which resembled banks' login sites. The malware might also grant scammers remote access to the victims' devices. This would allow scammers to obtain the victims' banking credentials and/or card details by keylogging or monitoring the victims' usage of their devices. Subsequently, the victims would realise that they had been scammed when they discovered unauthorised transactions on their bank accounts or debit/credit cards.

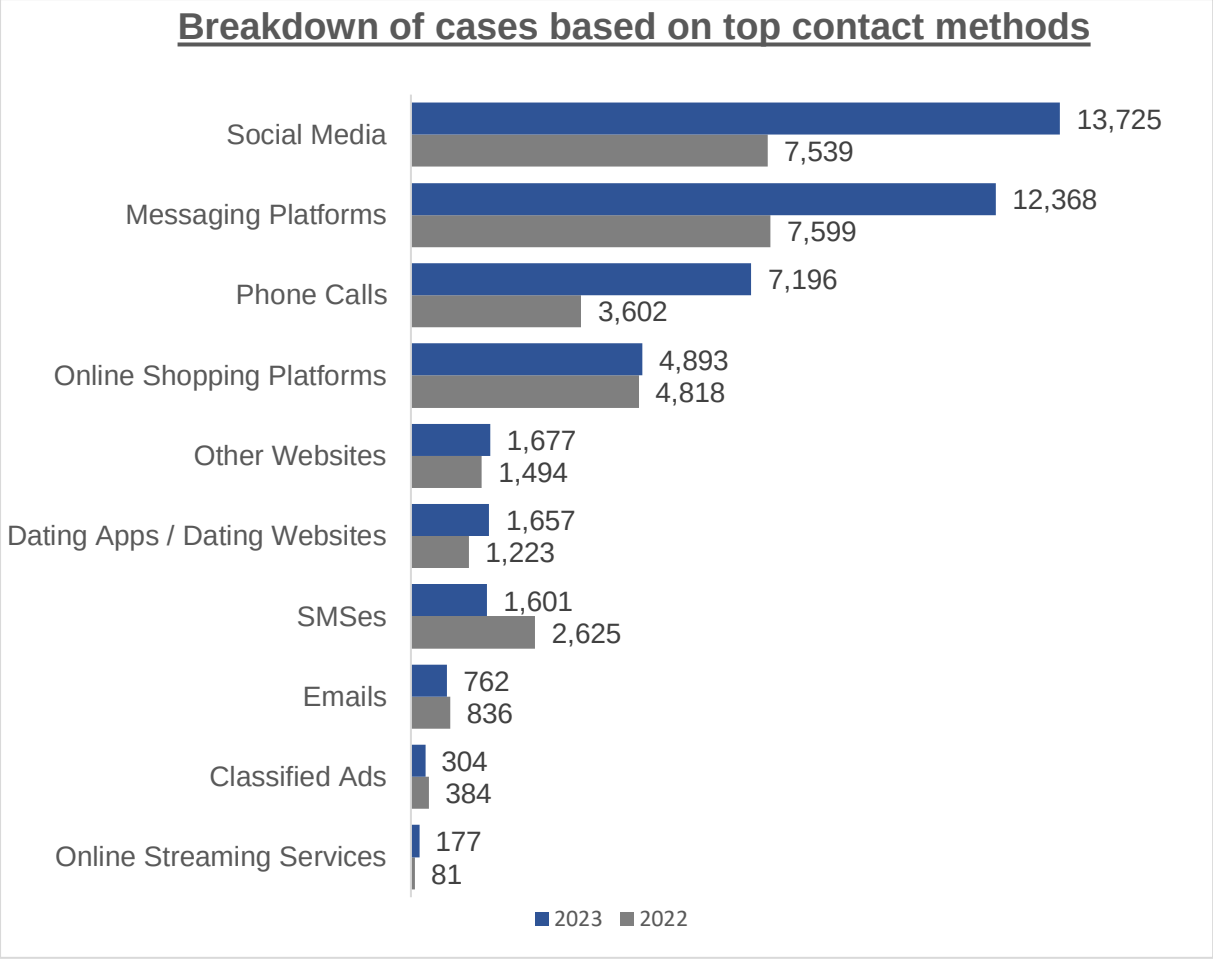
ii. The majority of malware-enabled scam victims were aged 30 to 49, making up 43.7% of victims for this scam type. Facebook and Instagram were the most common platforms used by scammers to contact potential victims.

iii. In response to the malware-enabled scam attacks, the Government launched a series of measures to protect Singaporeans, which led to a decline in cases towards the end of 2023. The Whole-of-Government (WOG) anti-malware-enabled scam measures include enhanced measures to safeguard Central Provident Fund (CPF) monies (more details in Para 55), publication of the Safe App Standard (more details in Para 60) and working with the banks to roll out counter malware-enabled scams measures (more details in Para 57).

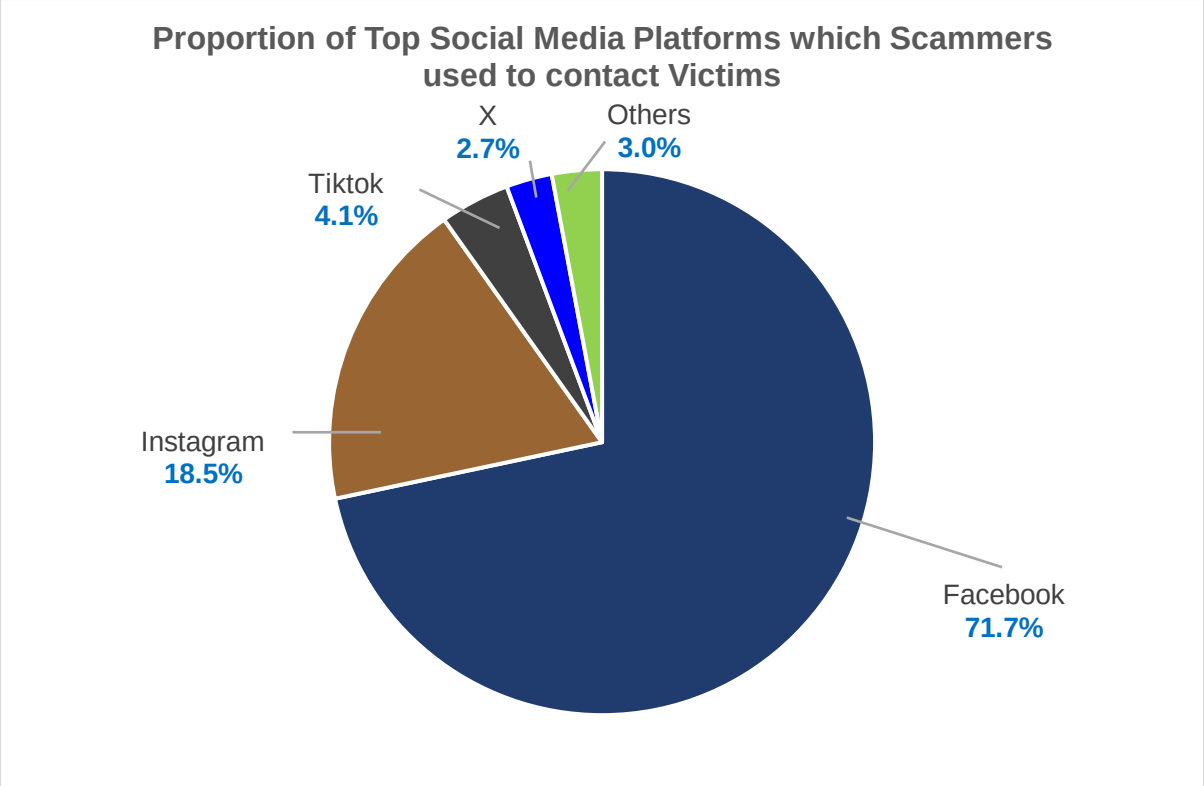
Top Contact Methods

11. Scammers tend to reach out to victims through social media, messaging platforms, phone calls, online shopping platforms and other websites. These formed the top five contact methods.

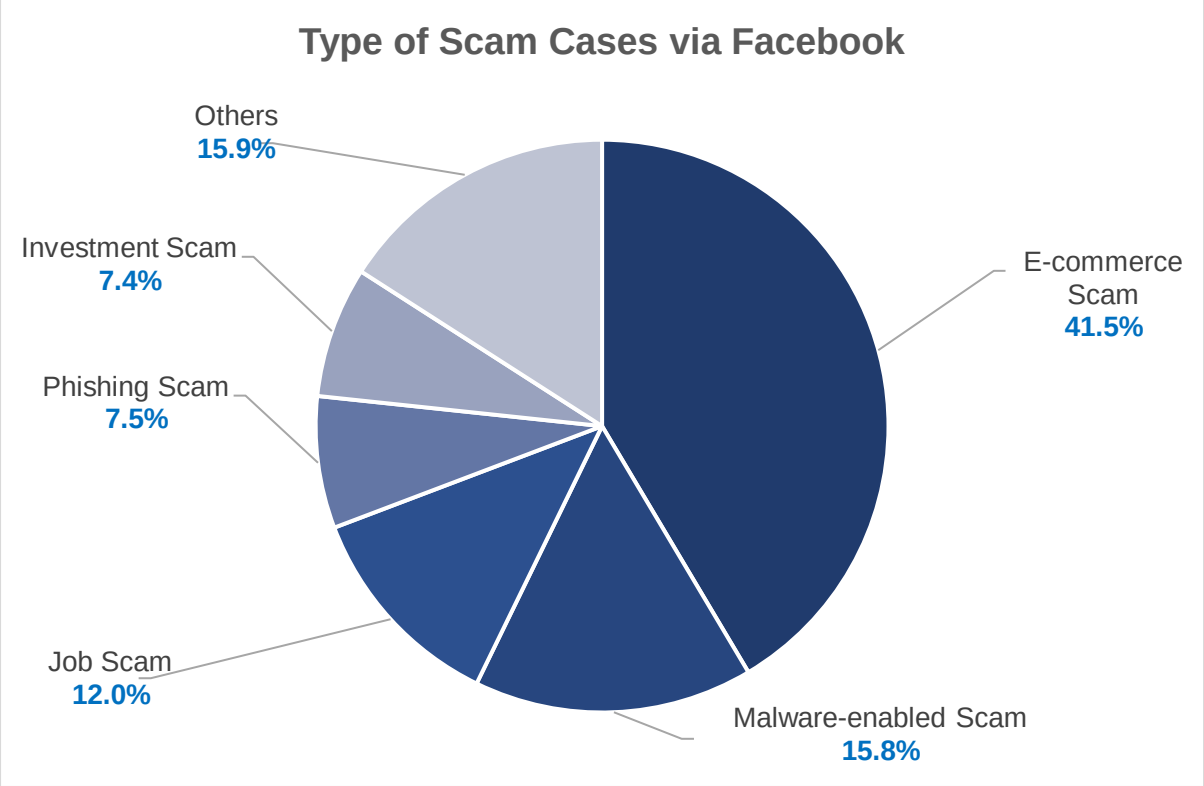
12. **Three products from Meta – Facebook, WhatsApp and Instagram – are of particular concern and continue to be over-represented amongst the platforms exploited by scammers to contact potential victims and conduct their scams.** For case studies on the top five scams perpetrated on Meta platforms, please refer to **Annex B**.



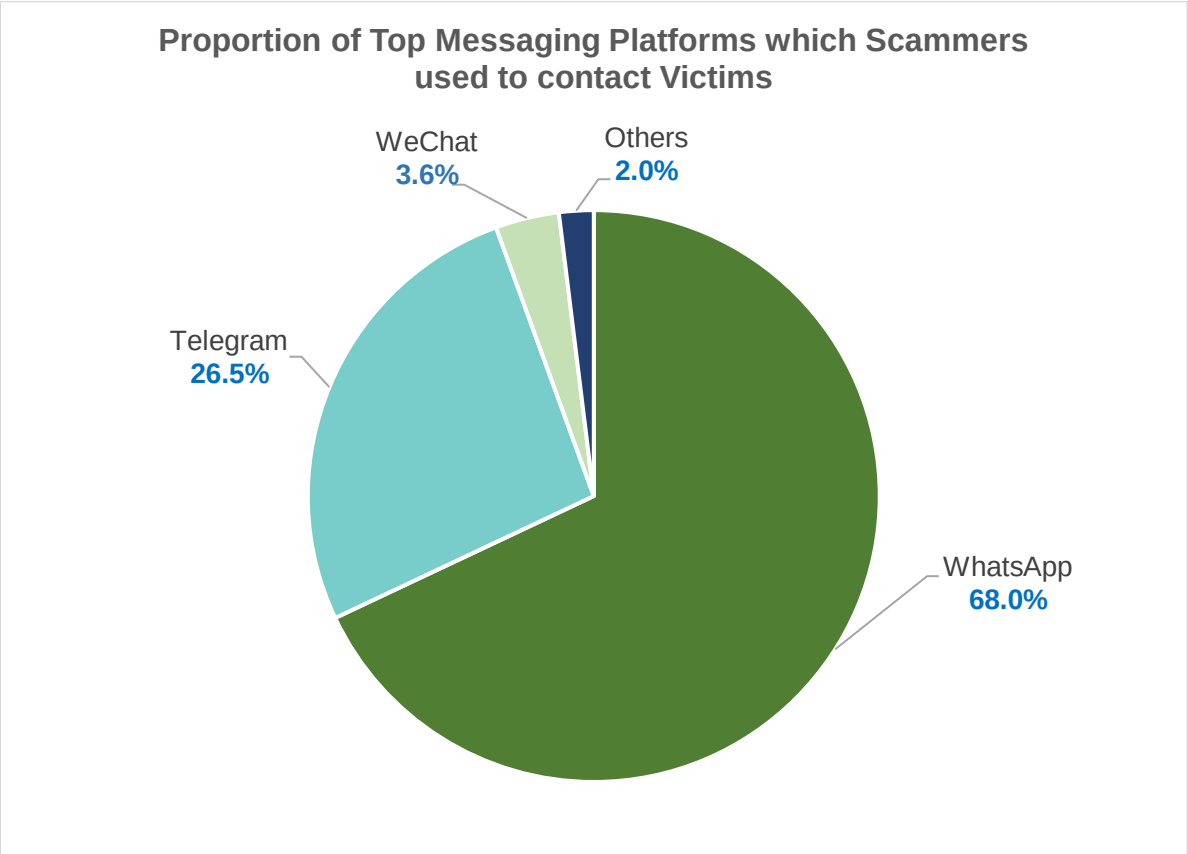
13. In 2023, the number of scam cases where scammers contacted victims via social media increased to 13,725 from 7,539 in 2022, with about 71.7% on Facebook, and 18.5% on Instagram.



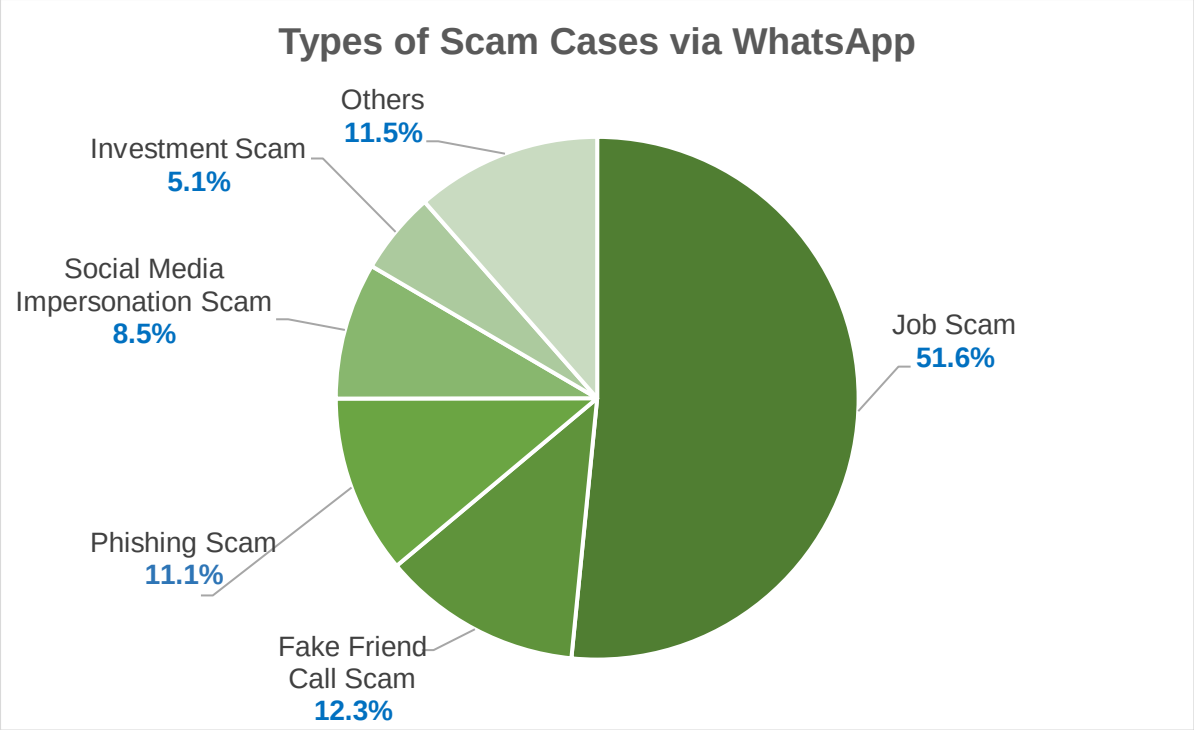
14. Among the scam cases where scammers contacted victims via Facebook, 41.5% were e-commerce scams, 15.8% were malware-enabled scams and 12.0% were job scams.



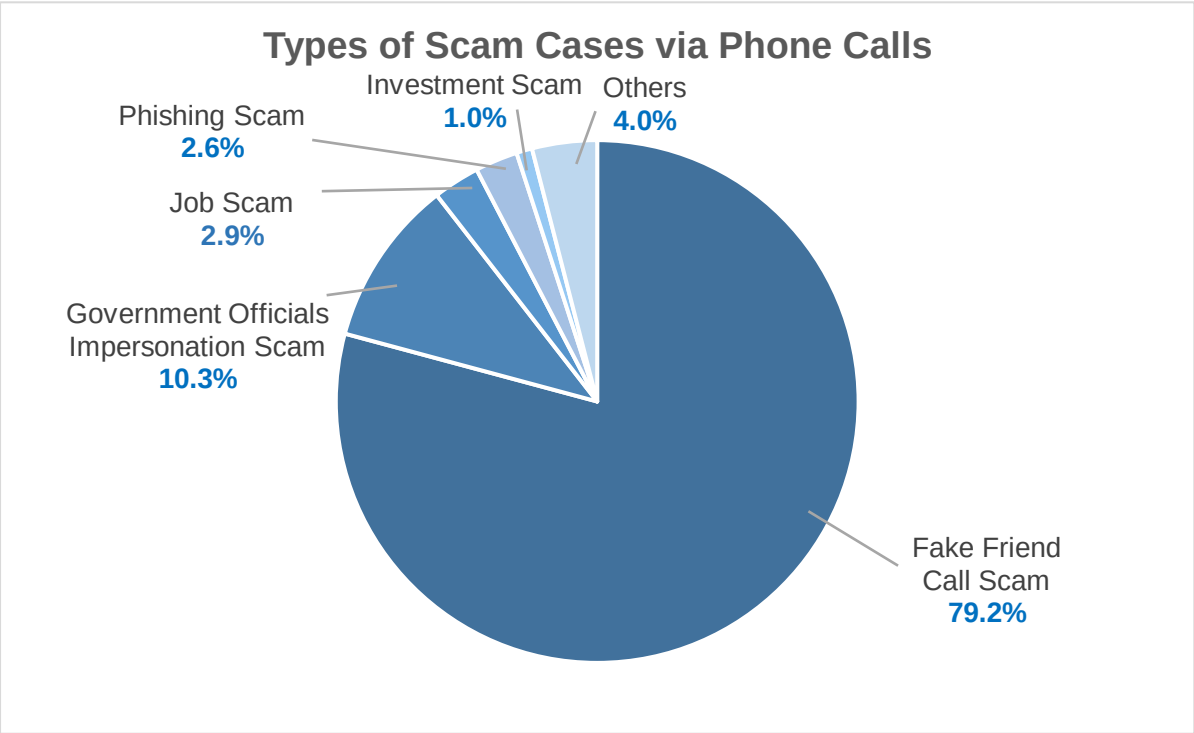
15. The number of scam cases where scammers contacted victims via messaging platforms increased to 12,368 in 2023, from 7,599 in 2022, with about 68.0% of the cases via WhatsApp, and 26.5% via Telegram.



16. Among the scam cases where scammers contacted victims via WhatsApp, 51.6% were job scams, 12.3% were fake friend call scams and 11.1% were phishing scams.



17. Another contact method of concern is phone calls. There was an increase in the number of scam cases perpetrated via phone calls to 7,196 in 2023 from 3,602 in 2022. Of which, 79.2% were fake friend call scams, 10.3% were government officials impersonation scams and 2.9% were job scams.



Scam Victim Profile

18. **73.0% of scam victims were youths, young adults and adults aged below 50.** The breakdown of scam victims by age group is as follows:

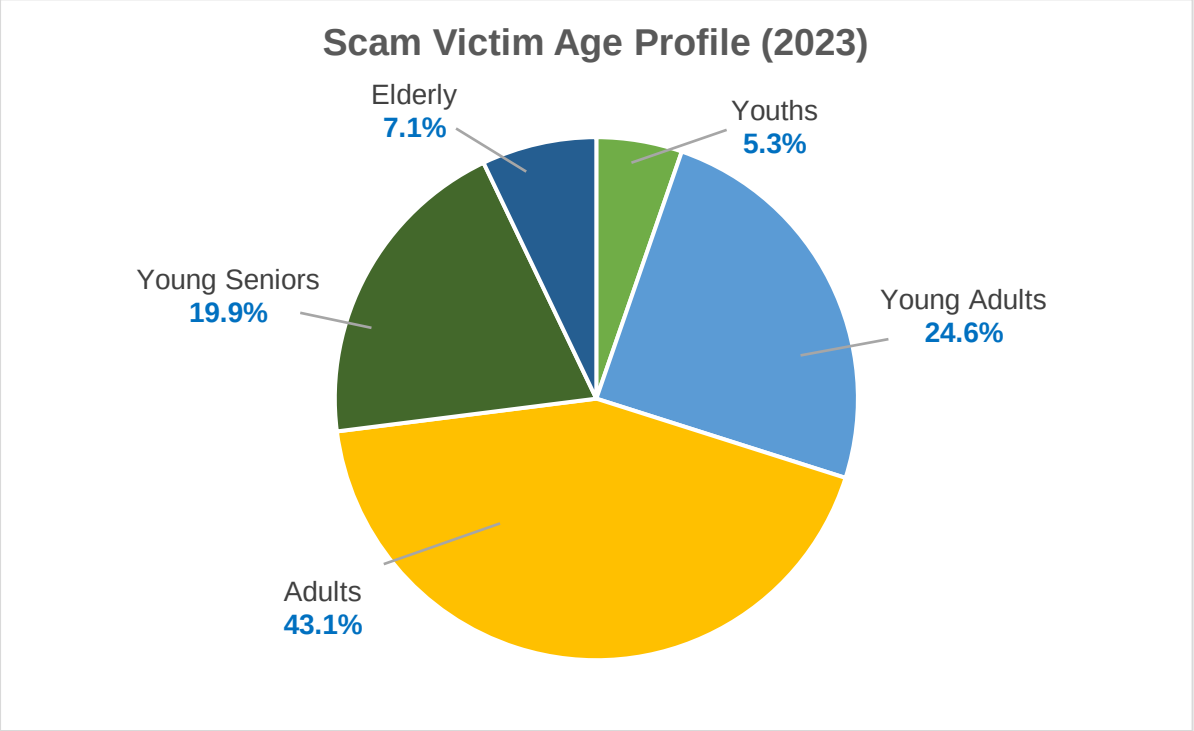
a) Youths, aged 19 and below, made up 5.3% of scam victims. 32.0% from this age group fell prey to e-commerce scams, while 25.4% fell prey to job scams and 16.6% fell prey to phishing scams. Scammers tend to contact youths via messaging platforms, online shopping platforms, and social media.

b) Young adults, aged 20 to 29, made up 24.6% of scam victims. 31.9% from this age group fell prey to job scams, while 25.9% fell prey to e-commerce scams and 10.6% fell prey to phishing scams. Scammers tend to contact young adults via messaging platforms, social media and online shopping platforms.

c) Adults, aged 30 to 49, made up 43.1% of scam victims. 24.6% fell prey to e-commerce scams, while 22.3% fell prey to job scams and 14.3% fell prey to phishing scams. Scammers tend to contact this victim group via social media, messaging platforms and online shopping platforms.

d) Young seniors, aged 50 to 64, made up 19.9% of scam victims. 28.0% fell prey to fake friend call scams, while 12.8% fell prey to e-commerce scams and 12.2% fell prey to phishing scams. Scammers tend to contact this victim group via social media, phone calls and messaging platforms.

e) The elderly, aged 65 and above, made up 7.1% of scam victims. 34.3% from this age group fell prey to fake friend call scams, while 13.7% fell prey to investment scams and 11.7% fell prey to phishing scams. Scammers tend to reach out to the elderly via phone calls, social media and messaging platforms.



Police's Efforts to Fight Scams and Cybercrimes

Enforcement

a) Harnessing strong public-private partnership

19. The Anti-Scam Command (ASCom) has expanded its partnerships to more than 100 institutions, comprising local and foreign banks, debit/credit card security groups, fintech companies, cryptocurrency houses and remittance service providers, 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 relationship with these partners. **In 2023, the ASCom froze more than 19,600 bank accounts based on reports referred to the Anti-Scam Centre (ASC) and recovered more than $100 million.**

Working with banks and Government Technology Agency to identify and flag unusual Singpass activities

20. 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 enables timely and successful victim interventions.

Working with e-commerce platforms to take down scam-related online monikers and advertisements

21. To enhance operational response in taking down scam-tainted online monikers and suspicious advertisements, this initiative was expanded to include the co-location of Carousell staff from 30 January 2024. This co-location initiative was instrumental in supporting the ASCom in its swift intervention in scam cases on the Carousell platform.

b) Other law enforcement interventions

Enforcement operations targeting fraudulent use of SIM cards

22. In 2023, SPF conducted four island-wide operations targeting 17 handphone shops and arrested 11 persons for their suspected involvement in fraudulently registering SIM cards using others' particulars. They allegedly helped scammers exploit pre-registered prepaid/postpaid SIM cards as an anonymous channel of communications for their illicit activities. The four operations resulted in the termination of more than 3,000 phone lines.

Enforcement operations targeting local scammers and money mules

23. SPF continues to take tough anti-scam enforcement actions against local scammers and money mules. In 2023, the ASCom, together with the Scam Strike Teams in the seven Police Land Divisions, conducted 24 island-wide anti-scam

enforcement operations, leading to the investigation of more than 9,600 money mules and scammers.

Enforcement operations against malware-enabled scams

24. SPF also conducted multiple operations against malware-enabled scams, leading to the arrest of more than 140 persons with more than 30 of them being prosecuted in court for offences such as (i) disclosing Singpass credentials under Section 8(2)(a) of the Computer Misuse Act 1993; (ii) conspiring to cheat the bank into opening a bank account under Section 417 read with Section 109 of the Penal Code 1871 (iii) abetting unknown persons to secure unauthorised access to the bank's computer system under Section 3(1) read with Section 12 and Section 14 of the Computer Misuse Act 1993.

Collaboration with local telecommunication companies and e-commerce platforms to terminate phone lines and remove information online related to scams

25. 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 2023, more than 9,200 mobile lines and more than 29,200 WhatsApp lines which were believed to be used in scams, were submitted for termination. Additionally, more than 4,100 scam-tainted online monikers and advertisements were submitted to the respective platforms for removal.

Collaboration with technology companies to flag and block malicious URLs

26. In July 2023, SPF was enrolled into the newly launched Google Cloud Priority Flagger Program, a programme that aims to accelerate the identification and flagging of potential phishing websites and malware hosted on the service. By being a priority flagger, SPF's submission of the malicious websites and malware will be prioritised by Google for their action.

27. SPF has also been working with online platforms, including Google, to introduce stronger safeguards to mitigate the risk of fraudulent takeover of online messaging accounts, such as through the pre-emptive detection and blocking of URLs linked to phishing sites.

Blocking of scam websites

28. SPF uses analytic tools to identify and block scam websites. In 2023, SPF worked with local Internet Service Providers to block over 25,000 scam websites.

c) Collaboration with foreign law enforcement agencies

29. Most online scams are perpetrated by scammers based outside of Singapore. Such cases are difficult to investigate and prosecute. 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. These scammers are typically part of organised criminal groups and run sophisticated

transnational operations which are not easy to uncover or dismantle. It is very difficult to recover monies that have been transferred outside Singapore. Nonetheless, SPF continues to work 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.

Take-down of scam syndicates through collaboration with overseas law enforcement agencies

30. In 2023, the close collaboration between SPF and overseas law enforcement agencies led to the successful take-down of 19 scam syndicates comprising eight job scam and money laundering syndicates, six fake friend call scam syndicates, three phishing scam syndicates and two Internet love scam syndicates. More than 110 persons based overseas, who were responsible for more than 730 scam cases, were arrested.

Participation in internationally coordinated scam operations

31. SPF also participates in internationally coordinated operations against scams. In 2023, the ASCom participated in two such operations. The first was INTERPOL's Operation First Light, which involved more than 76 countries. During the operation, more than 2,000 persons were investigated and over 5,300 bank accounts were frozen in Singapore, leading to the recovery of more than $11.5 million. In addition, a total of more than $30 million worth of virtual assets were seized by the ASCom.

32. The second was INTERPOL's Operation HAECHI, which involved 32 countries. During the operation, the ASCom investigated more than 800 suspects involved in scams and money laundering, blocked more than 4,900 bank accounts and seized over $16.4 million in Singapore. More than 300 virtual accounts were also blocked, with over $500,000 in virtual assets seized by the ASCom.

<u>Engagement</u>

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

33. In addition to enforcement, the ASCom also engaged in upstream interventions to identify and alert victims, and leveraged technology to strengthen its sense-making capabilities. Through Project A.S.T.R.O., which stands for 'Automation of Scam-fighting Tactics & Reaching Out', the ASCom works with banks such as OCBC, UOB and DBS, 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 six joint operations in 2023, more than 68,000 SMSes were sent to alert more than 28,500 victims. **This proactive approach averted over $148 million of potential losses.**

Proactive interventions with potential scam victims

34. To intensify SPF's reach to the community in the area of scam intervention, the ASCom and the Community Policing Units (CPUs) of the Police Land Divisions jointly conduct proactive interventions with potential scam victims. These victims were referred by the banks as they were found to be attempting monetary transfers observed to be suspicious. **In 2023, the ASCom successfully conducted more than 590 interventions, further averting more than $44 million of potential losses for these victims.**

35. SPF will explore more ways to conduct its outreach and prevent potential victims from being scammed.

36. Please see **Annex C** for comments from the Director of the Commercial Affairs Department.

Education

37. To keep pace with the ever-changing scam environment, SPF continues to focus on public education efforts to encourage individuals to proactively adopt anti-scam measures to safeguard themselves and those around them from scams. SPF will also continue to make it easier for members of the public to find information on scams and to seek help.

Setting up of a dedicated department for scam public education

38. SPF set up the Scam Public Education Office (SPEO) in 2023 to drive anti-scam public education and awareness efforts. Leveraging partnerships across public and private stakeholders, SPEO continues to expand the Government's outreach on scams through the following:

(a) Broad-based programmes and communications;
(b) Targeted programmes for different population segments; and
(c) Rallying the community to amplify and co-create anti-scam messages and programmes.

Availability of anti-scam information and resources via various platforms

Add, Check, Tell framework

39. To educate members of the public on anti-scam protective measures under the Add, Check, Tell framework, SPF continues to work closely with the National Crime Prevention Council (NCPC) on the "I can ACT against Scams" campaign. The ACT campaign video features a specially composed song which encourages people to act against scams. It was viewed over one million times since November 2023 when it was uploaded on social and digital platforms including NCPC's YouTube Channel.

40. Please see **Annex D** for comments from the Vice-Chairman of the National Crime Prevention Council.

Regular dissemination of information on latest and trending scam types

41. The SPF ensures timely dissemination of information on the latest and trending scam types. Public education efforts on scams are available on both physical and digital platforms, as well as mainstream and social media platforms. They include frequent Police news releases to the media outlets, features on the 'CrimeWatch' programme, bite-sized videos, infographics on digital display panels at HDB lift lobbies, as well as regular scam bulletins and columns. For example, since November 2023, SPF has been working with Singapore Press Holdings Media to publish a column on scams in local newspapers in the four vernacular languages, twice a month.

Dedicated app, helpline, messaging platforms and websites on scams

42. The ScamShield app has reached 850,000 downloads, and users have submitted over 7.9 million suspected scam SMSes via the app since its launch. Every report made through ScamShield improves the accuracy of the system in detecting scam messages, and helps prevent scammers from reaching more potential victims.

43. Other anti-scam resources promoted by the "I can ACT against Scams" campaign were also well received. For example, in 2023, the Anti-Scam Helpline received over 3,000 calls seeking scam-related advice; the ScamAlert WhatsApp and Telegram channels have a joint following of 31,000 users till date; and the ScamAlert website – one of the official sources to find information on scams – received over one million visitors. A new Anti-Scam Resource Guide was launched on the SPF website in December 2023, addressing frequently asked questions relating to police investigations into scams-related offences, and containing resources to support scam victims.

Scam education programmes for different population segments

44. In November 2023, the Domestic Guardians programme was expanded island-wide. The programme trains migrant domestic workers in scam prevention by sharing information on crimes and scams so that they may better detect and deter crimes in the community, and become advocates for crime prevention amongst their fellow migrant domestic workers.

45. SPF also works closely with WOG partners to tailor programmes for different population segments. Examples include collaborative outreach to the elderly with the Ministry of Communications and Information through "Getai" shows and with the Agency for Integrated Care through their Silver Generation Ambassadors. SPF also reaches out to migrant worker communities through the Ministry of Manpower's settling-in-programme for migrant workers and campaign for migrant domestic workers.

Rallying organisations and the community to fight against scams

46. SPF has been rallying community partners to play a more proactive role in the fight against scams. In 2023, two more sessions of the Conversation on Safeguarding the Community with Actionable Measures Against Scams (C-SCAMS) were conducted, targeting the youths and migrant workers. Through the sessions, participants brainstormed how to better keep the different population segments safe from scams, and how organisations can work with the Government on more effective

outreach to the different population segments. More than 110 participants and 30 organisations were engaged through the C-SCAMS series in 2023.

47. The Ministry of Home Affairs (MHA), SPF and NCPC also engaged TikTok content creators as part of the "Guess the Scam" campaign, where content creators created TikTok videos to raise awareness on the top scam types in Singapore, and highlighted the importance of anti-scam protective actions in the ACT framework.

E-Shoppers on Watch interest group of the Community Watch Scheme

48. The SPF formalised an e-Shoppers on Watch interest group under the Cyber category of the Community Watch Scheme (CWS) in 2021. The interest group harnesses the community to share relevant scam information they come across with the SPF and share scam-related advisories from the SPF with their loved ones. As of 31 December 2023, there were more than 7,700 CWS members in the e-Shoppers on Watch interest group, an increase of 79.1% from 4,300 members in 2022.

E-commerce Marketplace Transaction Safety Ratings ("TSR")

49. The E-commerce Marketplace TSR was launched in May 2022 to educate consumers on the extent to which different e-commerce marketplaces have safety features in place to protect them from scams.

50. In 2023, Facebook Marketplace continued to be rated the worst (one tick), as the platform has not implemented the recommended safeguards e.g. user verification against Government-issued records, and has had a significant number of e-commerce scam reports (1,138 cases in 2022, or 23.9% of total number of e-commerce scams). The recommended user verification measures have proven to be effective – platforms which have implemented them (i.e., Amazon, Lazada, Qoo10) have seen a low number of e-commerce scam reports, and were awarded the full four ticks in the TSR.

51. 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

52. The TSR can be found on MHA's website.

WOG Efforts to Fight Scams

Anti-scam measures by the Smart Nation Group

53. In November 2023, the SNG organised the second Smart Nation Grandparents' Day to educate seniors and their family members on the safe and secure use of digital government services. The one-day event saw about 2,500 participants engaging in

tech-related games and activities organised by partners from various sectors, including GovTech, National Library Board (NLB), SG Digital Office, Google, Mediacorp, RSVP Singapore, and more.

54. The SNG actively engages citizens through webinars and hybrid sessions on the #SmartNationTogether platform to raise awareness about the importance of staying vigilant, safeguarding their Singpass, and utilising tools such as ScamShield to counter scams. The permanent interactive cybersecurity exhibit at the Smart Nation PlayScape, situated at the Science Centre Singapore, aims to educate visitors about the significance of cyber safety in the face of evolving cyber threats.

55. As part of its public outreach efforts, GovTech ran the Singpass "Be Sure. Be Secure." public education campaign in August 2023 to educate Singapore residents on keeping their Singpass safe from scams. Besides that, GovTech has also enhanced Singpass' security measures to protect users against the threat of scams. For example, in response to malware-related scams involving unauthorised withdrawals of CPF monies, GovTech and CPF Board introduced additional factors such as facial verification in June 2023 to protect vulnerable CPF members who access CPF e-services. In addition, on 30 November 2023, CPF Board introduced a default online CPF Daily Withdrawal Limit of $2,000 a day, for all CPF members aged 55 and above. To prevent unauthorised adjustments to increase the Daily Withdrawal Limit, facial verification and a 12-hour cooling period are required. CPF members can also disable online CPF withdrawals by activating the CPF Withdrawal Lock, which instantly reduces this limit to $0. To safeguard members' basic retirement adequacy, amounts up to the Basic Retirement Sum are automatically reserved for retirement and cannot be withdrawn. Users who suspect their Singpass has been compromised can call the Singpass Helpdesk at 6335 3533 and press "9" for 24-hour support.

Anti-scam measures by the Monetary Authority of Singapore

56. The MAS continues to work closely with The Association of Banks in Singapore's Standing Committee on Fraud to combat digital banking scams.

57. In combatting malware-enabled scams and to protect customers from malware that take control of customers' devices and hence their mobile banking access, MAS, together with SPF, has worked with banks to implement counter measures. Starting with OCBC in August 2023, various banks have progressively rolled out upgraded versions of their banking apps with anti-malware measures. These measures restrict access to banking apps if an Android device was detected to have sideloaded apps with accessibility permissions granted. Since then, malware-enabled scam cases have started to decline drastically as more people had their banking apps upgraded.

58. Such collaboration with private stakeholders in developing upstream measures contributed directly to the decrease in malware-enabled scams towards the end of 2023.

59. In November 2023, local banks introduced Money Lock, a feature that lowers the impact of scams by allowing customers to set aside a portion of their funds in bank accounts that cannot be transferred digitally. As of January 2024, more than 49,000 Money Lock accounts have been set up, with more than $4.2 billion set aside. The

Money Lock feature would be progressivmalwaely introduced by other major retail banks by June 2024. Banks will continue to enhance their suite of anti-scam measures and raise their customers' awareness of red flags as the threat landscape changes.

Anti-scam measures by the Cyber Security Agency of Singapore

60. In January 2024, CSA published the Safe App Standard to help local app developers and providers enhance mobile app security. The Standard is targeted at apps that perform high-risk transactions. It provides a common benchmark and guidance to local app developers and providers on the necessary security controls and best practices to better protect their apps, and in turn, their end-users, against common malware and phishing attempts.

61. CSA has disseminated key anti-scam messages through multiple platforms, such as school talks, roadshows, social media and media partnerships. The revamped Be Cyber Safe Pop-up and Drama Skit was rolled out to schools in January 2024 to raise awareness on the importance of cybersecurity, common types of online scams and educate students on cyber tips to protect themselves.

62. As part of the 'Unseen Enemy' campaign launched on 30 September 2023, CSA will be organising two more community roadshows at Toa Payoh Hub and Heartbeat@Bedok in 2024. The roadshow setups mirror a home setting, showcasing the campaign's four refreshed Cyber Tips to help visitors learn how to protect themselves from the latest cyber threats and scams. The roadshows will also showcase booths from partners SPF, NCPC, IMDA and Singtel.

63. CSA has also collaborated with popular e-commerce platforms to raise cybersecurity awareness and adoption. Lazada created a microsite on their app to amplify the four Cyber Tips and highlight relevant cybersecurity products such as anti-virus software, as well as publicise CSA's recommended security app list. Zalora worked with CSA to adapt content based on the Cyber Tips and which was then pushed out through their social media platforms.

64. CSA has been partnering the industry to strengthen our collective effort to combat cybercrime and scams. As part of Total Defence Day 2024, CSA has launched playbooks for the conduct of simulated phishing exercises to help organisations raise awareness and train their employees to be more vigilant against phishing attempts. These playbooks were developed in partnership with Microsoft and Google. In February 2024, Google announced that, in partnership with CSA, they will be launching a new Android security feature to block the sideloading of high-risk apps. This is expected to be progressively rolled out from end-February onwards.

Anti-scam measures by the Infocomm Media Development Authority

Working with Telcos to implement anti-scam measures

65. As part of multi-layered measures to protect the public from scams, IMDA has worked with Telcos to implement anti-scam measures to strengthen safeguards for SMSes and calls to Singapore users from international numbers. This includes allowing subscribers to block incoming calls from international numbers on their mobile

phones, and the SMS Sender ID Registry where un-registered Sender IDs are labelled as “Likely-SCAM” as an alert to users.

Telcos to limit number of post-paid SIM cards per subscriber as part of anti-scam efforts

66. To safeguard against the illicit use of local SIM cards, each individual is only allowed to purchase a maximum of three pre-paid SIM cards today, which is sufficient to meet the needs of genuine users’ who are mainly foreign visitors, tourists and contract workers. The SPF and IMDA have observed signs that post-paid SIM cards, predominantly purchased by locals, are increasingly being misused for scams. Therefore, a limit of 10 post-paid SIM cards per individual will be imposed. A higher cap is adopted to cater to the needs of legitimate users who may register SIM cards for family members, while limiting illicit usage.

67. This measure will take effect from 15 April 2024 and it will only apply to new registrations. Subscribers who currently have more than 10 post-paid SIM cards will not be affected. However, they will not be able to register additional SIM cards. IMDA will review the post-paid SIM cards limit over time to ensure that it continues to be relevant.

Strengthening legislative levers

68. We have also updated our laws to allow the Government to act more effectively against scammers.

i. The Online Criminal Harms Act, which came into force on 1 February 2024, empowers law enforcement agencies to direct online services to prevent suspected scam accounts or activities from interacting with or reaching Singapore users.

   In addition, the SPF can also require designated online services to implement systems, processes or measures to counter scams, such as requiring the verification of user identities against government-issued identification documents.

ii. The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) and the Computer Misuse Act (CMA) were amended in May 2023, to allow the SPF to take more effective action against money mules and those who abuse Singpass for criminal activities. Specifically, new offences were introduced under the CDSA to make it easier for the SPF to make out a money laundering offence, while the CMA was amended to allow the SPF to deal with individuals who abuse their Singpass credentials.

   These new amendments took effect on 8 February 2024.

iii. MHA will be introducing new offences which criminalise the abuse of SIM cards. More details will be announced when ready.

Everyone Plays a Part in Fighting Scams

69. Everyone has a part to play in keeping Singapore safe and secure. Individuals should proactively adopt anti-scam measures to safeguard themselves and those around them from scams. SPF will continue to work with government agencies and community partners to engage and educate the public in building the community's vigilance and resilience towards scams. In addition, business operators, particularly banks, online marketplaces and telcos, also 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
18 FEBRUARY 2024 @ 3PM

Annex A

Top 10 scam types in Singapore (Based on number of reported cases)

Types of Scams	Cases reported		Total amount lost (at least)		Average amount lost per case		
	2023	2022	2023	2022	2023	2022	Difference
Job Scam	9,914	6,492	$135.7M	$117.4M	$13,692	$18,089	↓ $4,397
E-commerce Scam	9,783	4,762	$13.9M	$21.3M	$1,428	$4,491	↓ $3,063
Fake Friend Call Scam	6,859	2,106	$23.1M	$8.8M	$3,373	$4,201	↓ $828
Phishing Scam	5,938	7,097	$14.2M	$16.5M	$2,394	$2,338	↑ $56
Investment Scam	4,030	3,108	$204.5M	$198.3M	$50,754	$63,834	↓ $13,080
Malware-enabled Scam	1,899	-	$34.1M	-	$17,960	-	-
Social Media Impersonation Scam	1,570	1,696	$9.7M	$3.7M	$6,184	$2,231	↑ $3,953
Loan Scam	914	1,031	$6.1M	$9.3M	$6,676	$9,082	↓ $2,406
Internet Love Scam	913	868	$39.8M	$35.7M	$43,677	$41,200	↑ $2,477
Government Officials Impersonation Scam	893	771	$92.5M	$97.6M	$103,657	$126,697	↓ $23,040
Top 10 scams	42,713	27,931	$573.9M	$509.2M	$13,438	$18,232	↓ $4,794

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

Annex B

Case studies on how scammers exploited Meta platforms

(The case studies are based on real-life reported cases. The names mentioned are fictitious.)

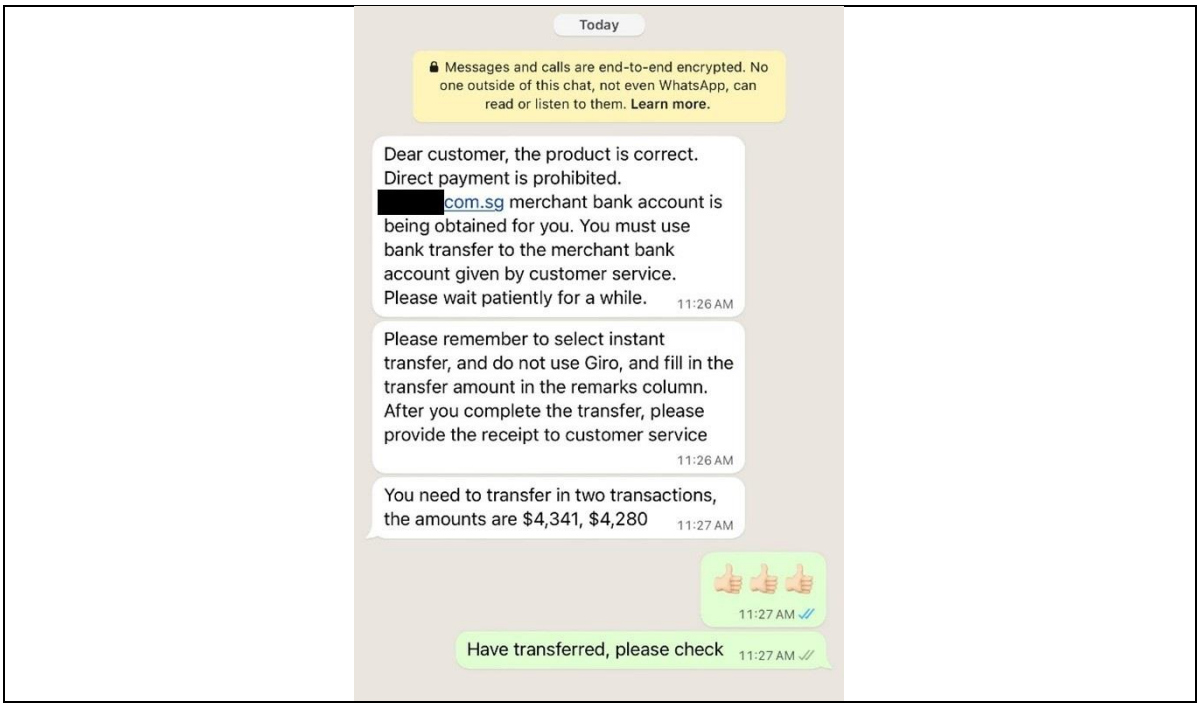
a. Job scam perpetrated via Instagram and WhatsApp

*Scammers befriended victims to ask for assistance or offer work involving boosting products on legitimate e-commerce platforms through **Instagram**.*

Adrian received a message from a lady named Evelyn on Instagram and continued their conversation on WhatsApp, where Adrian was offered an ad-hoc job opportunity to earn side income. Adrian was told to contact another WhatsApp number ("customer service") and that he could earn commissions by making payment for products from a legitimate company and they would also refund the payment made.

For Adrian's first task, he was asked to transfer $109 to a PayNow number by the "customer service". After Adrian completed the task, he received $114.45 (which included a reimbursement of the $109 that he had transferred earlier and a 5% commission of $5.45) in his bank account. Adrian was made to believe that this was a genuine work arrangement where his services would be compensated.

Adrian was then tasked by "customer service" to perform seven transactions of various amounts which totalled about $18,140. Adrian did as he was told but did not receive his reimbursement and commission. When he asked "customer service" about the non-payment via WhatsApp, "customer service" told him that he had to complete the latest task. Adrian latest task was to make another two transfers of $4,341 and $4,280. Adrian realised that he was scammed and lodged a police report.



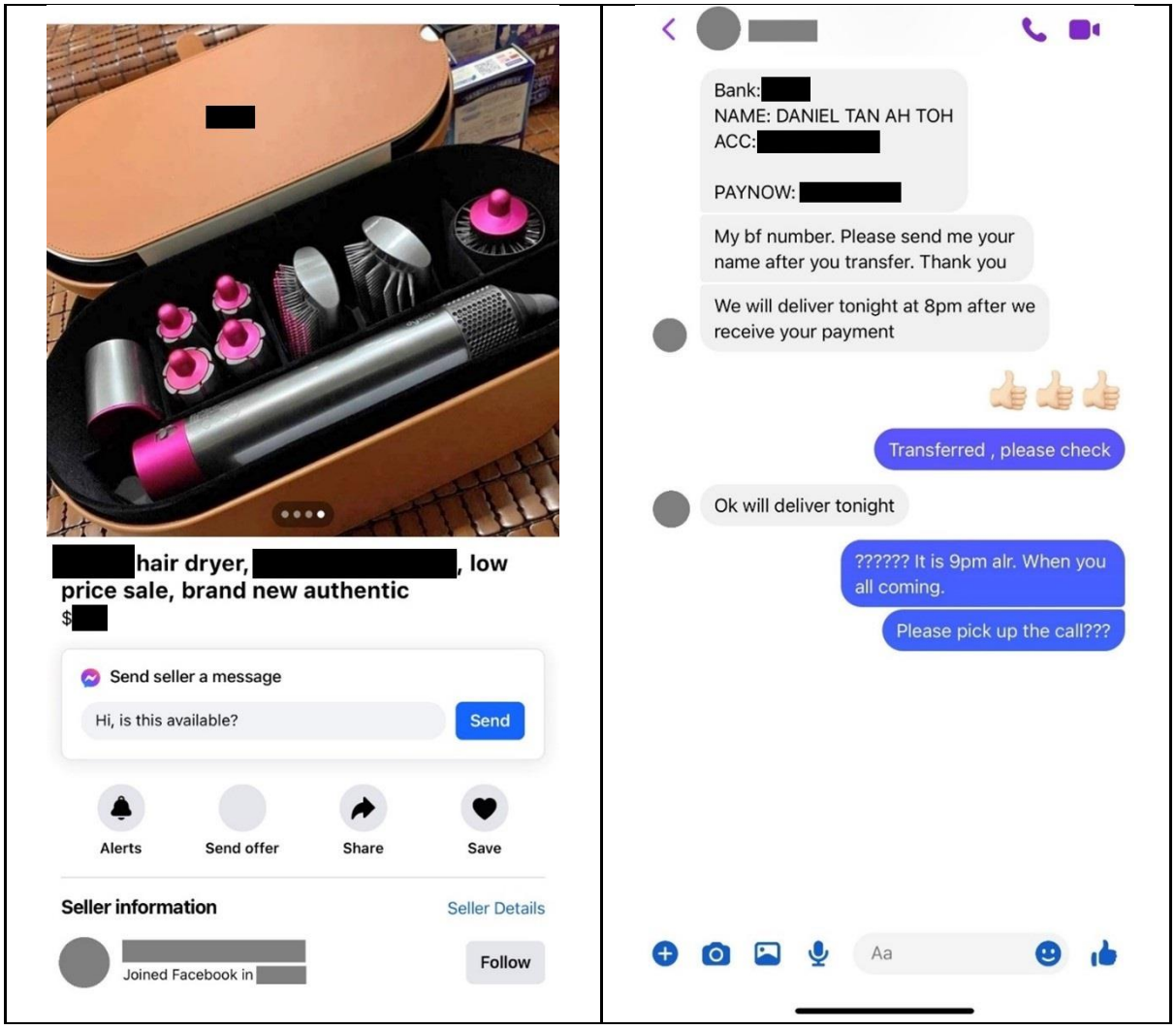
Screenshot of WhatsApp conversation between the scammer and victim

b. E-commerce scam perpetrated via Facebook

*The freecycling variant entails victims coming across listings offering free giveaways or the sale of items at discounted prices on **Facebook.** For free giveaways, scammers would request for goodwill deposits or payment for delivery. For the sale of discounted items, scammers would request for reservation fees. After victims have made payment, the scammers would become uncontactable.*

Cindy chanced upon a post on Facebook offering second-hand items and contacted the seller via Facebook messenger to purchase some electronic appliances amounting to $1,200. The seller told Cindy to make a payment of $300 to a PayNow number to secure the items and assured her that the items would be delivered by 7pm on the same day. Cindy made the transfer.

At 8pm when the goods did not arrive, Cindy texted the seller via Facebook but was told that the delivery would be delayed. At 9.29pm, Cindy contacted the seller again but the Facebook account was no longer available on Facebook messenger and she realised that she had been scammed.



Screenshot of Facebook account used to approach the victim	Screenshot of conversation between the scammer and victim

c. Fake friend call scam perpetrated via WhatsApp

*Victims received a phone or **WhatsApp call/message** from someone who pretended to be their friend or someone they know. In most cases, the caller would provide the bank details via **WhatsApp message** using a different phone number for victims to make the transfer.*

On 21 November 2023, Ah Tan received a call from a scammer asking Ah Tan to guess his identity. Ah Tan guessed that the scammer was his friend Klement. The scammer assumed the identity of "Klement" and told Ah Tan that he had lost his phone and identity card and the number which appeared on Ah Tan's phone was his new contact number.

The following day, the scammer called Ah Tan and said that he needed money to pay his supplier and sought Ah Tan's help for a loan of $3,800. Subsequently, Ah Tan received WhatsApp messages from the scammer providing bank details for the transfer. Prior to the transfer, Ah Tan requested for an invoice and the address of the company from the scammer for verification purposes. Ah Tan received an invoice via WhatsApp. Thinking that it was a legitimate company and the scammer was his friend, Klement, Ah Tan agreed to lend him the money and made the transfer of $3,800 via PayNow to a number provided by the scammer.

On the same day, the scammer called Ah Tan again asking for more money. Ah Tan then decided to call his friend Klement on the original contact number instead of the new one. Klement informed Ah Tan that he did not ask Ah Tan for any money. Ah Tan then realised that he had been scammed and lodged a police report.

Screenshot of WhatsApp conversation between the scammer and victim

d. Phishing scam perpetrated via Facebook

*Victims came across **Facebook promotional advertisements** that led to spoofed websites or phishing links. Scammers would send phishing links or QR codes that directed victims to spoofed websites of banks or delivery companies.*

On 6 January 2023, Daniel chanced upon an advertisement on Facebook selling an iPhone 14 Pro Max. Daniel clicked on the advertisement and was directed to a bank login page. Daniel logged in with his banking account credentials and entered the OTP.

After keying in the OTP, Daniel realised that he had received $1,000 credited into his bank account, and another $988 was deducted from it. Subsequently, Daniel was logged out of the i-banking application and received a SMS from the bank informing that he had successfully made a transfer of $988 to an account via PayNow. Daniel called the bank immediately and was informed by the bank that he was scammed and a loan of $1,000 was applied under his bank account. In total, Daniel suffered a loss of $988.

e. Investment scam perpetrated via Facebook and WhatsApp

*Victims were approached and befriended through **Facebook** and **WhatsApp** before scammers introduced "investment opportunities".*

On 8 October 2023, Jenny posted a room rental advertisement on Facebook and later received WhatsApp messages from a man, Pete, expressing interest to rent on behalf

of his sister. Jenny saw him as a potential tenant and unknowingly shared personal information with him.

Later in the conversation, Pete introduced Jenny to cryptocurrency mining and shared how much he was profiting from it. Jenny was convinced and under Pete's guidance, she set up a cryptocurrency wallet via the MetaMask app and linked it to a fraudulent website. Pete also asked Jenny to contact a "trader" to exchange cash for cryptocurrency. Jenny met up with the "trader" and handed over $5,000 in cash in exchange for cryptocurrency which was deposited in her MetaMask wallet. She saw a revenue of about 1% which was available to be withdrawn every day.

Jenny tried researching deeper into cryptocurrency mining but could not find much information online regarding this fraudulent website. Pete would scold Jenny for not trusting him whenever she tried to clarify with him.

Over the next few weeks, Pete continued to chat with Jenny while waiting for her to make more cryptocurrency purchases. During this period, Jenny purchased another $9,000 worth of cryptocurrency.

One day, Pete offered to help Jenny earn more cryptocurrency by setting up a "trading account" in the same fraudulent website and instructed her to transfer all her funds from her cryptocurrency wallet into the trading account. Jenny felt uneasy about the trading account when she noticed that the daily mining profits would go into that account automatically and her wallet has always been empty. To alleviate her worries, Jenny tested and managed to transfer 100 USDT back to her cryptocurrency wallet which was successful with 3% fees.

In addition, the scammer claimed to have a close friend in the United States of America with insider information on investment that would allow them to yield high earnings.

Over the next few days, Jenny was convinced that she had earned a total profit of more than 30,000 USDT under Pete's guidance. In between, Pete was urging Jenny to top up more cryptocurrency to receive higher returns. On 27 November 2023, Jenny was informed by Pete that their "trading account" was "frozen". Upon checking with the "customer service", Jenny was informed to return the alleged illegal profits gained within five days to unfreeze it.

Jenny contacted Metamask immediately and realised that she had been scammed, with her losses totaling to $14,000 ($5,000 + $9,000 used to purchase cryptocurrency).

Annex C

Quote by Director of Commercial Affairs Department

Scams continue to be a key concern. The Police work with multiple stakeholders to combat scams – across the whole-of-government, through partnerships with industry, and with international partners.

The Anti-Scam Command partners over 100 stakeholders to fight scams. We have seized close to 20,000 bank accounts and recovered over $100 million in 2023 and worked with our foreign law enforcement partners to dismantle 19 scam syndicates targeting Singapore victims from their operations overseas.

The government has implemented upstream measures such as enhancing legislative levers to tackle online harms and money mules. We have also partnered banks to introduce anti-malware security features for banking apps.

The fight against scams must continue and the responsibility cannot rest with law enforcement alone. Scams will continue to evolve, so a discerning and vigilant public is essential. The Police will continue to work closely with stakeholders and other government agencies to safeguard Singapore against scams.

– Mr. David Chew
Director of Commercial Affairs Department

Annex D

Quote by Vice-Chairman, National Crime Prevention Council

With more sophisticated scams emerging, it is critical for all of us to take precautionary measures to protect ourselves and our loved ones. Simple yet effective actions include downloading the ScamShield app; activating the Money Lock feature to further secure your bank savings; exercising caution before responding to any requests for personal info, and reporting to the Police immediately if you have been scammed. By taking ACTions, we can collectively prevent the scourge of scams on our community.

- Mr. Tan Puay Kern
Vice-Chairman, National Crime Prevention Council