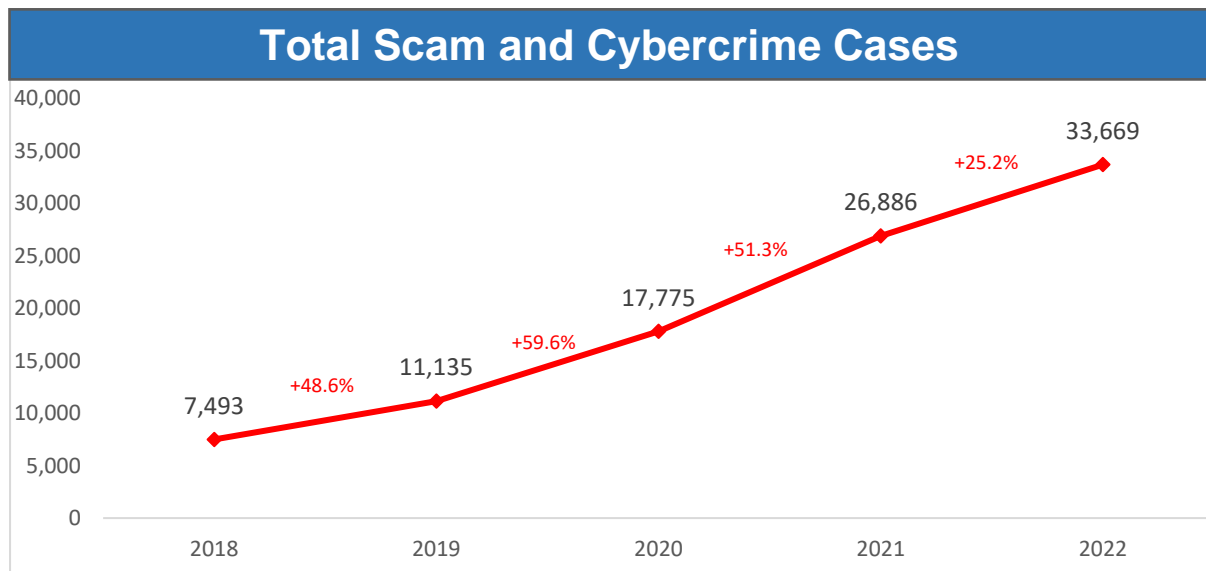




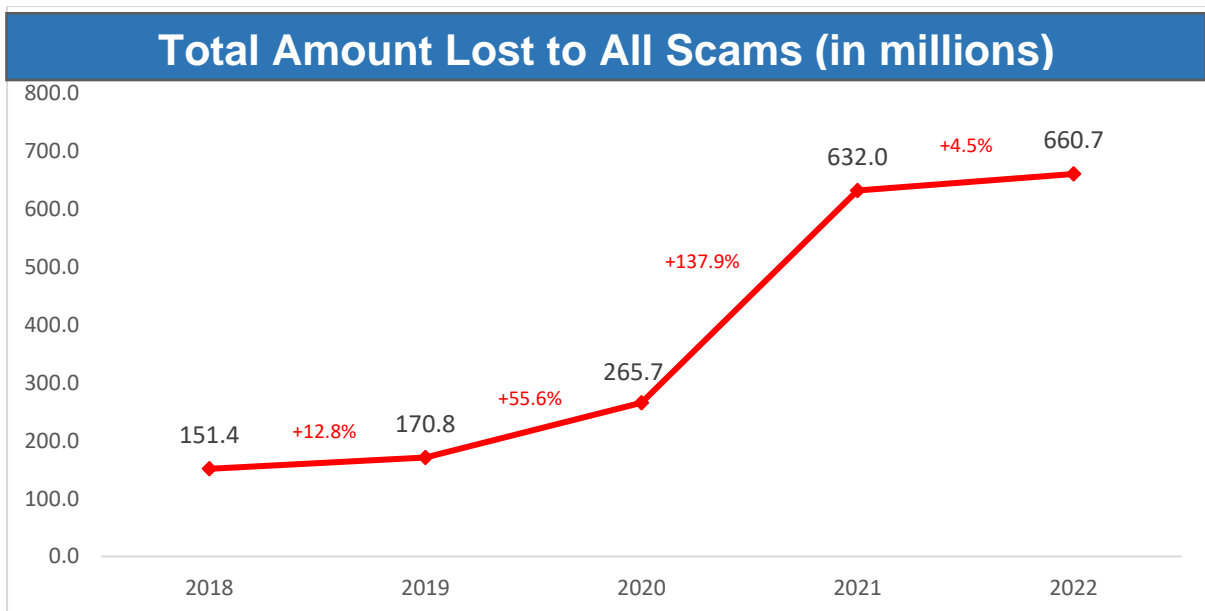
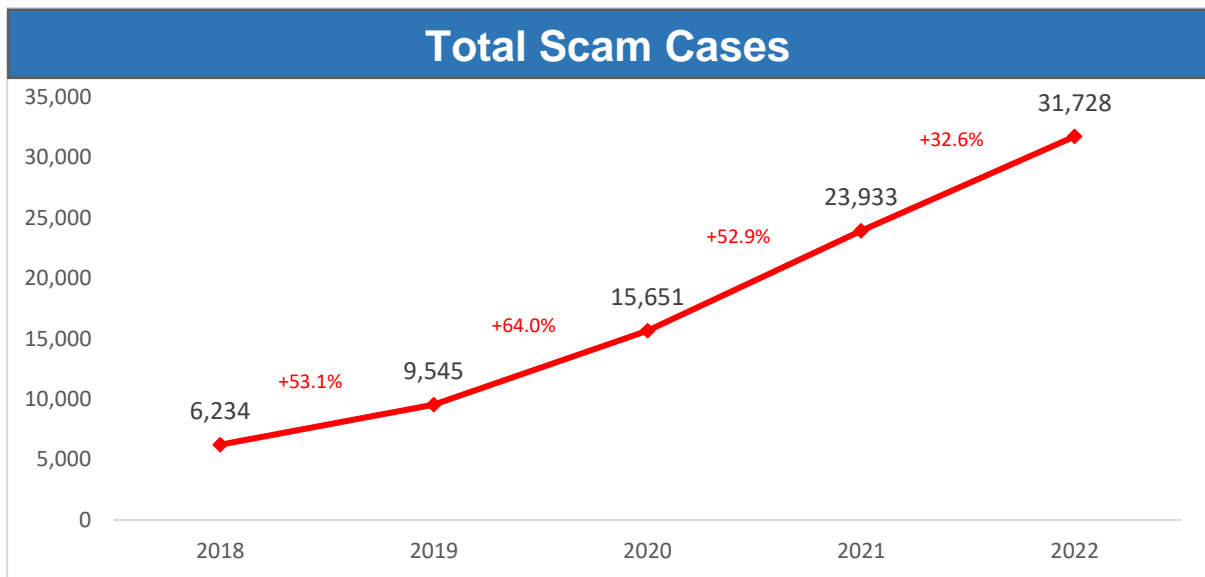
Annual Scams and Cybercrime Brief 2022

Overall Scams and Cybercrime Situation in 2022

Scams and cybercrime continue to be a key concern. The number of scam and cybercrime cases increased by 25.2% to 33,669 in 2022, compared to 26,886 cases in 2021.



2 Scams accounted for 94.2% of these 33,669 cases. The total number of scam cases increased by 32.6% to 31,728 in 2022, from 23,933 cases in 2021. The total amount reported to have been cheated from all scams increased by 4.5% to \$660.7 million in 2022, from \$632.0 million in 2021.

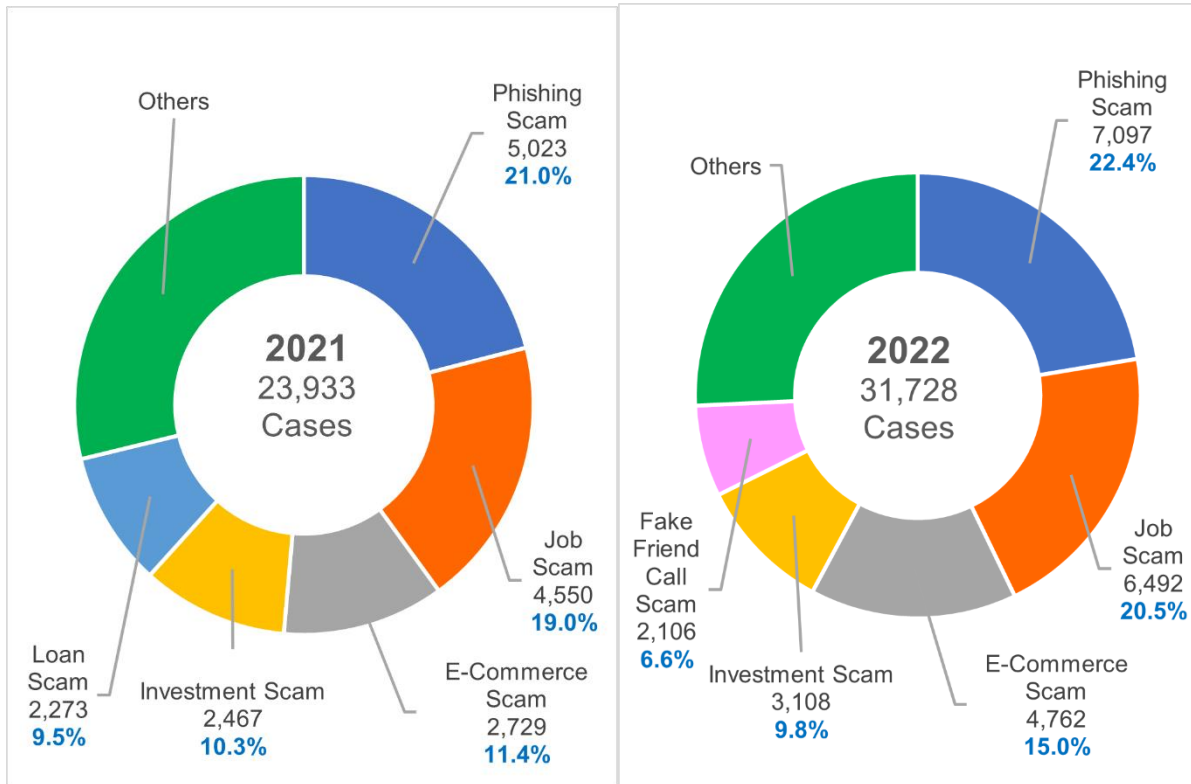


3 However, there were decreases in loan scam cases and internet love scam cases. There were 1,031 loan scam cases in 2022, which is a decrease of 54.6% from 2,273 cases in 2021. The number of internet love scam cases decreased by 20.7% to 868 in 2022, from 1,094 cases in 2021. Nonetheless, as scammers continue to evolve their tactics, we must keep up public vigilance.

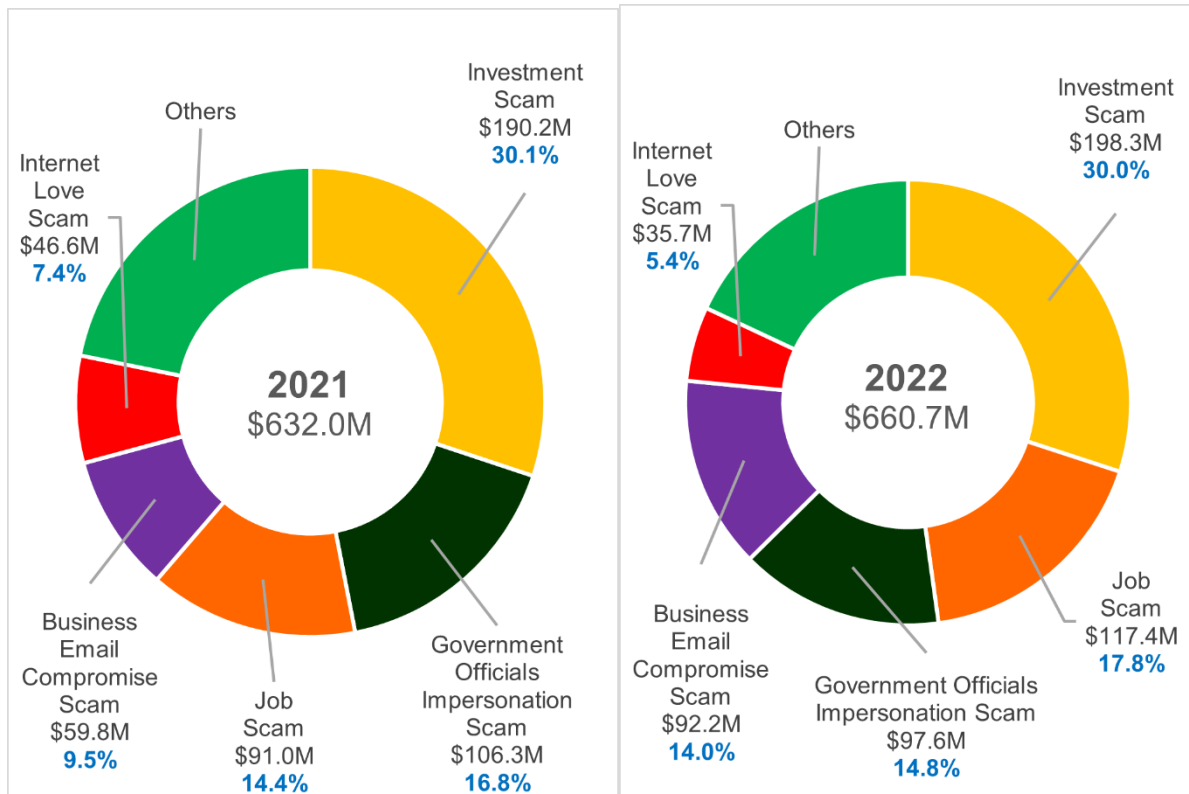
Top Scam Types

4 Phishing scams, job scams, e-commerce scams, investment scams, and fake friend call scams were the top five scam types of 2022. Of these, e-commerce scams has remained among the top five scam types for four consecutive years. These five scam types made up 82.5% of the top ten scam types reported in 2022. Please see [Annex A](#) for the statistics on the top ten scam types.

Breakdown of scam types by number of cases



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



a) Phishing scams

- Phishing scams generally involve emails, text messages or calls 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, scammers would perform unauthorised transactions on victims' credit card or bank accounts.
- Phishing scams recorded the highest number of reported cases amongst all scam types in 2022.
- There were 7,097 phishing scam cases reported in 2022, compared to 5,023 cases in 2021, an increase of 41.3%.
- However, the total amount reported to have been cheated decreased by 52.6% to at least \$16.5 million in 2022, from at least \$34.8 million in 2021.
- Calls (specifically in-app calls e.g., WhatsApp), SMSes and in-app chat messaging were the most common channels used by scammers to contact victims.
- About half of the victims (49.8%) were aged between 30 and 49.

b) Job scams

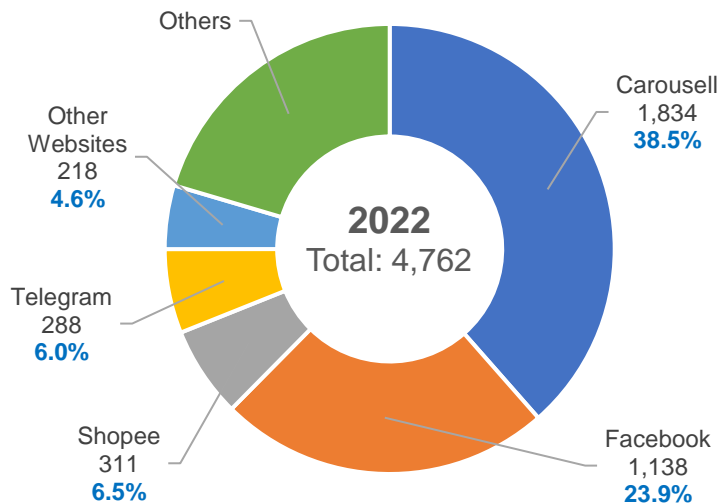
- Job scams typically involve victims being offered online jobs that could be performed from home. Victims would be asked to perform simple tasks like making advance purchases, liking social media posts, or reviewing hotels/restaurants. Victims would initially receive some commission, luring them into providing more funds, purportedly required to get more commission over time. Eventually, the victims would not be able to get their money back.
- There were 6,492 cases reported in 2022, compared to 4,550 cases in 2021, an increase of 42.7%.
- The total amount reported to have been cheated increased by 29.0% to at least \$117.4 million in 2022, from at least \$91.0 million in 2021.
- In most job scams, victims would receive their offers through unsolicited messages from unknown numbers through chat applications, or would come across online advertisements containing job offers. Scam communication would promise high salaries and remote work arrangements and would often include different WhatsApp or Telegram numbers/website links as additional contact points for interested victims to sign up for "jobs" or for creating their "accounts".
- The most common platforms which scammers used to contact victims included Telegram and WhatsApp.
- 66.8% of victims were aged between 20 and 39.

c) E-commerce scams

- E-commerce scams generally involve the sale of goods and services online without delivery of the items or services after payment is made.
- There were 4,762 e-commerce scam cases reported in 2022, compared to 2,729 cases in 2021, an increase of 74.5%.
- The total amount reported to have been cheated increased by 261.0% to at least \$21.3 million in 2022, from at least \$5.9 million in 2021.

- The most common platforms which victims encountered scammers included Carousell, Facebook, and Shopee, while the common items involved in the transactions were electronic goods, rental (residential unit) and gaming-related items. The breakdown of e-commerce scams on the various platforms are as follows:

Top Five Digital Platforms Used In E-Commerce Scams in 2022



- 65.7% of victims were aged between 20 and 39.

d) Investment scams

- Victims of investment scams usually come across “good” investment offers via their own internet searches or via recommendations from online friends. Victims would be enticed to invest by transferring money to unknown bank accounts. In some cases, victims would initially earn a small profit from their investment, and therefore would be enticed to transfer even more funds. After larger sums of money are transferred to the scammers, the victims would realise they could not cash out their earnings.
- There were 3,108 investment scam cases reported in 2022, compared to 2,467 cases in 2021, an increase of 26.0%.
- The total amount reported to have been cheated increased by 4.3% to at least \$198.3 million in 2022, from at least \$190.2 million in 2021.
- Common platforms used by scammers to contact victims included Instagram, Facebook and Telegram.
- 54.9% of victims were aged between 20 and 39.

e) Fake friend call scams

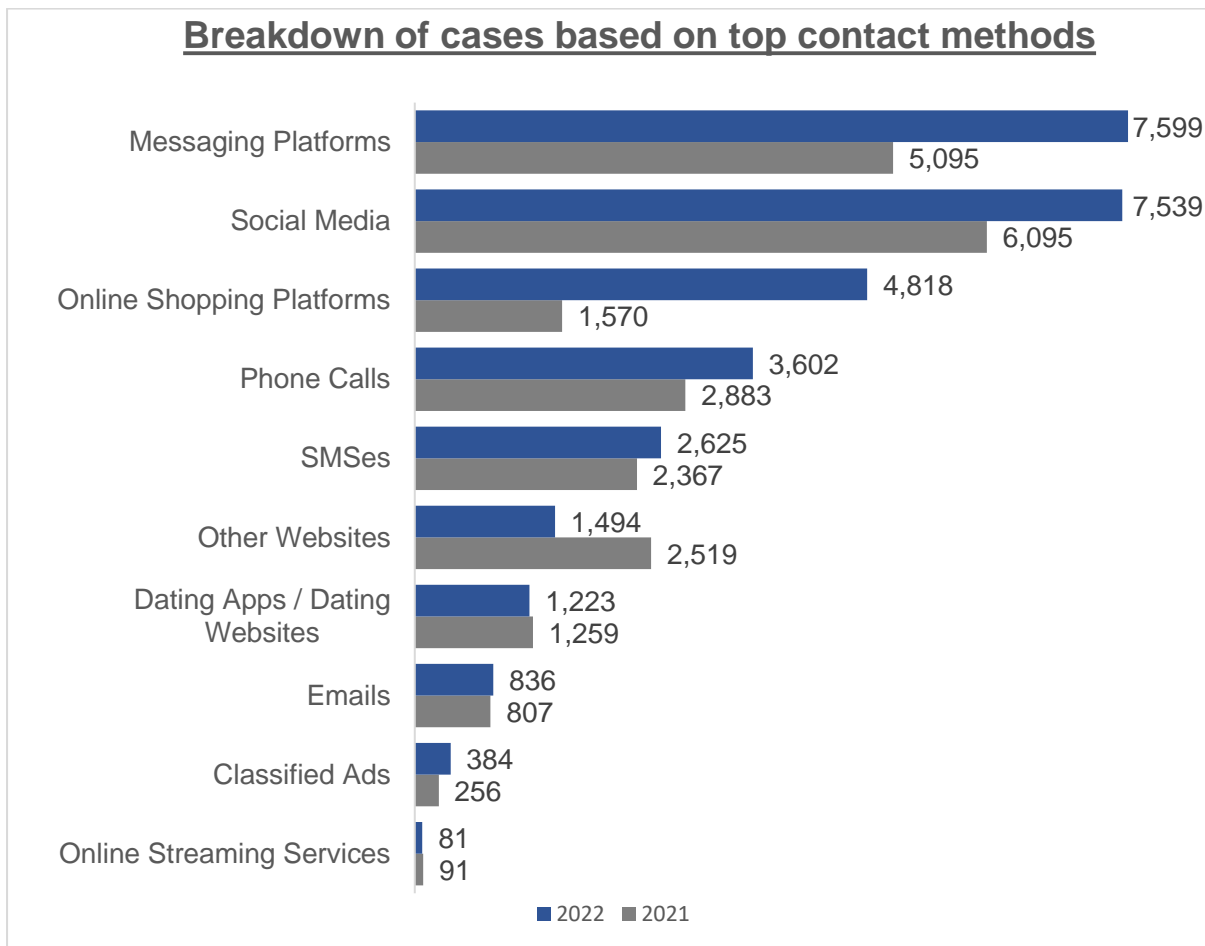
- Fake friend call scams typically involve scammers contacting victims via phone calls, pretending to be the victims’ friend or acquaintance. After establishing contact, scammers would capitalise on the friendship element, and use various reasons to request for money from the victims.

Victims would end up transferring money to bank accounts belonging to unknown individuals.

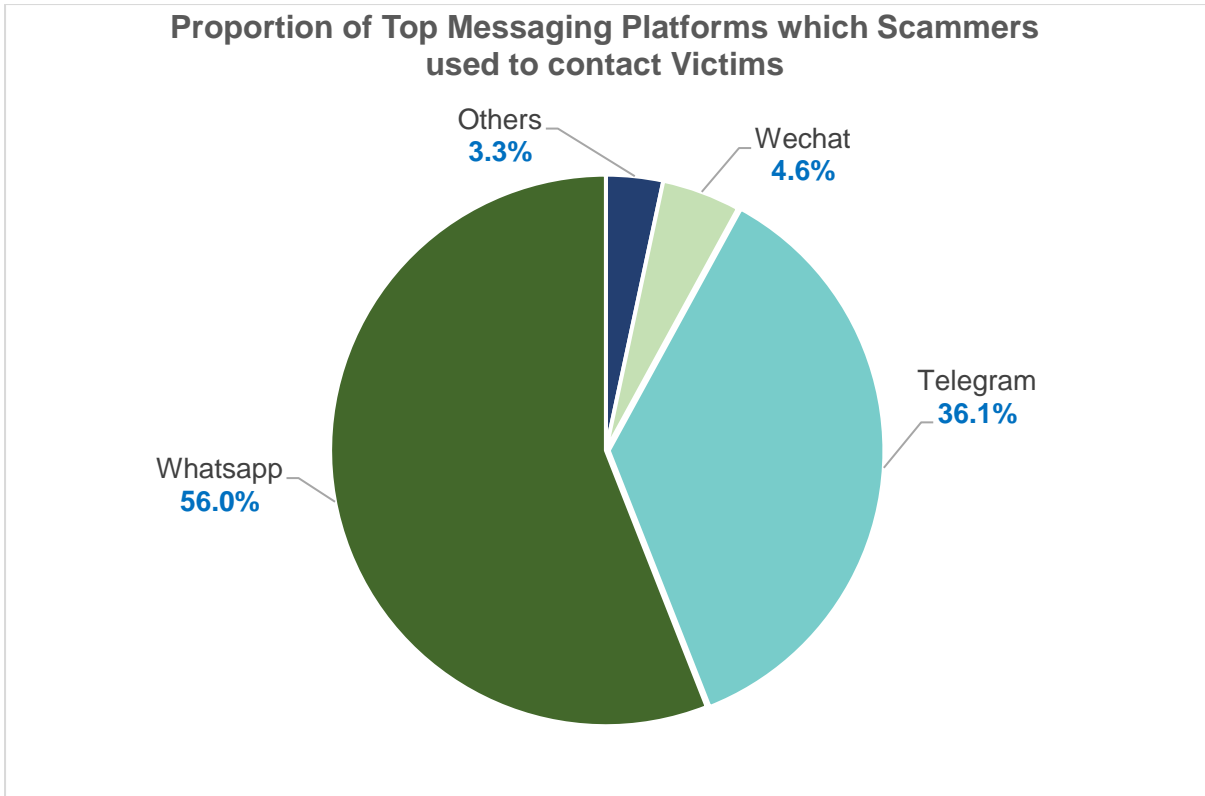
- There were 2,106 fake friend call scam cases in 2022, compared to 686 cases in 2021, an increase of 207.0%.
- The total amount reported to have been cheated increased by 95.6% to at least \$8.8 million in 2022, from at least \$4.5 million in 2021.
- Phone calls and WhatsApp were the most common channels used by scammers to contact potential victims.
- 46.3% of victims were aged between 30 and 49.

Top Contact Methods

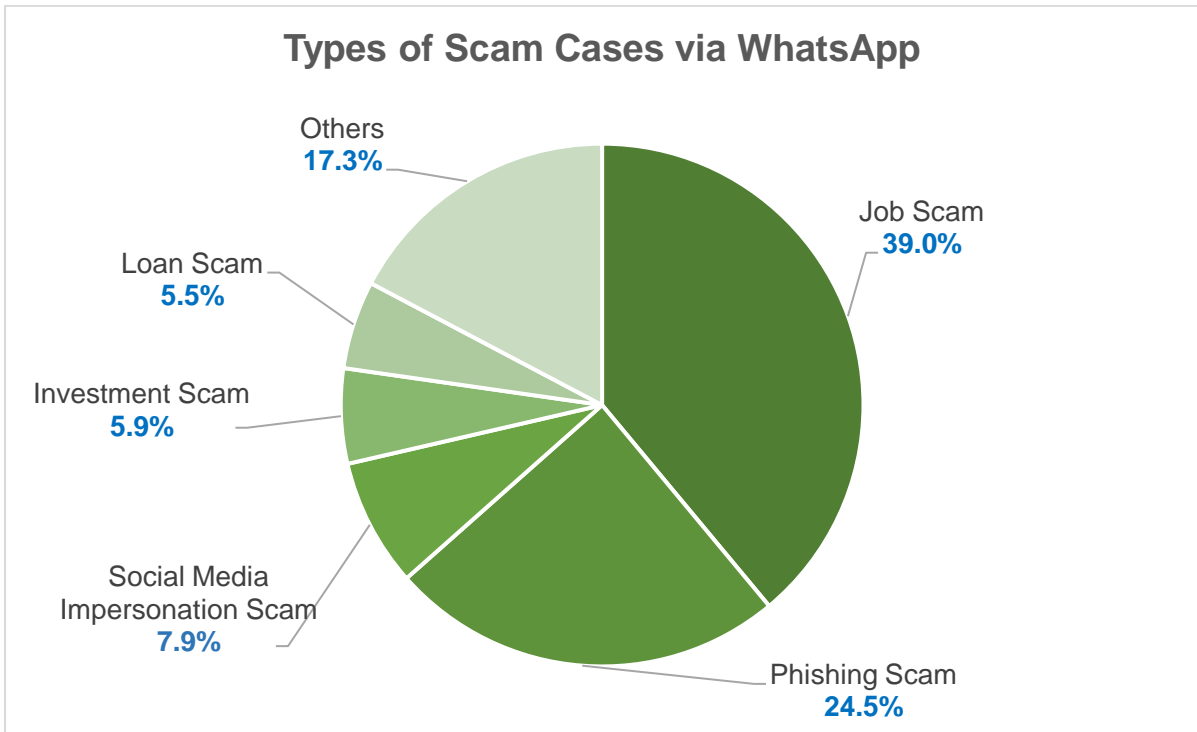
5 Scammers tend to reach out to victims through messaging platforms, social media, online shopping platforms, phone calls and SMSes. These formed the top five approach methods.



6 In 2022, the number of scam cases used by scammers to contact victims via messaging platforms increased to 7,599 from 5,095 in 2021, with about 56.0% of the cases via WhatsApp, and 36.1% via Telegram.

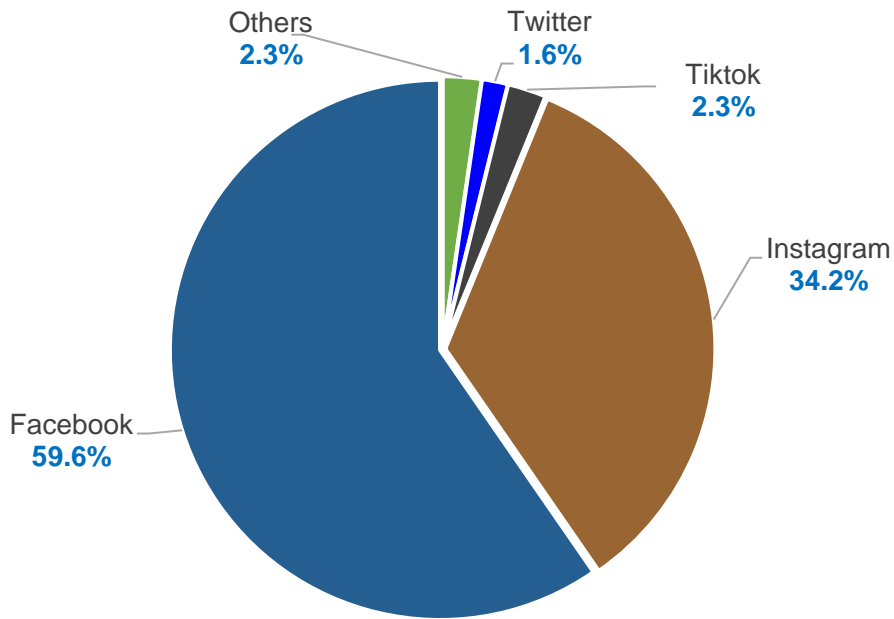


7 Among the scam cases which scammers used to contact victims via WhatsApp, 39.0% were job scams, 24.5% were phishing scams and 7.9% were social media impersonation scams.



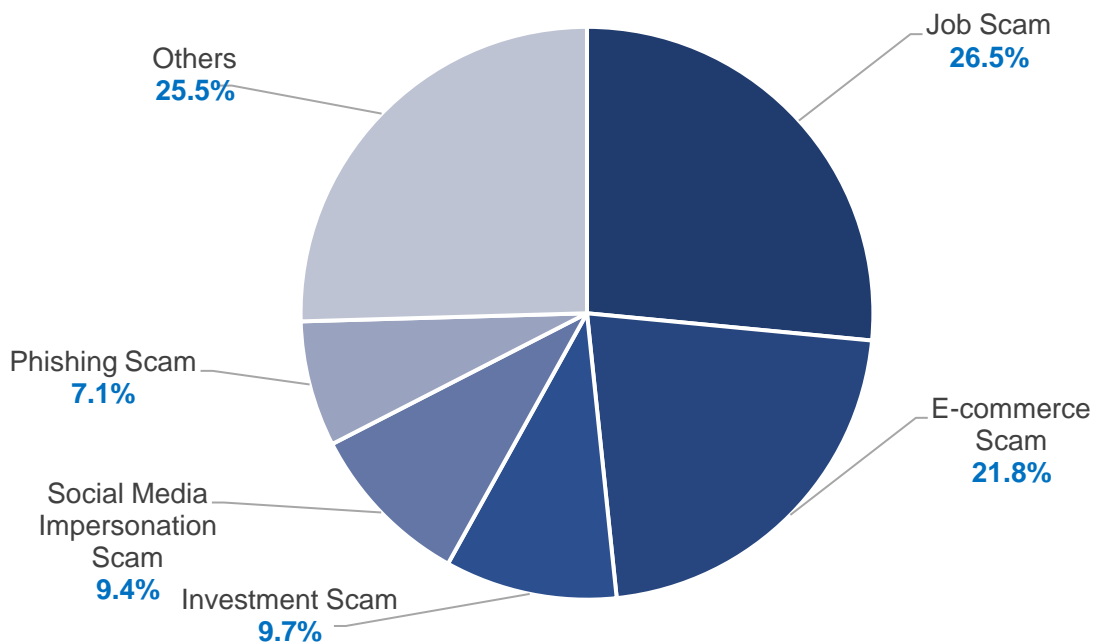
8 The number of scam cases which scammers used to contact victims via social media increased to 7,539 in 2022, from 6,095 in 2021, with about 59.6% on Facebook, and 34.2% on Instagram.

Proportion of Top Social Media Platforms which Scammers used to contact Victims

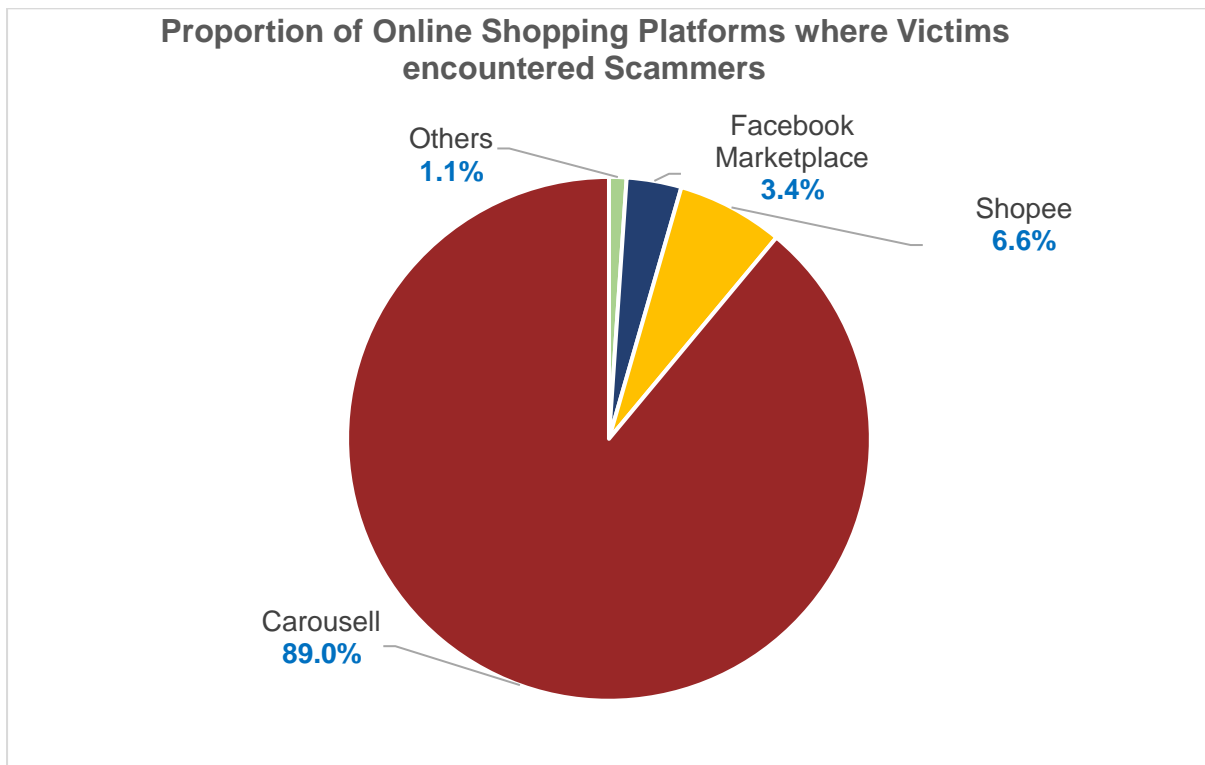


9 Among the scam cases which scammers used to contact victims via Facebook under social media, 26.5% were job scams, 21.8% were e-commerce scams and 9.7% were investment scams.

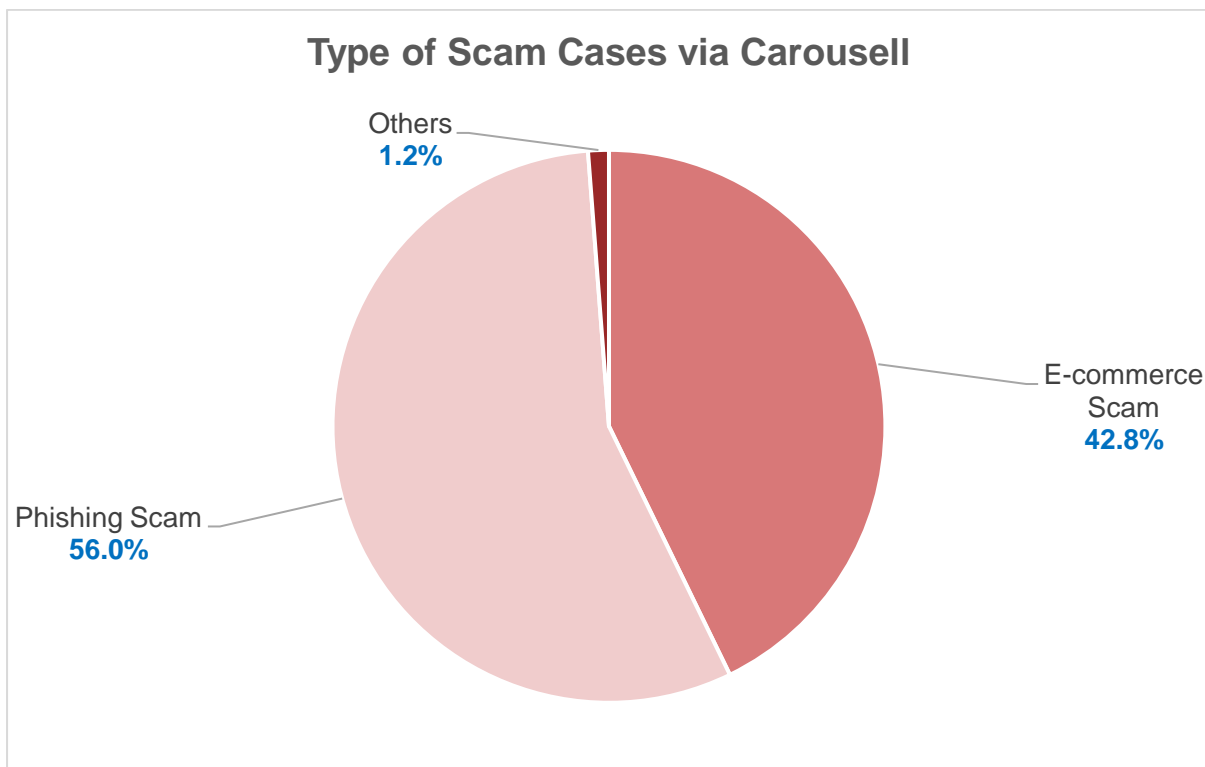
Type of Scam Cases via Facebook



10 Another contact method of concern is online shopping platforms. There was an increase in the number of scam cases to 4,818 in 2022 from 1,570 in 2021, with 89.0% of the cases where victims encountered scammers on Carousell and 6.6% on Shopee.



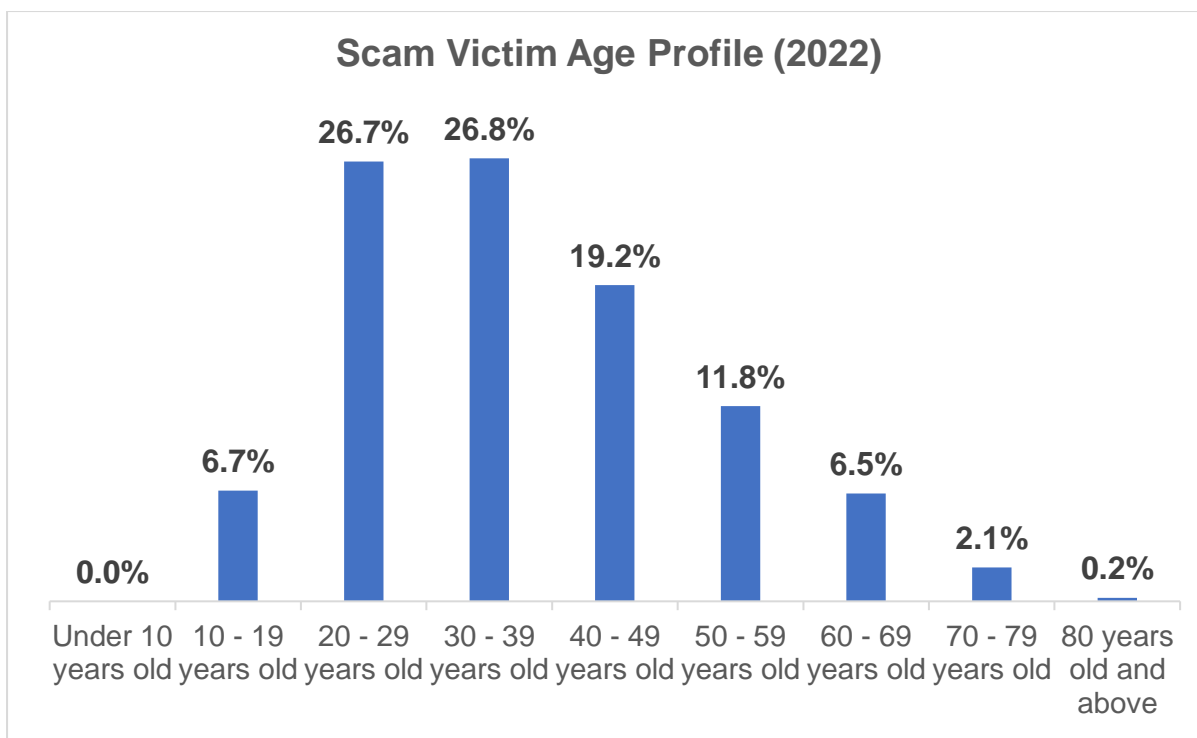
11 Among the scam cases which victims encountered scammers via Carousell, 56.0% were phishing scams and 42.8% were e-commerce scams.



Scam Victim Profile

12 Young adults are most likely to fall for scams. The breakdown of scam victims by age group is as follows:

- a) Youths, aged 10 to 19, made up 6.7% of the total number of scam victims. 21.8% from this age group fell prey to social media impersonation scams, while 21.7% fell prey to phishing scams and 20.3% fell prey to e-commerce scams. Scammers tend to contact youths via messaging platforms, social media, and online shopping platforms.
- b) Young adults, aged 20 to 29, made up 26.7% of the total number of scam victims. 27.2% from this age group fell prey to job scams, while 20.2% fell prey to e-commerce scams and 17.6% fell prey to phishing scams. Scammers tend to contact young adults via social media, messaging platforms, and online shopping platforms.
- c) Young adults, aged 30 to 39, made up 26.8% of the total number of scam victims. 24.8% from this age group fell prey to job scams, while 22.6% fell prey to phishing scams and 18.3% fell prey to e-commerce scams. Scammers tend to contact this victim group via social media, messaging platforms, and online shopping platforms.
- d) Adults, aged 40 to 49, made up 19.2% of the total number of scam victims. 26.8% fell prey to phishing scams while 17.7% fell prey to job scams and 13.8% fell prey to e-commerce scams. Scammers tend to contact this victim group via messaging platforms, social media and phone calls.
- e) Adults, aged 50 to 59, made up 11.8% of the total number of scam victims. 26.4% from this age group mainly fell prey to phishing scams, while 13.7% fell prey to job scams and 12.4% fell prey to fake friend call scams. Scammers tend to contact this victim group via messaging platforms, social media and phone calls.
- f) The elderly, aged 60 and above, made up 8.8% of the total number of scam victims. 22.7% from this age group fell prey to phishing scams, while 14.2% fell prey to fake friend call scams and 10.9% fell prey to investment scams. Scammers tend to reach out to the elderly via messaging platforms, phone calls, and social media.



Police's Efforts to Fight Scams and Cybercrimes

Enforcement

a) Strong public-private partnership to cripple scam operations

13 On 22 March 2022, the Commercial Affairs Department (CAD) operationalised the Anti-Scam Command (ASCom) for greater synergy among various scam-fighting units, by bringing scam investigation, incident response, intervention, enforcement and sense-making under a single Command. The ASCom comprises the Anti-Scam Centre (ASC), and three Anti-Scam Investigative Branches, and oversees the Scam Strike Teams situated within each of the seven Police Land Divisions.

14 The co-location initiative started in October 2019, with DBS being the first bank to station a member of staff at the ASCom. Subsequently, HSBC, Standard Chartered Bank and UOB joined the initiative in July 2022, and CIMB and OCBC joined in August 2022. Since August 2022, GovTech has also co-located their staff within the ASCom to enhance real-time coordination with SPF in investigative efforts in Singpass-related scams. The co-location allows enhanced real-time coordination with SPF in investigation, tracing the flow of funds, and swift freezing of bank accounts suspected to be involved in scammers' operations, and enables SPF to leverage Singpass' fraud analytics capabilities to identify and flag unusual account activities. In 2022, the ASCom froze more than 16,700 bank accounts based on reports referred to the ASC and recovered about \$146.6 million.

15 In May 2022, the strong public-private partnership involving ASCom and DBS led to the recovery of USD 11.5 million, the largest amount recovered from a single scam arrangement to date. Four overseas victims had fallen prey to 'Business Email

Compromise', which were spoofed emails purporting to be from the victims' business clients. As a result, the victims were defrauded into making large transactions amounting to USD 15.5 million to bank accounts held with DBS. Upon receipt of the report, ASCom worked immediately with DBS to conduct fund flow tracing, which led to the swift recovery of some of the funds.

b) Other law enforcement interventions

16 The ASC also works closely with local telecommunication companies to terminate mobile lines which are found to have been used for scams. The ASC also works closely with social media platforms and online marketplaces to remove suspicious accounts and advertisements. In 2022, more than 6,500 such mobile lines were terminated, and more than 3,100 online monikers and advertisements involved in suspected scams were removed. The ASC also engaged WhatsApp on more than 22,800 WhatsApp lines which were believed to be used in scams in 2022.

17 In January 2022, SPF conducted simultaneous raids targeting 17 handphone shops in a nine-hour island wide operation to target those who fraudulently exploit registered prepaid SIM cards as an anonymous channel of communications for illicit activities such as unlicensed moneylending, scams, and vice. Ten persons were arrested for their suspected involvement in fraudulently registering prepaid SIM cards using the particulars of unsuspecting customers or foreigners who have not entered or have left Singapore. 24 others are assisting with investigations.

18 SPF continues to take tough anti-scam enforcement actions against local scammers and money mules. In 2022, ASCom, together with the Scam Strike Teams in the seven Land Divisions, conducted 25 island wide anti-scam enforcement operations, leading to the investigation of more than 8,000 money mules and scammers.

c) Collaboration with foreign law enforcement agencies

19 The vast majority of online scams are perpetrated by scammers based outside Singapore. Such cases are difficult to investigate and prosecute. The success of our efforts to solve these cases will depend 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. Where monies have been transferred outside Singapore, recovery is very difficult. 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.

20 In 2022, the close collaboration between SPF and overseas law enforcement agencies led to the successful take-down of 13 scam syndicates comprising six job scam syndicates, three government officials impersonation scam syndicates, two phishing scam syndicates and two Internet love scam syndicates. More than 70 persons based overseas, who were responsible for more than 280 cases, were arrested.

21 In November 2022, SPF successfully brought back one individual who was involved in perpetrating scams targeting Singaporeans from Malaysia. The individual was responsible for procuring Singapore bank accounts through various chat platforms such as Telegram and Facebook, and the bank accounts were subsequently used to launder the syndicate's criminal proceeds, which were linked to scams targeting more than 50 victims of investment scams, job scams, fake friend impersonation scams, government official impersonation scams and job scams reported in Singapore, with total losses of more than S\$3.7 million.

Engagement

a) Proactive intervention for scam victims

22 The ASCom focuses on upstream interventions to disrupt scammers' operations and leverages technology to strengthen its sense-making capabilities. For example, the analysis of information submitted allows the detection of potential victims and alerts them to the danger before they fall prey to the scams. In 2022, the ASCom conducted more than 11,100 interventions and managed to alert these scam victims before they themselves realised that they were being scammed.

23 In November 2022, SPF developed a 30-second video based on the latest scam trends to spread scam awareness via communication channels such as WhatsApp and Telegram. As WhatsApp and Telegram are the top contact methods used by scammers, SPF produced and disseminated short videos with screenshots of scammers' exact messages and Police advisories to members of the public via the same medium. To date, the videos have reached more than 900,000 members of the public.

24 SPF will explore more ways to reach the public and prevent potential victims from being scammed.

25 Please see **Annex B** for comments from the Director of the Commercial Affairs Department.

Education

a) Continued public education efforts to raise awareness on scams

26 To educate the public, SPF and the National Crime Prevention Council (NCPC) proactively disseminate information and advisories on scams and highlight successful prosecutions on a regular basis. For example, NCPC's 'CrimeWatch' programme features a regular 'Scam Alert' segment which highlights topical scams and provides prevention tips to viewers. In addition, NCPC regularly shares scam prevention tips and advisories with the public through various social media and messaging platforms. NCPC has commissioned various media pieces to share crime prevention tips with members of the public and educate them on scam signs to look out for.

27 SPF formalised an e-Shoppers on Watch interest group under the Cyber category of the Community Watch Scheme (CWS). The interest group aims to harness community spirit to share relevant crime information they come across with SPF and

share crime-related advisories from SPF with their loved ones to prevent them from being victims of crime, and remind them to be vigilant. As of 16 December 2022, there are more than 4,300 CWS members under the e-Shoppers on Watch interest group. Curated scam advisories which target the top five scam types are shared with these members on a monthly basis to raise awareness on the latest scam information. SPF also partners other Government agencies to reach out to the wider community, through disseminating timely crime prevention advisories via their various outreach platforms.

28 SPF has also collaborated with other stakeholders to educate the public on scams. Between September and December 2022, SPF worked with Shopee to develop an interactive in-app game in the form of an anti-scam quiz with sound effects and attractive visuals. Consumers who participated in the game by answering questions on a variety of scams prevalent in Singapore were rewarded with Shopee coins, vouchers, and other attractive prizes.

29 Since November 2021, SPF has worked with iJooz company to display anti-scam messages on 473 vending machines island-wide and distributed 500,000 cups with printed anti-scam messages. In April 2022, SPF collaborated with Canadian Pizza to include anti-scam messages on their various marketing platforms such as website, pizza boxes and flyers. SPF will work with more stakeholders to increase scam awareness and better safeguard our community against the scourge of scams.

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

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

31 E-commerce marketplaces are assessed based on the number of safety features that they adopt to ensure (a) user authenticity, (b) transaction safety, (c) availability of loss remediation channels for consumers, as well as (d) the effectiveness of their anti-scam measures. The safety features that are used in the assessment are based on the guidelines in the Technical Reference 76 “Guidelines for Electronic Commerce Transactions” published by the Singapore Standards Council. E-commerce marketplaces that adopt all the necessary safety features will score a maximum of four ticks. As at October 2022, the e-commerce marketplaces were rated as follows:

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

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

ScamShield mobile application by NCPC and GovTech

33 The ScamShield mobile app, jointly developed by NCPC and GovTech, identifies and filters out scam messages using artificial intelligence. It also blocks calls from phone numbers that were used in other scam cases or reported by ScamShield users. These two functions reduce opportunities for scammers to reach out to potential victims.

34 The ScamShield app for iOS and Android was launched on 20 November 2020 and 28 September 2022 respectively.

35 As at 31 December 2022, the ScamShield app has been downloaded by close to 500,000 users. More than 7.4 million SMSes have been reported as potential scams, and more than 47,000 unique scam-tainted phone numbers have been blocked.

'I Can ACT Against Scams' campaign by NCPC

36 On 18 January 2023, NCPC, in collaboration with MHA and SPF, launched the 9th edition of the anti-scam campaign at the *Scaminar! ACT Against Scams* event. The "I Can ACT Against Scams" campaign aims to educate and encourage members of the public to translate scam awareness into action by proactively adopting anti-scam measures. The word "ACT" in the campaign headline stands for "Add. Check. Tell" – the three main actions that individuals should proactively take to safeguard themselves and our community against scams. Please see **Annex C** for the campaign visuals.

- **Add** security features such as ScamShield and enable 2-Factor Authentication for personal accounts.
- **Check** for potential scam signs by asking questions, fact checking requests for personal information and money transfers, and verifying the legitimacy of online listings and reviews. When we receive an SMS or message asking us to click on a URL link and requesting for our personal or banking information, take time to pause and check if the SMS or message is legitimate.
- **Tell** the authorities and platform owners about your scam encounters. We can play our part by reporting them to the bank, via ScamShield, or filing a Police report as soon as possible. The faster scams are reported to the authorities and the platforms, the faster they can take action to prevent more people from falling prey. Tell others also about ongoing scams or preventive steps they can take.

37 Please see **Annex D** for comments from the Vice-Chairman of NCPC.

Implementation of SMS Sender ID Registry and SMS anti-scam filtering solutions by IMDA

38 The Infocomm Media Development Authority (IMDA) has implemented two new measures in their effort to fight scams.

Full SMS Sender ID Registration

39 First, registration with the Singapore SMS Sender ID Registry (“SSIR”) is now mandatory for all organisations that use SMS Sender IDs. This means only bona fide Sender IDs belonging to organisations, and registered with the SSIR, will be allowed. All other Sender IDs will be blocked. The full registration requirement took effect on 31 January 2023. This is a further step forward from the previous voluntary registration regime in building stronger anti-scam capabilities. IMDA notes the support for the proposal by both the public and merchants.

40 As some organisations may need more time to prepare and register for Sender IDs, their SMS cannot be clearly differentiated from other SMS that come from unknown sources and may be scam messages. Therefore, as a transition measure, all non-registered SMS Sender-IDs will be channelled to a Sender ID with the header “Likely-SCAM”. This is akin to a “spam filter and spam bin” and will be in place for around six months. Consumers are advised to exercise caution upon receiving such SMS as these are non-registered Sender IDs. Merchants are also urged to have their Sender IDs registered as early as possible with the SSIR.

Anti-Scam SMS Filtering Solutions

41 Second, telecom operators will implement SMS anti-scam filtering solutions within their mobile networks, to automatically filter potential scam messages before they reach consumers. This is part of the multi-pronged effort by IMDA and other stakeholders to further safeguard SMS as a communications channel.

42 Automated machine-scanning and pattern recognition technology have made it possible to identify and filter potential scam messages upstream. Specifically, these solutions can detect malicious links within SMSes sent via our telecoms network. IMDA notes the public’s support for this proposal. Mobile operators such as Singtel, Starhub, and M1 have implemented anti-scam filtering solutions in their networks.

Additional anti-scam measures by MAS

43 In 2022, the Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS) introduced two rounds of anti-scam measures to strengthen the security of digital banking.¹ Banks have removed all clickable links in emails or SMSes sent to retail customers and introduced an emergency self-service “kill switch”

¹ [MAS and ABS Announce Measures to Bolster the Security of Digital Banking, 19 January 2022](#) and [Additional Measures to Strengthen the Security of Digital Banking, 2 June 2022](#).

which will give customers a way to suspend their accounts quickly if they suspect that their bank accounts have been compromised.

44 Apart from staying vigilant, the ABS' Standing Committee on Fraud, comprising the major retail banks, will continue to evaluate and improve the suite of measures in place to tackle digital banking scams as they evolve.

Fraud surveillance capabilities for Government agencies and strengthening Singpass against phishing by SNDGG

45 Government agencies will only send links ending with "gov.sg", so that members of the public can easily identify trusted links. The public should only log in to Government services on legitimate Government websites with domains ending with "gov.sg". However, there are exceptions for websites that are collaborations between Government agencies and non-Government entities. These legitimate websites are listed on www.gov.sg/trusted-sites, which members of the public are encouraged to check against if they are asked to transact on unfamiliar website domains.

46 Government agencies have also been using the Singpass Inbox in the Singpass application to securely disseminate public announcements, and reminders of renewal of personal documents like the passport.

Security enhancements in Singpass

47 As part of the Government's continuous effort in tackling cybercrimes, the Smart National and Digital Government Group (SNDGG) has introduced a series of measures such as additional security verifications for higher risk transactions with Singpass, and stepped-up cybercrime detection and investigation procedures.

a) Introducing additional security verification in Singpass

48 SNDGG continuously enhances Singpass' threat detection and login security in response to and in anticipation of evolving scams. For instance, users may be required to perform an additional security verification using Singpass Face Verification for higher risk Singpass transactions, e.g., setting up their Singpass app. Their face scan is compared against the Government's database to authenticate the user, as an additional measure to mitigate impersonation scams and prevent unauthorised access to their Singpass account.

b) Stepping up scam detection and improving incident reporting

49 Since September 2022, the Singpass hotline has been extended to provide 24/7 scam support to users who need to report any suspicious account activity.

Singpass users can call the official Singpass hotline at 6335 3533 and press “9” to access this service.

Internet Hygiene Portal

50 In October 2022, the Cyber Security Agency of Singapore (CSA) launched the Internet Hygiene Portal (IHP). The Portal is a one-stop platform for enterprises to access resources and self-assessment tools, to enable them to adopt internet security best practices.²

51 The IHP also provides visibility on the cyber hygiene of digital platforms, by publishing an Internet Hygiene Rating table with a simplified view of each digital platform’s internet hygiene.³ This is aimed at helping consumers make informed choices to better safeguard their digital transactions from cyber threats.

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 such as banks, online marketplaces and telcos in particular have a responsibility to prevent, deter and detect crimes committed through their platforms. Putting in place anti-scam measures and precautions against crimes will help keep their customers safe.

**PUBLIC AFFAIRS DEPARTMENT
SINGAPORE POLICE FORCE
8 FEBRUARY 2023**

² <https://ihp.csa.gov.sg>

³ <https://ihp.csa.gov.sg/information-resources/ihr-ecommerce>

Annex A

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

Types of Scams	Cases Reported		Total Amount Reported to Have Been Cheated (at least)	
	2022	2021	2022	2021
Phishing Scam	7,097	5,023	\$16.5M	\$34.8M
Job Scam	6,492	4,550	\$117.4M	\$91.0M
E-Commerce Scam	4,762	2,729	\$21.3M	\$5.9M
Investment Scam	3,108	2,467	\$198.3M	\$190.2M
Fake Friend Call Scam	2,106	686	\$8.8M	\$4.5M
Social Media Impersonation Scam	1,696	1,614	\$3.7M	\$5.5M
Loan Scam	1,031	2,273	\$9.3M	\$18.3M
Internet Love Scam	868	1,094	\$35.7M	\$46.6M
Government Officials Impersonation Scam	771	750	\$97.6M	\$106.3M
Credit-For-Sex Scam	626	628	\$2.1M	\$1.3M
Top 10 scams	28,557	21,814	\$511.3M	\$504.8M

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

Annex B

Quote by Director of Commercial Affairs Department

To combat the rise in scam cases, the Police have collaborated with other Ministries and agencies in a whole-of-government effort to roll out various upstream and downstream initiatives.

Since the operationalisation of the Anti-Scam Command in March 2022, we have frozen more than 16,700 bank accounts, and recovered more than S\$146 million of scam proceeds in 2022 alone.

I would also like to thank the community for their support in combatting scams. In 2022, we recognised 45 organisations for their swift intervention as well as their close collaboration with the Police in developing and implementing enforcement and crime prevention initiatives to combat scams.

Fighting scams is a community effort. The Police will continue to work closely with other Government agencies and private stakeholders to strengthen our public education and awareness efforts, to better protect the public against scams.

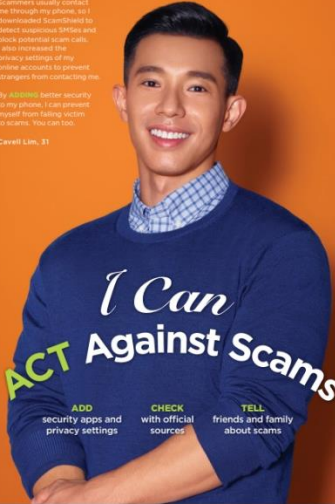
*– Mr. David Chew
Director of Commercial Affairs Department*

Annex C

Scammers usually contact me through my phone, so I downloaded ScamShield to detect suspicious letters and block potential scam calls. I also increased the privacy settings of my online accounts to prevent strangers from contacting me.

By **ADDING** better security to my phone, I can prevent myself from being victim to scams. You can too.

Carroll Lim, 31







I Can ACT Against Scams

ADD security apps and privacy settings

CHECK with official sources

TELL friends and family about scams

SPOT THE SIGNS. STOP THE CRIMES.    

Sometimes it's hard to spot a scam. So I always verify with people I trust, and visit official websites for updated information on scams.

By **CHECKING** with official sources, I can protect myself from scams. You can too.

Norliah Ahmad, 69



I Can ACT Against Scams

ADD security apps and privacy settings

CHECK with official sources

TELL friends and family about scams

SPOT THE SIGNS. STOP THE CRIMES.    

To protect my friends and family from scams, I share the latest scam alerts with them and report scam encounters to the authorities.

By **TELLING** my loved ones and the authorities about scams, I can prevent others from falling prey to scams. You can too.

Sofea Shakir Marican, 24



I Can ACT Against Scams

ADD security apps and privacy settings

CHECK with official sources

TELL friends and family about scams

SPOT THE SIGNS. STOP THE CRIMES.    

Annex D

Quote by Vice-Chairman, National Crime Prevention Council

We are losing millions of dollars to scams every month. Any one of us can be a scam victim, but if we stand together, we can fight scams effectively. Do not hesitate, ACT now — download the ScamShield app on your mobile phone to block calls and SMSes from scammers; learn the latest scam trends and share them with friends and family; look out for scam signs before responding; and report to the Police immediately if you have been scammed. Do not let the scammers win.

- Mr. Tan Puay Kern

Vice-Chairman, National Crime Prevention Council