

Let's ACT Against Scams

Stories from our Community



CONTENT PAGE

| | |
|---|----|
| Foreword | 03 |
| Welcome Message | 04 |
| A Note about the eBook | 05 |
| Scam Trends | 06 |
| ACT Against Scams | 08 |
| Story 1: "A Tempting Offer" | 09 |
| Story 2: "Within Minutes" | 10 |
| How to Download ScamShield | 11 |
| Story 3: "Fake Love" | 13 |
| Story 4: "I Didn't Order Anything" | 14 |
| How to Spot Phishing Scams | 15 |
| Story 5: "Grandma, Help Me!" | 17 |
| Story 6: "Remember Me?" | 19 |
| How to Check and Verify | 20 |
| Story 7: "I Won't Fall for a Scam!" | 21 |
| Story 8: "A Get-Rich-Quick Offer" | 23 |
| How to Know if a Loved One is Being Scammed & Convince them | 24 |
| Helpful Resources | 26 |
| FAQ | 29 |
| References | 30 |
| About HTBSC and OCP | 31 |

FOREWORD

Scams continue to be a real and persistent threat to our society, affecting the young and elderly, students and working adults alike. No one is spared from the scourge of scams. Government agencies are partnering with corporates to scale up infrastructure and system protections. But scammers continue to evolve their methods, coming up with new scams to target more victims. The impact of scams on individuals and society is huge and wide-ranging. They exact a financial and emotional toll on victims and their families. This eBook has compiled stories of scam victims, near misses and guardians who have protected others.

By studying these stories and sharing them, we help to protect and empower those around us as we can learn from the experiences of those who have been impacted by scams, and better understand the ways scammers prey on our human tendencies. Fighting scams is a community effort. We can learn from one another to better protect ourselves and our loved ones. Together, let's ACT against scams.

Fighting scams is a community effort – let's ACT against scams!

Ms Sun Xueling

Minister of State

Ministry of Home Affairs & Ministry of Social and Family Development

Chairperson, Inter-Ministry Committee on Scams

WELCOME MESSAGE



With great pleasure, I introduce the 'Let's ACT Against Scams: Stories from our Community' eBook to you. This eBook uncovers the current scam landscape in Singapore through the stories of scam victims, near misses, and guardians in our society. Beyond financial loss, scams can also cause adverse emotional and psychological costs. Fostering an understanding and supportive community is crucial to encouraging more people to share their stories, in hopes to prevent further scam victimisation. I hope that with the stories in this eBook, more of us can start looking out for others against scams and be around to support those who are affected by scams.

Dr Majeed Khader, Ph.D
Chief Psychologist
Ministry of Home Affairs

Scams remain the main crime source in Singapore. Over 28,557 cases were reported in the entire year of 2022 alone, with total losses for top 10 scam types exceeding \$500 million. Scammers employ various tactics which are constantly evolving and we can expect scams to become increasingly more difficult to fight. Thus, we must stay ahead of the game by remaining vigilant and constantly educating ourselves on the latest trends and modus operandi used by the perpetrators. The Singapore Police Force remains committed to working closely with the community in partnership with the National Crime Prevention Council to ACT against scams.



AC Devrajan Bala
1 Deputy Director, Operations Department
Singapore Police Force

A NOTE ABOUT THE EBOOK

Scams continue to present as a real threat in Singapore, as scammers devise new ways to defraud victims. Unlike other crimes, scams present a threat to anyone, anywhere, and at any time, with scammers often mass-targeting no demographic in particular. This eBook aims to explore the experiences of scam victims, near misses, and guardians within our society. Using a storytelling approach, this eBook presents the composite accounts of individuals who have reported their scam experiences on the National Crime Prevention Council's ScamAlert website. The characters in the stories are not actual persons, but their experiences were based on real scam cases. Additionally, the images used to exemplify all story characters are purely for illustration purposes only.

We sincerely thank all members of the public who have posted their scam incidents and stories to the ScamAlert website. Through sharing their experiences, others can become aware of similar scam incidents and be better equipped to protect themselves. Let's ACT against scams together!

This is an interactive PDF! 

Look out for clickable images & links, which will guide you to other helpful resources!



Look out for the key messages highlighted in each story!



**SCAM
ALERT**

To read more stories or submit your own stories, visit:
www.scamalert.sg



GET SCAM-RELATED ADVICE:
CALL 1800-722-6688
(Mon-Fri 9am-5pm, excl. PH)



 Join **NCPC's ScamAlert Telegram** channel for the latest scam updates

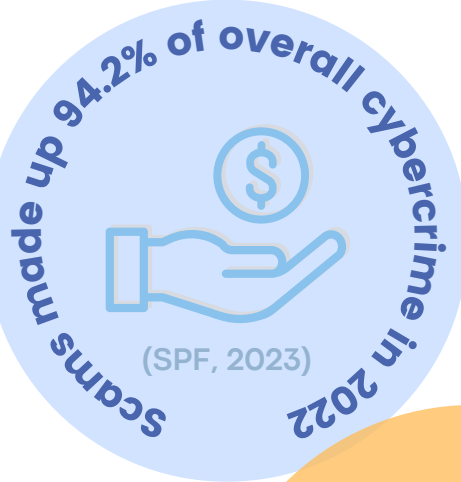
SCAM TRENDS

From 2021 to 2022, more than 50,000 scam cases were reported in Singapore, with a combined loss of more than S\$1 billion*



Singaporeans have reported high awareness of cyber safe practices, but only few adopt these practices

(CSA, 2021)



Scam Victims' Common Online Practices



Clicking pop-up ads



Opening emails from unknown senders



Clicking unfamiliar links



Signing up for "free" limited-time trial offers

(HTBSC, 2020)

30%

of victims always/often click on links without knowing what they might actually lead to

(HTBSC, 2020)

Only 38% of victims make immediate police reports

(HTBSC, 2020)



to read the "Scammer Beware" eBook, which highlights the results of the National Prevalence Survey of Scams 2020



PHISHING SCAMS

were the top scam of concern in the entire year of 2022

(SPF, 2023)

* statistics based on SPF's annual crime briefs

SCAM TRENDS

TOP 6 SCAMS FROM JAN – DEC 2022*



PHISHING SCAMS

7,097 cases

Phishing scams often use SMS or email prompts to steal personal information via fake websites that are created to look similar to official sites of organisations or banks.

JOB SCAMS

6,492 cases

Job scams are usually unsolicited and received via messaging apps, social media, or online ads. Often, potential "employers" will offer "high pay" for jobs involving little time commitment or effort.



E-COMMERCE SCAMS 4,762 cases

E-Commerce scams occur on popular online marketplaces, fake websites, or social media ads. They often offer unusually good deals, but provide little to nothing in return.

INVESTMENT SCAMS 3,108 cases

Investment scams often occur via online ads, emails, social media pages, or direct messages. Scammers set up enticing investment offers and products to encourage victims to "invest" money.



FAKE FRIEND CALL SCAMS 2,106 cases

Scammers make contact via phone calls or messaging apps, without identifying themselves. They then assume the identity of a friend that the victim guessed they were. This premise of friendship is used to seek financial "help".

SOCIAL MEDIA IMPERSONATION SCAMS 1,696 cases

Scammers impersonate you or people you know using social media accounts, and ask victims to transfer money under various pretexts such as medical emergency, join a lottery campaign, or to buy cryptocurrencies.



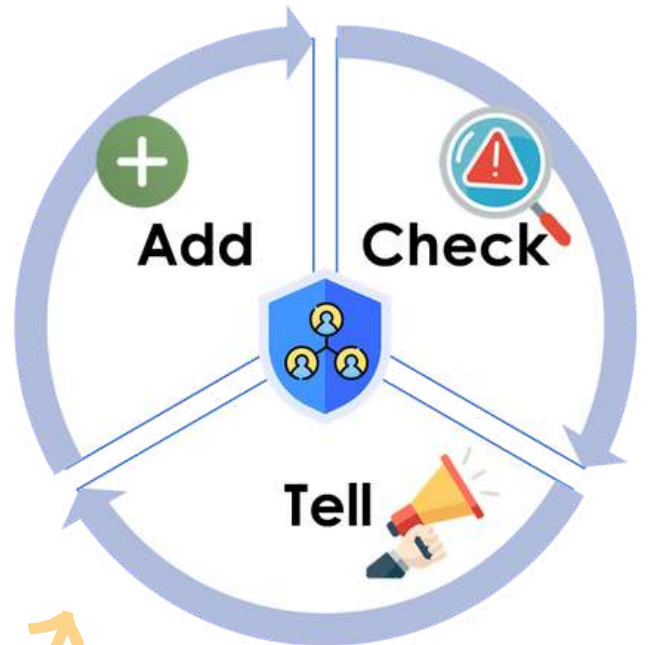
*Above statistics are sourced from Singapore Police Force's 2022 Annual Scams and Cybercrime Brief.

ACT AGAINST SCAMS



What does ACT against scams mean? Let's break it down!

ACT Against Scams refers to a set of actions we can take to reduce the likelihood of being exposed to scams and actually being scammed. It is also a call for individuals and community to start taking pro-active actions.

ACT Stands For:
Add, Check, Tell



How can we ACT?

| ADD | CHECK | TELL |
|---|---|---|
| <ul style="list-style-type: none">• ADD refers to adding hardware, software, and security settings.• For example, adding ScamShield, privacy settings, 2FA, strong passwords, and more.  | <ul style="list-style-type: none">• CHECK refers to checking with trusted others, looking out for scam signs and reconsidering decisions.• For example, slow down to think before responding to requests for money or personal information and check with trusted others or official sources. | <ul style="list-style-type: none">• TELL refers to telling authorities and our community about scam encounters promptly.• For example, telling your peers and family about scam encounters.  |



Look out for more key anti-scam ACTions throughout this eBook!

" A TEMPTING OFFER "

TARGET Siti, 24, University Student
SCAM TYPE Job Scam

Siti was having coffee with her friend Nisha after their lesson. As Siti was sharing that she wanted to look for a part-time job during the semester break, she received a notification of an incoming message from an unknown number. The message read:

"Hello, I'm Nina, Head of Recruitment at B-STAR Studios, are you looking for a job? Pay is 80-400SGD/day"

Siti smiled and excitedly showed Nisha the SMS, stating that this could be the opportunity she needed. Nisha was worried and asked Siti if she had applied for any jobs, especially with "B-STAR Studios". Siti replied, "No I haven't...but this offer sounds pretty good!". Nisha explained to Siti, "I think that's exactly what they want you to think – these unsolicited job offers are tempting so that you respond quickly without much thought. I used to get a lot of these SMSes too". Siti nodded, taking in the information, and asked, "So you don't receive offers anymore?".

Nisha pulled out her mobile phone – "Let me show you something". Nisha opened the ScamShield app on her mobile phone and explained that the app can detect and block scam messages and calls. Siti decided not to respond to the SMS, but to add ScamShield to her mobile phone instead. The next morning, Siti read the newspaper and saw an article about Job Scams, using the same kind of SMS she received the day prior. Siti reached for her mobile phone and sent Nisha a text, thanking her for protecting her from a job scam.



Unsolicited job offers appear tempting, they are designed to make you respond quickly without much thought
Let's slow down and CHECK!

"WITHIN MINUTES"

| | |
|------------------|---------------------------|
| TARGET | Ahmed, 29, Migrant Worker |
| SCAM TYPE | Impersonation Call |

Ahmed was enjoying a meal with his co-workers. His mobile phone started ringing with a call from an unknown number. He decided to pick it up, in case it was important. The caller claimed to be "Mr Zhou" from ICA Singapore. Mr Zhou claimed that Ahmed's work permit would be cancelled next week if he didn't pay a renewal fee of \$800.

Ahmed was confused to hear this as this was the first time "ICA" had ever contacted him in such a manner. But the caller knew Ahmed's name and contact number, so he was worried that his permit might actually be cancelled if he didn't pay the fee! "How can I verify you are from ICA?" Ahmed asked, doubting that a real ICA officer would speak so aggressively. The caller responded agitatedly, "This is no way to talk to someone handling your permit! If you don't believe me then I'll cancel your work permit!".

Sensing something was amiss, Ahmed hung up the call and used Google to search "ICA number". He dialled one of the numbers listed on ICA's official website to speak to an ICA officer. The officer confirmed it was a scam call and commended Ahmed for doing the right thing.

Within minutes, Ahmed had saved himself from potential financial loss and emotional distress. Ahmed decided to immediately tell his co-workers about the experience, to make sure they wouldn't fall prey to the same scam. He also blocked the number from contacting him again.



How to Download & Use ScamShield

FOR IOS

DOWNLOAD

Open "App Store" on your iPhone and search for "ScamShield". Select "Get" and enter your Apple ID password.

1

OR Scan the QR Code below (bottom left)



ALLOW ACCESS

2

Once ScamShield is downloaded, open the app and select "Allow" for ScamShield to work on your device.

To Enable Call Blocking...

- Open the "Settings" app
- Select "Phone"
- Select "Call Blocking & Identification"
- Swipe to enable ScamShield

3



REPORT

4

If you receive any scam messages, you can report them using ScamShield's in-app reporting function. Open the app and select the "Report" button at the bottom of the screen.



SCAN TO DOWNLOAD
ScamShield ON IOS



For more information on ScamShield go to
www.scamshield.org.sg/setup-guide/

How to Download & Use ScamShield

FOR ANDROID

DOWNLOAD

Open "Google Play Store" on your mobile phone. Search for "ScamShield" and select "Install".

1

OR Scan the QR Code below (bottom left)



ALLOW ACCESS

2

Once ScamShield is downloaded, open the app and select "Allow" for ScamShield to work on your device.

To Enable Call Blocking...

- A pop-up will ask "Set ScamShield as your default caller ID and spam app?"
- Select "ScamShield"
- Then select "Allow"

3



REPORT

4

If you receive any scam messages, you can report them using ScamShield's in-app reporting function. Open the app and select the "Report" button at the bottom of the screen.



SCAN TO DOWNLOAD
ScamShield ON ANDROID



For more information on ScamShield go to
www.scamshield.org.sg/setup-guide/

"FAKE LOVE"

TARGET Ian, 21, Student
SCAM TYPE Internet Love Scam

Ian was checking his mobile phone after work. He was excited to see he had been matched with a young woman - "Lisa" - on a dating app. She looked beautiful in her profile picture and he was excited to contact her. Lisa messaged first - "Hey handsome, nice profile". Ian responded quickly and after a few messages Lisa asked - "What is your WhatsApp number? Let's take this somewhere private..." Ian hesitated as he had just e-met Lisa, but he went along as he was interested in Lisa.

LISA

Hey handsome, nice profile

IAN

Hey! Whats up? 😊

LISA

What's your WhatsApp number?

Let's take this somewhere private...

On WhatsApp, Lisa expressed she was having trouble fulfilling an online order. She asked Ian for "help" in fulfilling the online order from an unfamiliar website - "myseresa.com". Ian felt suspicious, given that he hardly knew Lisa but she was already asking him for favours.

Before responding to her request, Ian recalled seeing posters about love scams in the MRT, showcasing a similar scenario. With a quick Google search for "love scam posters", Ian found NCPCC's ScamAlert website was at the top of his search. He clicked through the website and found numerous stories from real scam victims. Reading the stories, Ian realised "Lisa" was using the same trick on him! Ian blocked "Lisa" on WhatsApp and reported the incident to the dating app. He felt grateful that he took the time to access the resources available to avoid being scammed.



Use ScamAlert resources to CHECK and TELL your experiences!

ScamAlert Hotline: **1800-722-6688**

ScamAlert Website: **www.scamalert.sg**



(©[RyanKing999] via Canva.com)

"I DIDN'T ORDER ANYTHING"

TARGET Mr Guo, 60, Retiree
SCAM TYPE Phishing Scam

Mr Guo and his wife were at home when he noticed a notification on his mobile phone. He had just received an email from "FedEx". The email seemed official and stated:

"Dear Customer, your parcel (#74259UHS) is awaiting delivery. To fulfil outstanding payment for delivery, please visit the [Uniform Resource Locator website](#). Thanks, FedEx Team."

Mr Guo didn't remember ordering anything as he seldom shopped online. He wondered whether someone else had placed the order. He asked his wife – she hadn't ordered anything either. Given that neither of them had placed an order, the couple decided to call their son and check if he had done so. Their son answered the call, confused by the question, and responded no – he hadn't.

Mr Guo decided to call FedEx to check. He searched for the official FedEx website through Google and called the official number listed on the website. Upon checking with FedEx, Mr Guo learned that he had received a phishing email. He decided to block and report the scam email, feeling glad that he had checked first.

Over dinner with some friends that night, Mr Guo told his friends about the incident and reminded them to be careful. One of Mr Guo's friends also suggested changing the settings on his email account to make sure spam/scam messages go straight to the "Junk" folder.



Do not click on any links in unsolicited emails, SMSes, or direct messages. When in doubt, CHECK with others.

DID YOU KNOW?



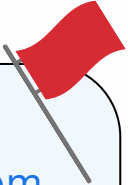
In 2021, roughly 55,000 unique phishing URLs were found to be containing a Singapore link (CSA, 2021)

How to CHECK for Email Phishing Scams



CHECK THE EMAIL ADDRESS

- 1** Legitimate organisations do not:
1. Use external email domains (e.g. Gmail, Hotmail).
 2. Have spelling errors in their email address.

- 
1. amazon@gmail.com
 2. amazonamazzon.com

SPOT SUSPICIOUS LINKS

- 2** Before clicking any links, hover your mouse over the link - it will display the REAL URL!

CLICK HERE:
www.secureURL.com



www.scamURL.com

SEARCH FOR ERRORS

- 3** Illegitimate emails with phishing links often have spelling or grammatical errors. They may not be easy to spot. So slow down and CHECK.

Dear **cardholder**,

Your card is on hold in 48hr for **suspicious** activity. Please re-login for **acount** information.

BEWARE OF URGENT REQUESTS

- 4** Scammers try to instil panic or fear by pressuring you to reply quickly, often posing as the authorities. Be wary of phrases such as "urgent action required" or "respond immediately to...".

~~URGENT~~

FAKE



Visit Cyber Security Agency's Website to learn how to protect yourself from phishing scams and other cyber threats.

How to CHECK for SMS Phishing Scams



1

CLICK HERE!

Scammers often try to get you to tap on links in SMSes by **promising you something** attractive or important (e.g., prizes, banking alerts, or delivery updates).



2

LOOK FOR URGENT REQUESTS

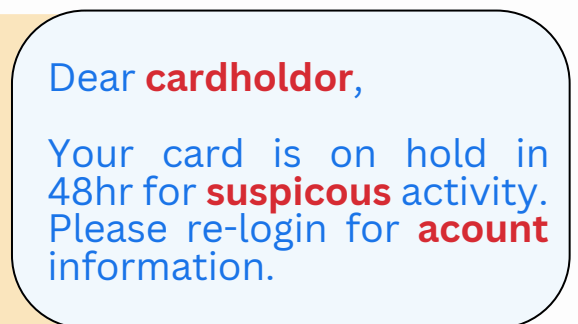
Scammers try to instil panic or fear by pressuring you to reply quickly, often posing as the authorities. Be wary of phrases such as "urgent action required" or "respond immediately to...".



3

SEARCH FOR ERRORS

Illegitimate SMSes with phishing links may include spelling or grammatical errors. They are not always easy to spot. So keep an eye out!



ADDITIONAL TIPS

DON'T OPEN ATTACHMENTS

Unexpected attachments in emails, SMSes, or via messaging apps may include malware, spyware, or viruses, that could damage or steal your data.



Ogy5.html

NO MORE CLICKABLE LINKS

As of January 2022, banks in Singapore have removed clickable links in emails and texts from banks (MAS, 2022).



Visit Cyber Security Agency's Website to learn how to protect yourself from phishing scams and other cyber threats.

"GRANDMA, HELP ME!"

TARGET Mrs Tan, 64, Retiree

SCAM TYPE Social Media Impersonation Scam

Mrs Tan was excited that her family was coming over for dinner. As she was preparing dinner, she suddenly received a Facebook Messenger notification. She immediately checked the notification and realised that her granddaughter "Cindy" had sent her a message, asking for money urgently.

Mrs Tan wondered why Cindy had messaged her using Facebook Messenger, instead of WhatsApp – their usual communication platform, but she thought it may just be out of urgency. The message read:

Grandma, help me! I am in trouble with the police. I need \$500 urgently!

Mrs Tan was confused and texted back "Are you okay? What happened!?" The replies came quickly and warned Mrs Tan not to tell anyone and to quickly transfer the money. Starting to become extremely worried, Mrs Tan attempted to call Cindy through Facebook Messenger several times, but the calls were declined. She then received a message from Cindy stating "I cannot call now, please transfer the \$500. I am scared and need your help fast! Please Grandma! Help me!".



(©[psisa from Getty Images] via Canva.com)

Feeling worried for Cindy, Mrs Tan agreed to transfer the money and typed:

MRS TAN

I will transfer to your PayLah number, okay?

CINDY

No. PayLah to this number +65 12344667. My other Paylah is deactivated.

Without much hesitation, Mrs Tan immediately transferred the money to the stated number and continued to send messages, asking whether Cindy received the transfer.

The doorbell rang. Mrs Tan rushed to the door to find her family standing and smiling. As Mrs Tan saw Cindy's face, she rushed to hug her, with tears rolling down her cheeks. "Are you okay now?! Did you receive the money?", she asked. The whole family was bewildered and asked what was going on. At that moment, Mrs Tan realised she had been scammed. Relieved that her granddaughter was okay, but filled with guilt and shame - Mrs Tan wondered what she could have done differently.

Later that night, Mrs Tan's family discussed how to prevent this from happening again. They agreed that if a similar scenario were to ever occur, they would contact each other directly by their mobile phone numbers (not via third-party messaging apps such as Facebook, Instagram, etc.). They decided to take this as an opportunity to help Mrs Tan add privacy settings to her social media accounts, allowing only "friends" to message her.



Beyond financial loss, scams can negatively impact our mental health.

Let's look out for others and offer support to loved ones who have been scammed.

How to adjust your privacy settings on social media accounts:



1. Select **Settings & Privacy**, then select **Settings**
2. Select **Privacy**
3. Adjust the settings to prevent unknown persons from viewing your profile in full, or contacting and adding you

"REMEMBER ME?"

| | |
|------------------|-----------------------------|
| TARGET | Ms Farhana, 32, F&B Manager |
| SCAM TYPE | Fake Friend Call |

At work, Farhana received an unexpected call. The number was unfamiliar, but she decided to answer it thinking that it might be a customer calling. Upon answering the call, the caller immediately claimed to have changed his number and wanted to let her know. When Farhana asked who he was, the caller asked "you don't remember me? I am your old friend!". Farhana was confused, not knowing who he could be. The caller continued to press her and asked:



"YOU DON'T KNOW WHO I AM?"

Farhana said she still didn't recognise the voice, so the caller stated he would just message her on WhatsApp. Shortly after, Farhana received a message from the same number, stating it was her "old friend, George", and that it was nice to "finally talk" to her again. Farhana did know a business associate called "George" but was not on close terms with him, so she was confused. "George" sent another message, stating that he wished to borrow some money from her. Feeling uneasy, Farhana decided to check whether this caller was the George she knew. While she didn't have his number, Farhana knew his LinkedIn profile and reached out to the George she did know.

The real "George" confirmed it was not him asking for money and advised her to report and block the number. Farhana did so and was glad she had checked that the caller was not her "friend". She had saved herself a lot of stress, time, and money.

FARHANA



If you receive unsolicited calls or requests from "friends", CHECK their legitimacy through alternative means!

(e.g., via original contact details or physical meetups)

DID YOU KNOW?



In the year of 2022, fake friend call scams victimised over 2,106 people, with a combined loss of S\$8.8 million (SPF, 2023)

How to Check



CHECK FOR SCAM SIGNS

Look out for scam signs such as urgent requests or instructions from unknown persons online. To find out scam-specific signs, click the ScamAlert icon to the right!

1

**SCAM
ALERT**

Click
Me!



or visit
www.scamalert.sg



CHECK WITH AUTHORITIES

When in doubt, contact or refer to legitimate sources such as Singapore Police Force, your bank, or the ScamAlert website!

2

CHECK WITH TRUSTED OTHERS

Get a second opinion from people you know personally and trust! This could be any of your friends, family, or colleagues.

3



Slow Down!



**Scammers Use
Fake Emergencies**

CHECK YOURSELF

Slow down! Delay your responses to requests, orders, or instructions that make you feel pressured, anxious, or uncomfortable.

4

"I WON'T FALL FOR A SCAM!"

| | |
|------------------|---|
| TARGET | Lynn, 24, Student & Cheryl, 51, Stay-at-Home Mother |
| SCAM TYPE | E-Commerce Scam |

Lynn and her mother (Cheryl) were discussing gift ideas for Lynn's younger brother (Shan). Shan's birthday was coming up and time was running out to purchase a gift for his 18th birthday. Cheryl knew Shan loved gaming and suggested splurging and buying him a PlayStation 5. Lynn liked the idea but was hesitant – she knew the console had already sold out in official stores so they would have to buy pre-owned sets or from unofficial sellers. Lynn warned her mother – “Mum, just be careful purchasing online, okay? I've heard many stories of scammers taking money without giving any product in return.” Her mother seemed annoyed and stated:

“**Do you think I'm silly!?
Of course I won't fall for a scam!**”

Lynn reassured her mother, “No, I don't think you are silly. Scammers use a lot of deceptive tactics that anyone could fall for! Even my friends...” Lynn was trying to warn her mother. “Oh...”, Cheryl replied, “but then how do I know whether the seller is a scammer?” Lynn was pleased to see that her mother wanted to learn how to better protect herself. “Well, let me show you.” Lynn used an e-commerce app on her tablet to search 'PlayStation 5'. Looking through the search results, Lynn clicked on a listing that was selling a “brand new” PlayStation for just \$300. “Look Mum, this listing seems really cheap for something originally selling for \$700”.



“Maybe they just want to sell it off quickly?” Cheryl asked. “Maybe...let’s take a look at the seller’s profile” Lynn replied. Lynn clicked on the profile and explained to her mother what each section of the profile means – “Look...this seller has no previous ratings, and the account isn’t verified!” “I see”, Cheryl nodded. Lynn continued - “And here it shows their account is relatively new...with what we’ve just seen, along with the low-price listing, this is very likely a scam.”

“Ah I see...that makes sense actually. But how do I know for sure it’s a scam?” Cheryl asked. Lynn replied, “Well, scammers usually request payment outside of the e-commerce platform...so please arrange to pay in person or use secure in-platform payment system...also, when shopping online, it's safer to use e-commerce platforms with high Transaction Safety Ratings!” Cheryl continued her search for a “legitimate seller”. Lynn stood up, “I leave it to you now, you’ve got this! And remember mum, if you ever have any doubts about shopping online, I’m just a call away!”



Let’s teach our loved ones to only purchase from verified or reputable sellers, and to pay using in-platform secure payment system

PROTECT YOURSELF



ADD

Only use highly rated, safe, and official E-commerce platforms

CHECK

Check for E-Commerce scam signs such as:

- **Low or no past ratings from buyers or sellers**
- **Recently joined users**
- **No verification status**

TELL

If you encounter a scam or a scam sign, tell:

- **Authorities via ScamShield and ScamAlert**
- **the E-Commerce platform**
- **Your bank (if needed)**

5 FEATURES OF SAFE E-COMMERCE PLATFORM*

(MINISTRY OF HOME AFFAIRS, 2022)

- 1 Verification of seller identity.** Transact with verified sellers with high reviews.
- 2 Monitoring for fraudulent seller behaviour.** Choose platforms with processes to monitor for reporting and dispute-resolution options.
- 3 Availability of secure payment solutions.** You can protect yourself by using in-platform secure payment solutions.
- 4 Maintenance of transaction records and user data.** Choose platforms with these options.
- 5 Reporting and dispute resolution options.** Choose platforms with these mechanisms.

***[Click here to find out more about Transaction Safety Ratings from MHA!](#)**  **Click Me!**

" A GET-RICH-QUICK OFFER "

TARGET Aqil, 28, Delivery Rider
SCAM TYPE Investment Scam

Aqil received a new follower on Instagram named "Daniel". He swiped through the profile and found Daniel to be a cool guy with a luxurious lifestyle, making numerous posts on Crypto investments. Aqil was curious about Crypto investments, so he followed Daniel back on Instagram. The two began messaging each other, often involving Aqil asking about Crypto. Soon after, Daniel offered to teach Aqil how to invest by saying "Come...let me teach you...I have an insider tip...let's get rich together!".



"LET'S GET RICH TOGETHER!"

Aqil was overwhelmed with excitement about the opportunity as he wanted to provide more for his young family. Without asking many questions, Aqil agreed to trade with "TeGen Crypto International". He provided Daniel his personal and banking details to set up a trading account. However, things took a turn when Aqil realised that he started receiving notifications from his bank stating funds had been transferred out. Aqil was shocked when he realised his life savings were gone. He tried to contact Daniel but could no longer do so because Daniel's Instagram account was deactivated. Weeks passed and Aqil could not retrieve the money lost. He regretted not asking more questions and rushing into the "opportunity". Now he is worried about how to explain the situation to his wife.



Always invest with legitimate platforms or through a licensed investment advisor

Do not handover personal, banking and credit card details to others without checking

DID YOU KNOW?



Investment scams accounted for \$198.3 million in the year of 2022 alone (SPF, 2023)

How to Know if a Loved One is Being Scammed

Unfortunately, **anyone can fall prey to scams**, including **you and your loved ones**. However, if scammed, most would not want to believe or admit they have been scammed. Victims may feel embarrassed or ashamed, making it difficult for them to tell others or to seek help.

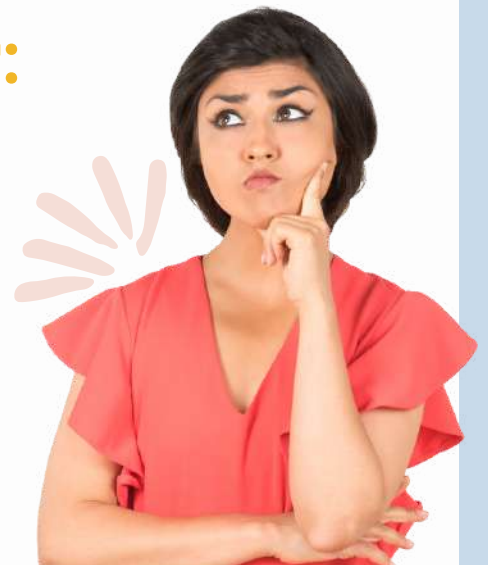
This means that someone you love could be getting scammed right now and you may not even know. **They may not even know it themselves!** Here are some ways to detect if a loved one is or has been scammed.

Some signs to look out for:

LIFESTYLE CHANGES

If you notice changes in lifestyle, routine, or mood, ask yourself "Why?". For example, is your outgoing friend suddenly becoming withdrawn? Or does a family member seem anxious while using their phone? These signs could suggest that something is wrong.

1



MONEY MATTERS

You may notice changes in spending habits or a sudden secrecy about money matters. There are many reasons why this may happen but it could also be a sign of scam victimisation. For example, is a family member borrowing money for unknown reasons, when they usually don't?

2



DENIAL

Scam victims may be in denial, refusing to believe they have been scammed. It can be hard to admit that a relationship, friendship, or job offer isn't real. They may refuse to listen to friends, family, bank staff, and even the police.

3



How to Convince a Loved One They're Being Scammed

GENTLY ASK QUESTIONS

Gently ask your loved one about what is going on, and tell them you are concerned and available to listen or help. Having them verbally explain the situation and repeat it may point out inconsistencies and suspicious aspects of the scenario, for both you and themselves.

1



PROVIDE INFORMATION

For some scam victims, it can be hard to admit that a relationship, friendship, or job offer isn't real. Showing tangible evidence of others who've been victimised may help them see the truth. Real victim stories can be found by visiting www.scamalert.sg/stories.

2



OFFER EMOTIONAL SUPPORT & LISTEN

Victims may be embarrassed or unaware that they have been scammed. They may withdraw and experience emotions such as anger, sadness, or guilt over the situation. The best thing you can do is offer a non-judgemental listening ear, and remain patient.

3



Read & compare real scam stories!

REACH OUT FOR HELP

If and when a loved one agrees that a scam/crime has been committed against them, be ready to assist them to report the case to their nearest Neighbourhood Police Centre or online (via SPF's e-reporting function - "I-Witness"), and seek professional help if required.

4





HELPFUL RESOURCES

SCAM ALERT

Visit the ScamAlert website to:

- Get the latest updates on scams
- Learn how to spot scams
- Share scam encounters

SCAM ALERT
BRINGING YOU THE LATEST SCAM INFO



SCAMSHIELD

Use ScamShield to:

- Block and detect scam calls and SMSes
- Report scam incidents



GET IT ON
Google Play

Download on the
App Store



CYBER SECURITY AGENCY

Visit CSA's website to:

- Get updates on the latest cyber-threats and learn tips
- Report cybersecurity incidents



STOP SCAMS MICROSITE

Visit The Straits Times' microsite to:

- Read latest news on scams
- Learn about scam trends and the advice of experts





HELPFUL RESOURCES

DIGITAL FOR LIFE

Visit Digital For Life by IMDA to:

- Learn about digital literacy and online safety



CASE COMPANY ALERT LIST

Visit CASE's Alert list to:

- Check for fraudulent companies
- Learn how to be a smarter consumer



Consumers
Association
of Singapore



MAS FINANCIAL INSTITUTION DIRECTORY

Visit MAS's Directory to:

- Check for financial institutions regulated by MAS and the regulated activities they are authorised to conduct in Singapore



Monetary Authority
of Singapore



MENTAL HEALTH RESOURCES

24HRS HELPLINE BY INSTITUTE OF MENTAL HEALTH

For anyone seeking mental health support

TEL:
6389 2222
24hrs

HELP123 BY TOUCH & FEI YUE COMMUNITY SERVICES

Provides basic counselling and information on cyber wellness-related issues

TEL:
1800 6123 123
Mon-Fri 10am-6pm, except PH

24HRS HELPLINE BY SAMARITANS OF SINGAPORE (SOS)

For anyone seeking mental health support

TEL:
1 767
24hrs

FAQS



Q

What should I do if I suspect I have been scammed?


A

Take action as soon as possible!

1. Contact your bank

- If you suspect you've been scammed, contact your bank immediately to freeze your bank accounts and cancel your cards/e-wallets

2. Report the incident to the Police

- After contacting your bank, lodge a police report via **one** of the following options:
 - **Lodge an online report** 
 - **Call 1800-255-0000**
 - **Report in-person at a nearby police station**
- Reporting your case quickly will assist the police in launching investigations early

3. (Optional) Share your story on ScamAlert, to prevent further community victimisation

Q

Does the ScamShield app block calls and SMSes from people I know?

A

No. ScamShield only blocks calls and SMSes from a database of blocked numbers, managed centrally by the National Crime Prevention Council (NCPC) and Singapore Police Force (SPF).

Read more about ScamShield at www.scamshield.org.sg/faq/ 

REFERENCES

Cyber Security Agency of Singapore [CSA]. (2021). *Singapore Cyber Landscape 2021*. <https://www.csa.gov.sg/News/Publications/singapore-cyber-landscape-2021>

Home Team Behavioural Sciences Centre [HTBSC]. (2020). Scammer, Beware: Building Societal Resilience to Scams. https://scamalert.sg/docs/default-source/default-document-library/building-societal-resilience-to-scams-ebook.pdf?sfvrsn=c5328718_2

Ministry of Home Affairs. (2022). *E-Commerce Marketplace Transaction Safety Ratings*. <https://www.mha.gov.sg/e-commerce-marketplace-transaction-safety-ratings>

Monetary Authority of Singapore [MAS]. (2022, January 19). *MAS and ABS announce measures to bolster the security of digital banking*. <https://www.mas.gov.sg/news/media-releases/2022/mas-and-abs-announce-measures-to-bolster-the-security-of-digital-banking>

ScamAlert. (n.d.). *Scam Stories*. <https://www.scamalert.sg/stories>

ScamShield Open Government Products. (n.d.). *FAQ*. <https://www.scamshield.org.sg/faq/>

Singapore Police Force [SPF]. (2023, February 08). *Annual Scams and Cybercrime Brief 2022*. <https://www.police.gov.sg/media-room/statistics>

Singapore Police Force [SPF]. (2023, February 08). *Annual Scams and Cybercrime Brief 2022 Infographic*. <https://www.police.gov.sg/media-room/statistics>

ABOUT HTBSC



Inaugurated in 2005, the Home Team Behavioural Sciences Centre (HTBSC) is a research centre that aims to provide a behavioural sciences angle to support the Home Team's operational work.

HTBSC strives to be a path-finding centre of excellence for behavioural sciences research and training in the area of crime, safety, and security. The centre serves to equip Home Team (HT) officers with the knowledge and skills to deal with issues relating to human behaviours, so as to complement their operational effectiveness as well as enhance their efficiency.

Key specialised psychological branches of the HTBSC include:

Crime, Investigation and Forensic Psychology (CIFP) branch

Operations and Leadership Psychology (OLP) branch

Resilience, Safety and Security Psychology (RSSP) branch

For Enquiries:

Home Team Behavioural Sciences Centre (HTBSC)

Home Team Academy

Ministry of Home Affairs

Government of Singapore

501 Old Chua Chu Kang Road, Singapore 698298

Email: MHA_HTBSC_COMMS@MHA.GOV.SG

Main Line: 6465 3730

Fax: 6465 3731

ABOUT OCP



The Office of Chief Psychologist (OCP) was established on 1 February 2017 to align the psychological efforts of the Home Team Departments to MHA's strategic priorities and to build expertise in MHA's psychological services.

Since its inception, the OCP has taken on an active role in organising HT psychological services resources in support of MHA's key focal areas. In addition, the OCP has created platforms and established strategic links that enable MHA to leverage the knowledge and support of international and local partners to provide solutions to challenges faced by MHA.

EDITORIAL TEAM

| | |
|-----------------------|--|
| Publisher | Home Team Behavioural Sciences Centre Crime, Investigation and Forensic Psychology Branch |
| Advisor | Mr Boon Siang Kwek |
| Editorial Team | Ms Chloe Alexandra Mr Joel Ong Mr Karthigan Subramaniam Ms Joan Teo Ms Vivian Seah Ms Stephanie Chan Mr Yongjie Chen |

Copyright© 2022. All rights are reserved. Views expressed in this publication are the authors' only and do not represent or imply any official position or view of HTBSC, OCP, or MHA. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photography, recording or any information storage and retrieval system, without written permission from the Home Team Behavioural Sciences Centre.