

In support of:



INTRODUCTION

In Singapore, a whopping \$651.8 million was lost to scammers in 2023, a figure that continues to remain high. Clearly, scammers are getting bolder and more creative with their approach.

But here's a twist - it's not just the elderly who are being targeted. Over 67% of the scam victims were between 20 and 49 years old, showing that digital savviness doesn't equal scam immunity.

To keep you one step ahead of these crafty scammers, we've created this guide spotlighting the most prevalent phone scams in Singapore for 2024. Being informed makes identifying and stopping scams much simpler. As you continue reading, you'll discover key warning signs and, just in case you ever encounter a scam, we've included valuable tips to help you recover quickly!

CONTENTS

- 1** Identifying different types of scams
- 2** ACT against scams
- 3** In case we haven't met, we're Circles Life





SECTION 1

Identifying different types of scams



Scam tactics are constantly changing. As soon as a particular scam gets widely recognised, scammers quickly develop a new strategy to replace it. However, there are certain red flags that consistently stand out, alerting you when something doesn't quite add up.

Be wary of random or unknown calls asking for:

-  **Personal information (like your date of birth or address)**
-  **Banking details, including One-Time Passwords (OTP)**
-  **Passwords or urgent requests for money transfers**
-  **A caller playing the 'Guess Who' game, pretending to be someone you know**

Hang up on any call asking for this information immediately! Even if they don't ask for banking or financial details, sharing personal information can be just as harmful as it paves the way for identity theft and unauthorised access to your online accounts.

Of course, outright money requests from unknown callers are a clear no-go, but scammers often employ more subtle and convincing tactics to lure you in.

Though the nature of scam calls changes frequently, there are several common types that continue to persist.

Robocall Scams with AI impersonating voices

In Robocall scams, AI-generated voices, often imitating reputable entities like banks or government offices, deliver pre-recorded messages to appear credible. The goal is to mislead you into divulging personal or financial details.

With technological advancements, these scams have become more sophisticated, allowing easy imitation of familiar voices. It's increasingly important to be cautious, even when the caller sounds like someone you know – or your loved ones.



Lottery Scams

Free gift or special offer scams are particularly devious as they prey on the excitement of its victims by offering extravagant prizes like cars or cruises. In the excitement, victims may lower their guards and provide personal details, such as bank account credentials or OTPs, or even pay an administrative fee to "claim" the prize.

As a general rule, if it seems too good to be true, it probably is. Don't share any personal or banking information over the phone.

Internet Love Scams

Dating scams can be difficult to spot as they often start on legitimate dating sites, where scammers create fake profiles to form emotional connections over weeks or months. As the relationship deepens, they may ask for money or sensitive information - only to vanish afterwards.

To stay safe, never share personal details or send money to anyone you haven't met in person.

Fake Charity Scams

In these scams, scammers impersonate real charities or invent fake ones to solicit donations. They emotionally appeal to potential donors about their cause, and then ask for financial contributions or credit card details.

To avoid falling for these scams, it's best to politely decline phone payment requests and verify the charity's legitimacy on charities.gov.sg before making any donations through official channels.

Investment Scams

Like charity scams, investment scammers seek your money or banking information through enticing "exclusive offers" or lucrative cryptocurrency investments. Be cautious if they directly request financial details, as this is a major red flag.

Always verify the legitimacy of any investment company on the MAS website and avoid disclosing personal information to unfamiliar parties.



Job Scams

Employment scams involve fake job offers or unemployment cheques, where scammers ask for your personal or banking information or even money to 'secure' a job. Such requests are clear indicators of a scam.

No legitimate employer or recruiter would ever require this information over the phone!

Cyber Extortion Scams

Extortion scams operate by instilling panic, claiming to possess sensitive information about you, ranging from alleged debts to threats of releasing private pictures online. They demand money or financial details in exchange for withholding that information.

These scams can be easily identified by their highly unusual and threatening nature, but their alarming content may cause victims to unintentionally divulge their details.

Software Update Scams

Tech support scams trick you into believing that your computer has issues. Scammers may pose as representatives from your device's manufacturer and often request sensitive information like passwords, email and home addresses.

Remember, genuine **manufacturers and service providers will never ask for such information over the phone.**



Bank Impersonation Scams

Scammers may fabricate issues with your account or card, like suspicious transactions, and ask for banking details under the guise of verification, including:

- Bank account numbers
- Card details
- Banking passwords
- ATM pins

Remember, banks never request such information via phone or instruct you to transfer funds to unknown accounts. Always verify directly with your bank if you're uncertain.



Tax Time Scams

Scammers typically double down on their activity during tax seasons, often alleging serious problems with your tax returns to cause panic.

They might claim you have unpaid taxes or have evaded them, then ask for your banking or tax details.

Keep in mind that the IRAS will never ask for sensitive information over the phone.



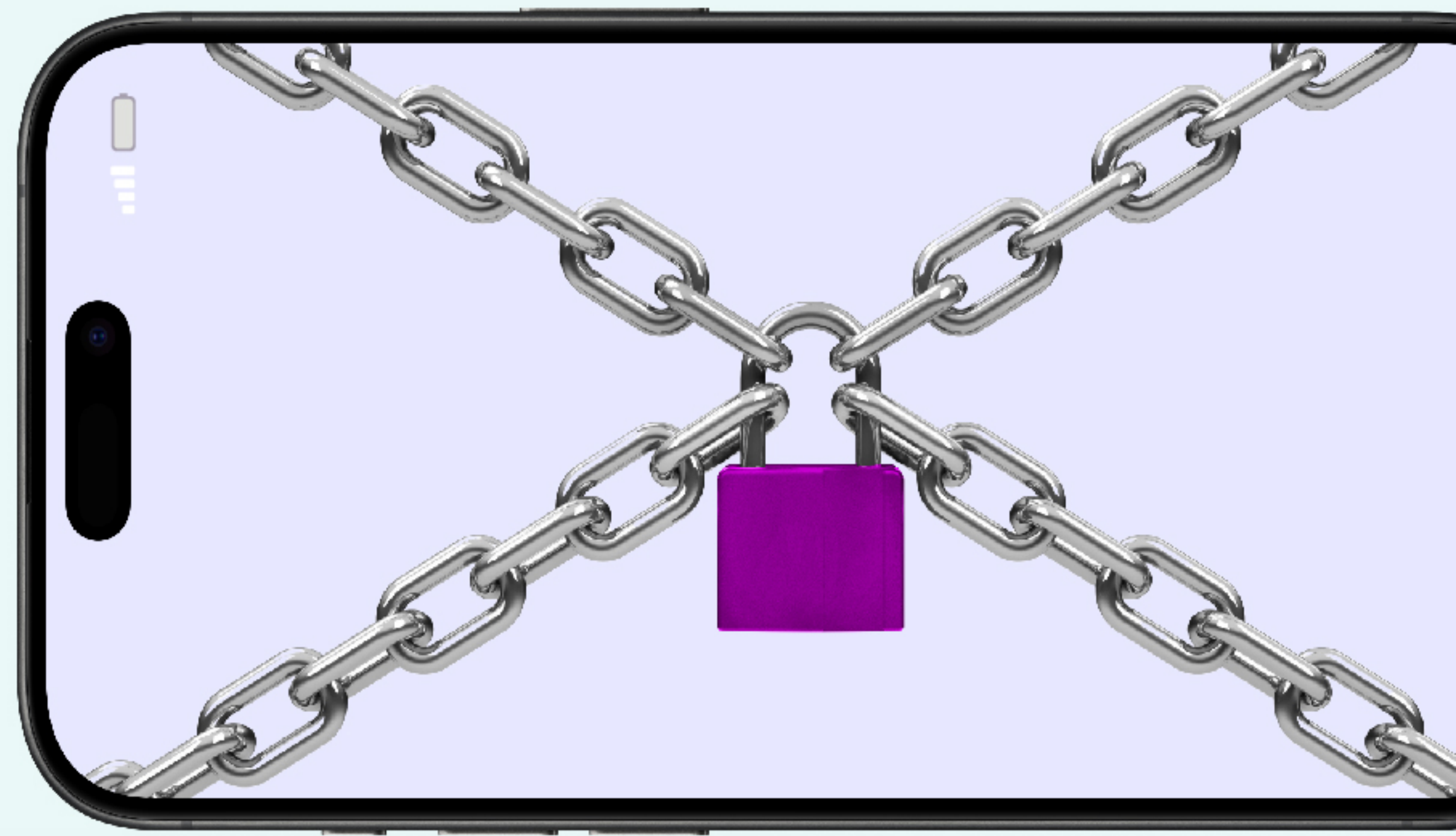
Enforcement Scams

Enforcement scams are prevalent in Singapore, where scammers impersonate officials from agencies like ICA or SPF, accusing you of involvement in criminal activities such as money laundering. In an attempt to create urgency and anxiety, they might even urge you to transfer your savings to a supposed 'Government's holding account' or ask for personal details like passport information to aid police investigations.

Always remember, SPF would never instruct you to transfer money or share sensitive information over the phone. They will contact you through official channels if necessary.

SECTION 2

ACT against scams



Add Security Features

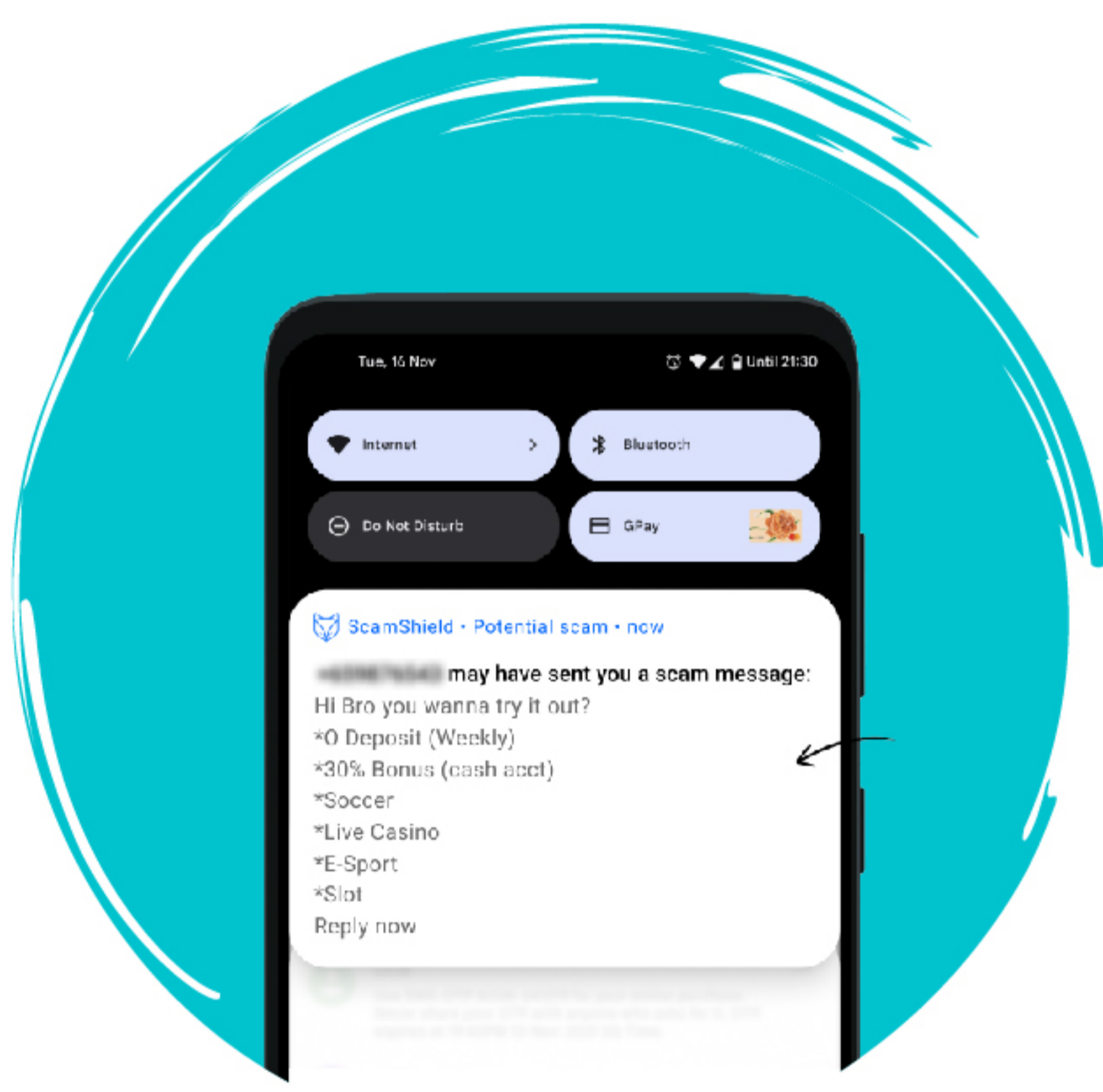
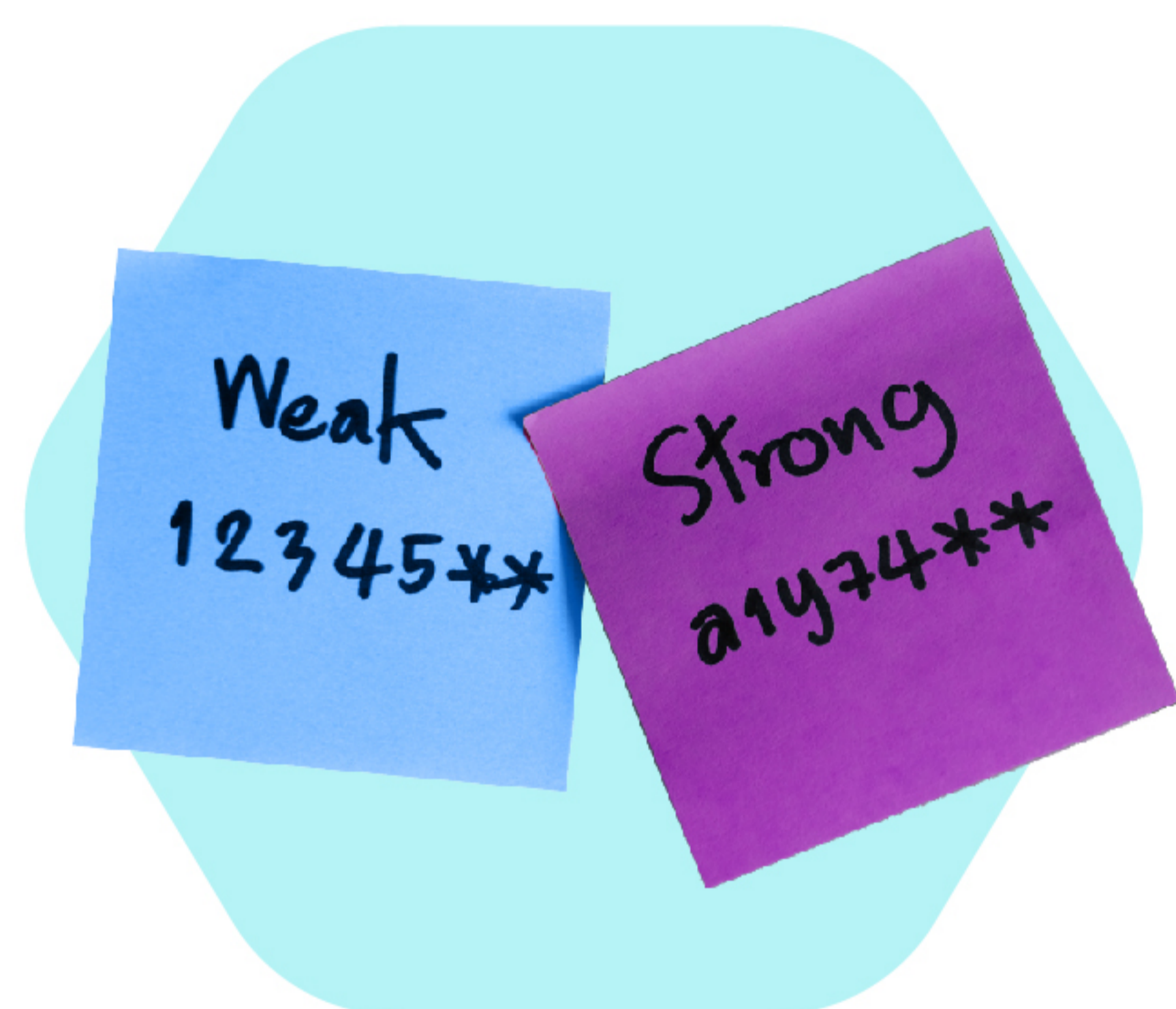


Secure Your Online Social Media Accounts

To ensure your safety on social media, secure your accounts with two-factor authentication and regularly update your unique passwords. This protects not only your personal data, like phone numbers and credit card details, but also prevents scammers from exploiting your account to spread deceptive content to your contacts.

Strong Passwords and PINs

To protect your personal and financial information, personalise your device and account passwords and PINs. Use a mix of numbers, upper and lower case letters, and symbols, avoiding simple choices like "1234" or "0000". Update them regularly to prevent security breaches and avoid using the same ones across different platforms.



Add ScamShield and Anti-virus Apps

Install the ScamShield App to block scam calls and detect scam SMSes. Also, install anti-virus apps to prevent malware from official app stores.

Safeguard your savings with Money Lock

Work with your bank to 'lock up' all or part of your funds to prevent scammers from digitally transferring them from your bank account. To access your secured funds, physical verification would be needed.



Be Careful About Unidentified Missed Calls

Avoid responding to calls or SMS from numbers you don't recognise. Genuine callers will likely find alternative ways to reach you or call back.

Be Aware When Shopping Online

Protect yourself by verifying website security through SSL certificates (HTTPS in the URL) and being alert to browser warnings like unusual padlock symbols (e.g. red, open or warning triangle) or URL strikethroughs. Always use secure networks and research the retailer's credibility.

Whenever possible, use credit cards for purchases as they offer better scam protection – banks may help recover stolen funds, unlike debit card transactions. Always be cautious, even on secure WiFi, to protect your card details from theft.



Check for Signs



Be Careful About Sharing Personal Information

Never share personal information, especially over calls or texts. If in doubt about a caller's legitimacy, hang up and contact your bank directly using their official number.

Communicate With Your Bank

Inform your bank immediately if you suspect your passwords have been compromised or if you have inadvertently sent money to a scammer. Prompt action can help prevent further unauthorised access or financial loss.



Watch Out for Unusual Payment Requests

Stay vigilant with your banking transactions and verify the legitimacy of unfamiliar payment requests by reaching out to the company directly using their official contact information. Be cautious even if you're offered help with stopping suspicious payments, as these could be scam attempts.

Tell the Authorities

If you encounter any form of scam in Singapore, report it to the Police at your nearest Neighbourhood Police Post or online. For more information on how to respond to scams, visit www.scamalert.sg or call the Anti-Scam Helpline at 1800-722-6688.

If you have any information on scams, you can:

- 1) Call the police hotline at 1800-255-0000;
- 2) Submit it online at www.police.gov.sg/iwitness;
- 3) Submit the information through the ScamShield app.
- 4) Block the person on the platforms (i.e. WhatsApp, Telegram etc) where you were contacted on the scam

Additionally, inform your bank for banking and financial scams and report e-commerce issues to the relevant platforms. For spam-related scams, reach out to the Personal Data Protection Commission (PDPC).



SECTION 3

In case we haven't met, we're Circles.Life

Circles.Life emerged as a tech-focused telco provider with the goal of empowering customers through hyper-convenience, radical transparency, and delightful experiences.

Our range of data plans, from **20GB at \$12/month** to **1TB at \$30/month**, ensures safe and reliable online transactions, safeguarding you from the vulnerabilities of public WiFi. Alongside our data offerings, we provide no-contract SIM-only plans, roaming packs, eSIMs, and an exciting loyalty program.

Stay Secure and Delightfully Connected with Circles.Life!