BE CYBER SAFE

A GUIDE TO STAYING SAFE ONLINE

保持网络安全

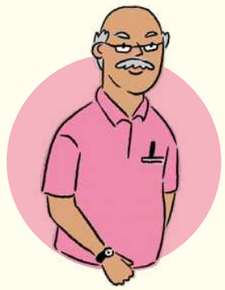
网络安全指南

CSA SINGAPORE
Cyber Security Agency of Singapore

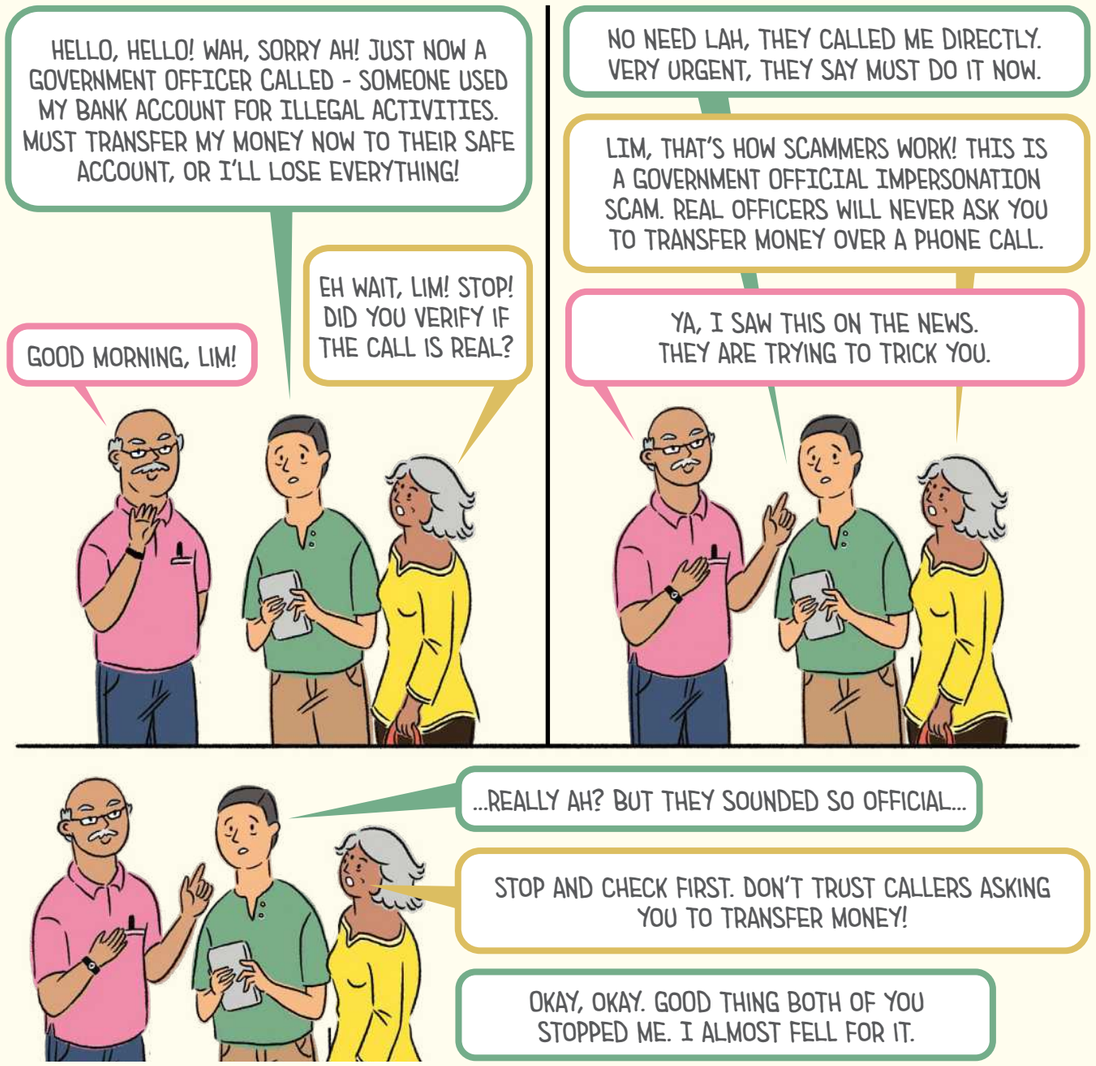
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

LIM
Taxi Driver

RANI
Administrative Assistant



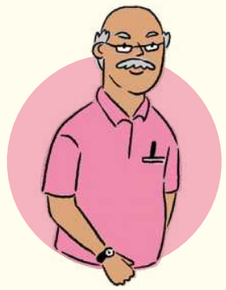
MUHAMMAD
Retired Teacher



Smartphones and smart devices have made life more convenient. However, this has also created more opportunities for cybercriminals to carry out cybercrimes. This handbook will arm you with the information you need to protect yourself and your loved ones online.

林先生
德士司机

拉妮
行政助理



穆罕默德
退休教师

智能手机和各种智能设备让我们的生活更加方便，但这也给网络犯罪分子创造了更多机会。这本手册将提供您所需的信息，帮助您如何在网上保护自己和亲人。

WHAT DANGERS ARE WE EXPOSED TO?

As we go online more often to do banking or shopping at our own convenience, we are at risk from cyber threats in the form of online scams and data theft.

WHAT IS PHISHING?

Phishing is a method used by cybercriminals to trick you into giving out personal and financial information such as passwords, One-Time Passwords (OTPs) or bank account numbers.

Cybercriminals may pretend to be from the government, banks or businesses, claiming that there are urgent issues requiring your immediate attention. They may contact you through social media, messaging platforms, and phone calls to trick you into revealing personal and banking information that can be used to make unauthorised transactions.

STOP AND CHECK!

Cybercriminals often use fear and urgency to pressure you into making hasty decisions.

By taking a moment to stop and check with official sources, family and friends, you can better protect yourself from falling prey to cybercriminals out to steal your hard-earned money and data.

我们面临哪些网络风险？

随着我们越来越常在网上进行银行交易或购物，虽然更加方便，但也面临各种网络威胁，例如网络诈骗和资料被盗。

什么是网络钓鱼？

网络钓鱼是一种诈骗手法，网络犯罪分子会诱骗您泄露个人和财务信息，例如密码、一次性密码（OTP）或银行账户号码。

网络犯罪分子可能冒充政府、银行或商家，谎称有紧急问题需要您马上处理。他们可能通过社交媒体、通讯平台和电话联系您，诱骗您泄露个人和银行信息，以进行未经授权的交易。

停一停，查一查！

网络犯罪分子常利用恐惧和紧迫感，迫使您仓促作出决定。

只要先停一停，并向官方渠道、家人或朋友核实，您就能更好保护自己，避免落入网络罪犯盗取您血汗钱和个人资料的圈套。

COMMON TYPES OF ONLINE SCAMS

GOVERNMENT OFFICIALS IMPERSONATION SCAMS

Cybercriminals typically pose as government officers and trick you into revealing personal information, banking details and/or transferring money to bank accounts they provide.

What to look out for:

Government officials will **never** ask you to do the following over a phone call:

- Transfer money
- Disclose banking details
- Install mobile apps from unofficial app stores
- Transfer your call directly to the police

IMPERSONATION OF BANK REPRESENTATIVES

CYBERCRIMINALS MAY ALSO PRETEND TO BE BANK EMPLOYEES, CLAIMING THERE ARE ISSUES WITH YOUR ACCOUNT.

DO NOT PANIC. CALL YOUR BANK'S OFFICIAL HOTLINE TO VERIFY THE ISSUE. REMEMBER, BANKS WILL NEVER SEND CLICKABLE LINKS VIA SMS OR TRANSFER YOUR CALL TO THE POLICE.

常见网络诈骗类型

冒充政府官员诈骗

网络犯罪分子通常会冒充政府官员，诱骗您透露个人资料、银行账户信息，或将钱转入他们提供的银行账户。

需要注意的事项：

政府官员**绝对不会**在电话中：

- 要求您转账
- 索取任何用于登录银行账户的资料
- 要求您安装源自非官方应用平台的手机应用程序
- 将您电话转接给警方

冒充银行职员诈骗

网络犯罪分子也可能冒充银行职员，声称您的银行账户出现问题。
不要惊慌。请拨打银行的官方热线核实情况。记住，银行绝不会通过短信发送可点击链接，也不会把您的电话转接给警方。

INVESTMENT SCAMS

Cybercriminals use social media and messaging platforms to carry out investment scams. They advertise fake investments promising high returns, or adding you to chat groups where accomplices share fake success stories or payment screenshots to make the scam appear genuine. Some may befriend you first to build trust before tricking you into transferring money.

JOB SCAMS

Cybercriminals may promise you commission for carrying out simple tasks such as reviewing hotels or completing surveys via WhatsApp or Telegram chat groups. Small payouts will be given to you to build your trust. Following this, you will be encouraged to take on other tasks with higher payout that require you to create accounts and transfer large sums of money to unknown bank accounts.

E-COMMERCE SCAMS

Cybercriminals use attractive deals to pressure you into immediate payment before delivery. Once paid, they become uncontactable. In some cases, they ask you to download a malicious app to make payment or process a refund. Installing the app gives them access to your device, banking, and social media accounts.

What to look out for:

These are the signs of phishing to look out for. Cybercriminals may do the following to trick you:

- Send unexpected or unsolicited emails, messages or calls
- Promise attractive rewards or promote exclusive deals
- Use urgent or threatening language to pressure action
- Request for personal and/or banking information
- Include suspicious links or attachments

投资诈骗

网络犯罪分子会通过社交媒体和通讯平台进行投资诈骗。他们会宣传承诺高回报的虚假投资项目，或把您拉进聊天群组，由同伙分享伪造的投资成功案例或转账截图，让诈骗看似真实。有些网络犯罪分子还会先与您建立关系取得信任，然后诱骗您转账。

工作诈骗

网络犯罪分子可能承诺，只要完成一些简单任务（例如为酒店撰写评价或完成问卷调查），就能获得佣金，并通过 WhatsApp 或 Telegram 聊天群组与您联系。起初，他们可能会给您一些小额报酬，以建立与您的信任。随后，他们会鼓励您参与回报更高的任务，但这些任务通常会要求您开设户口，并把大笔资金转入不明来源的银行账户。

电子商务诈骗

网络犯罪分子以超值优惠为诱饵，要求您在发货前立即付款。一旦付款，他们便失联。有些情况下，他们会要求您下载恶意应用程序，以进行付款或办理退款。安装该应用程序后，他们便可获取使用您手机的权限、从而取得您的银行账户及社交媒体账户。

需要注意的事项：

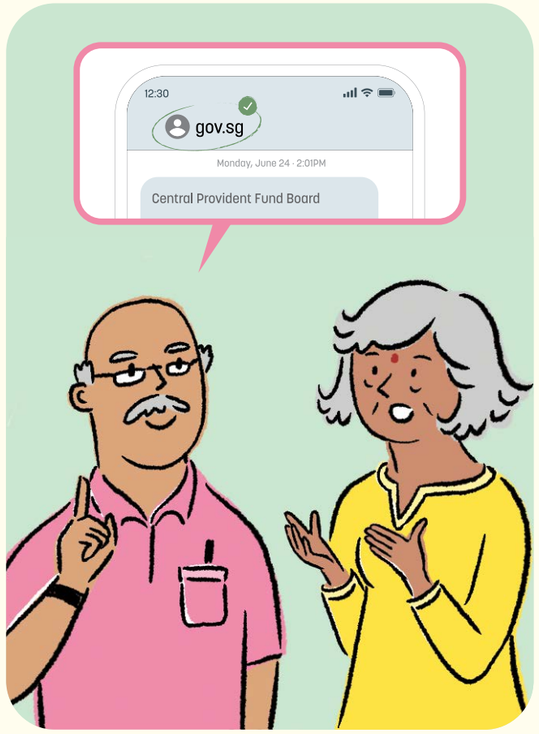
以下是网络钓鱼的常见迹象。网络犯罪分子可能会通过以下方式行骗：

- 发送来历不明或未经请求的电邮、讯息或来电
- 承诺诱人的奖励或宣传限时优惠
- 使用紧急或威胁性的语言催促您立即采取行动
- 要求提供个人及／或银行资料
- 附带可疑链接或附件

What you can do:

Take a moment to **STOP** and **CHECK** using the steps below:

- **Verify unexpected calls or messages** by contacting the official hotline or visiting the official app or website directly. To confirm messages or calls from a friend, call the number saved in your contacts.
- **Rethink** if the purchase or investment returns sound too good to be true
- **Call for advice.** Check with your family members or friends, or call the ScamShield Helpline at 1799.
- **Do not share** your personal and banking information unless you are sure it is a legitimate request
- **Do not click** on any attachment or link in the message. Delete it.
- **Do not download** unknown apps or software from a third-party website



WHAT IS MALWARE?

Malware is short for "malicious software". It refers to a type of software that infects your devices, steals your information, corrupts and even deletes your data.

MALWARE-ENABLED SCAMS

Cybercriminals may trick you into installing malware by asking you to download their app to enjoy free deliveries or discounts.

Once installed, the malware gives them access to your device and allows them to steal your banking details, passwords and OTPs to make unauthorised transactions.

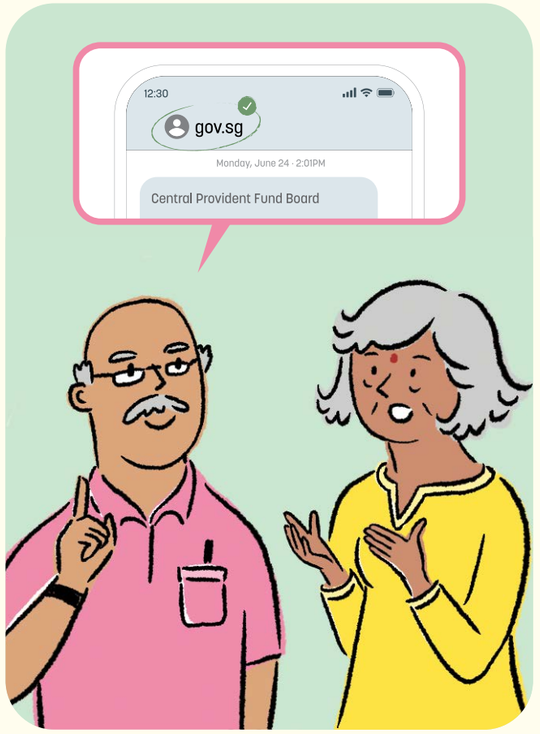
What to look out for:

Be cautious if someone asks you to download an app from unofficial sources for discounts or free services. Cybercriminals may also pressure you and give step-by-step instructions on how to download the app.

您可以这样做：

请花点时间，按照以下步骤，**停一停**，**查一查**：

- 通过拨打官方热线或直接访问官方应用程序或网站，**核实来电或讯息的真实性**。如需确认朋友的来电或讯息，请拨打您通讯记录中原有的号码。
- 如果购物优惠或投资回报听起来好得不真实，**请重新思考**
- **寻求建议**。向家人或朋友核实，或拨打 ScamShield 反诈骗热线 1799。
- 在确认请求合法之前，**不要透露**个人及银行资料
- **不要点击**讯息中的任何附件或链接，并立即删除
- **不要**从第三方网站**下载**不明应用程序或软件



什么是恶意软件？

"恶意软件"也称为"恶意程序"。它是一种能入侵您的电子设备、窃取资料、破坏甚至删除数据的软件。

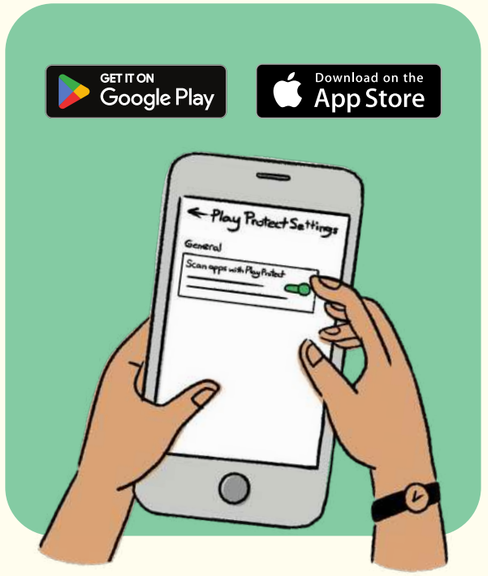
恶意软件诈骗

网络犯罪分子可能以"免费送货"或"折扣优惠"为诱饵，诱骗您下载他们的应用程序。

一旦安装，恶意软件就会让他们取得您设备的控制权，窃取银行资料、密码和 OTP，进行未经授权的交易。

需要注意的事项：

若有人要求您从非官方来源下载某应用程序以获取折扣或免费服务，应提高警惕。
网络犯罪分子也可能施压，并逐步指导您如何下载该应用程序。



What you can do:

- **Do not grant accessibility permissions** to unknown apps
- **Only download apps from official app stores** such as Google Play Store (Android) or Apple App Store (iOS) as these platforms have measures in place to detect and remove malicious apps

How can you tell if your phone has been infected with malware?

- Excessive and unexplained data use
- Random pop-ups or new apps not installed by you
- Noticeably slower responses or performance
- Battery drains unusually
- Unexpected or suspicious behaviours from the device such as auto-activation of camera or microphone

What should you do if your phone has been infected with malware?

- Turn on the "airplane mode" and keep Wi-Fi off
- Run an anti-virus scan on your phone with an updated anti-virus app
- Use a different and trusted device to check for any unauthorised banking, Singpass or CPF transactions
- If there are unauthorised transactions, report them to the bank and Police immediately
- After completing these steps, if you believe your phone is not infected, you may resume use. As a precaution, consider a "factory reset" and changing important passwords. Back up your data first.

您可以这样做：

- **不要**向来源不明的应用程序**授予辅助功能权限**
- **切勿从非官方来源下载应用**。仅使用 Google Play Store (Android) 或 Apple App Store (iOS) 等官方应用商店。这些商店已采取检测和删除恶意应用的措施，确保下载的应用安全运行。

如何识别您的手机是否遭恶意软件入侵？

- 过度和难以解释的数据用量
- 出现随意弹窗或出现并非您安装的新应用程序
- 手机反应或运作明显变慢
- 电池异常快速耗电
- 设备出现异常或可疑行为，例如摄像头或麦克风自动启动

如果手机遭恶意软件入侵，应怎么做？

- 开启 "飞行模式"，并关闭 Wi-Fi
- 使用已更新的防病毒应用程序扫描手机
- 使用另一部可信设备，检查是否有未授权的银行、Singpass 或公积金交易
- 若发现未授权交易，应立即通知银行并向警方报案
- 完成以上步骤后，如确认手机未受感染，可恢复使用。为安全起见，可考虑恢复出厂设置并更改重要密码，记得先备份资料。

DEEPFAKES

Deepfakes are photos, videos, or audio recordings digitally created or altered using Generative Artificial Intelligence (AI). As technology advances, deepfakes are becoming increasingly convincing. They are used in online scams to impersonate authority figures and celebrities, tricking you into revealing personal details or authorising fraudulent payments. This can lead to irreversible financial losses.

What to look out for:

- Check if content comes from an official or trusted source
- Be extra careful if the content:
  - Includes the use of urgent language ("transfer now", "last chance")
  - Asks for sensitive information (NRIC, bank account, OTP)
  - Requests for money transfers
- Look for unnatural signs in videos/audio:
  - Blurring around face edges
  - Unnatural blinking or facial movements
  - Lips not matching speech

What you can do:

- **Pause and think.** Do not rush, especially if the message is urgent, unsafe, or unusual.
- **Verify the source.** Contact the person or organisation using a phone number or channel you already know (e.g. official hotline, saved contact), not the one given in the message.
- **Do not share sensitive information.** Never reveal your passwords, OTPs, or full bank details over calls, messages, or videos.
- **Do not transfer money.** Discuss with family members and friends first.

LEARN MORE

Scan the QR code for more information on Generative AI & Deepfakes!

深伪

深伪是一种利用人工智能 (AI) 生成逼真但虚假音频、视频或图像的技术。随着科技进步，深伪内容越来越逼真。网络犯罪分子可能利用深伪冒充权威人士或名人，诱骗您透露个人资料或授权进行诈骗付款。这可能导致无法挽回的金钱损失。

需要注意的事项：

- 确认内容是否来自官方或可信来源
- 若内容涉及以下情况，请格外谨慎：
  - 使用紧急字眼（例如“马上转账”“最后机会”）
  - 要求提供敏感资料（如身份证号码、银行账户、OTP）
  - 要求转账汇款
- 留意视频或音频中的异常迹象：
  - 面部边缘模糊不清
  - 眨眼或面部动作不自然
  - 嘴型与说话内容不一致

您可以这样做：

- **停下来想一想。**尤其当讯息显得紧急、不安全或异常时，切勿仓促行动。
- **核实来源。**使用您已知的电话号码或官方热线或已保存的联系方式联系相关人士或机构，而不要使用讯息中提供的号码。
- **不要透露敏感资料。**切勿通过电话、讯息或视频透露密码、OTP或完整银行资料。
- **不要转账。**先与家人或朋友商量。

了解更多

扫描QR码了解更多关于生成式人工智能与深伪技术的相关信息！

HOW TO BE CYBER SAFE

Practising good cyber hygiene helps protect you from falling prey to online scams. Protect yourself through the adoption of three cyber tips:

Enable 2FA and Use Strong Passphrases

Using Two-Factor Authentication (2FA) together with a strong passphrase provides an additional layer of protection for your online accounts.

2FA uses more than one type of information to verify your identity and access your online accounts.

How to create a strong passphrase:

Step 1: **String together 5 different words** from a personal memory

Bread → ihadbread**at8am**

Step 2: **Use uppercase, lowercase, numbers and symbols** (at least 12 characters)

ihadBREADat8am!

Do not use easily obtainable information such as your name, NRIC number, or birthdate.

Do not share your passwords with anyone or write them down.

如何保持网络安全

养成良好的网络卫生习惯，有助于防范网络诈骗。通过采用以下三项网络安全贴士，保护自己：

启用双重身份验证（2FA）并使用安全性高的密码短语

结合双重身份验证（2FA）和强密码短语，可为您的网上账户提供额外一层保护。

双重身份验证（2FA）会使用两种或以上不同类型的信息来核实您的身份，以登录网上账户。

如何创建强密码短语：

步骤一： **选取5个**与您个人记忆相关的**不同词语，并将它们组合成一句密码短语。**

Bread → ihadbread**at8am**

步骤二： **加入大小写字母、数字和符号**（至少12个字符）。

ihadBREADat8am!

不要使用容易获取的资料，例如姓名、身份证号码或出生日期。

不要与他人分享密码，也不要把密码写下来。

Update Software Promptly

Software and app updates contain important security fixes that can help keep your devices safe.

LEARN MORE

Scan here to find out how to enable automatic updates!

Add ScamShield and Anti-Virus Apps

ScamShield is a suite of products and tools that help defend against scams. Download the app to block and filter scam calls and messages.

Anti-Virus Apps help detect malware and malicious phishing links. They are key to safeguarding your devices and accounts.

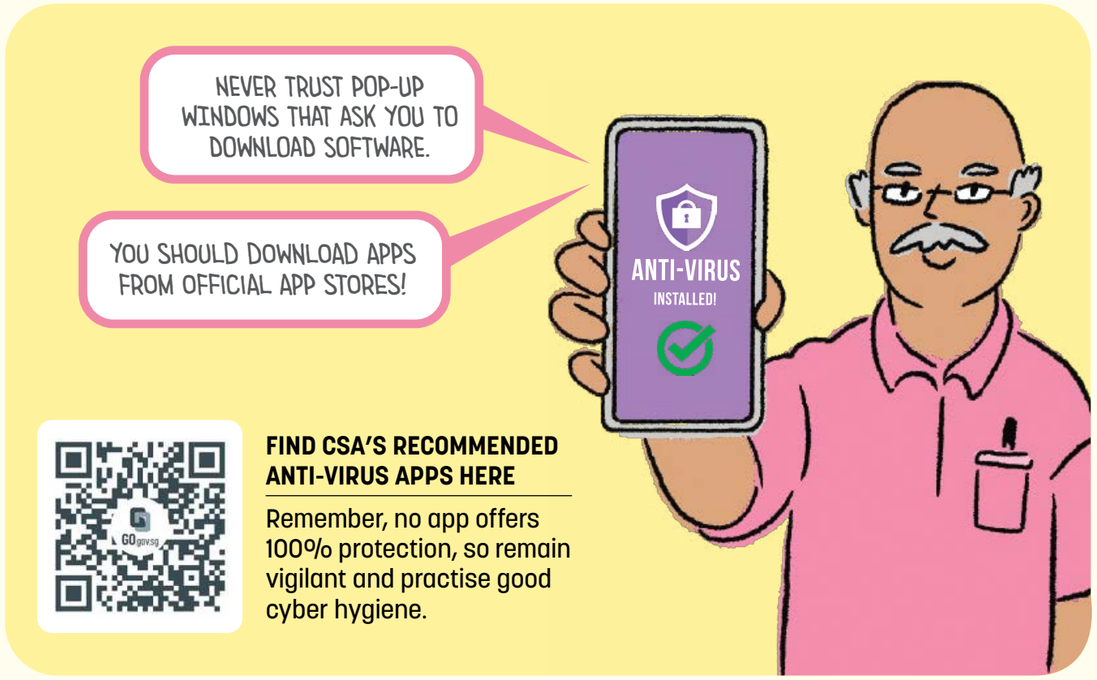
How to choose an Anti-Virus App

Anti-virus apps from different brands have varying functions and capabilities. Here are some tips when choosing an anti-virus app:

- **Download from official app stores** such as Google Play Store (Android) or Apple App Store (iOS)
- **Check out app reviews before downloading.** Look at the developer's reputation, app ratings and the number of downloads too.
- **Choose apps with detection and removal capabilities.** Look for those that provide real time malware detection (for Android devices only) and removal capabilities.

LEARN MORE

Scan here for more information on ScamShield



FIND CSA'S RECOMMENDED ANTI-VIRUS APPS HERE

Remember, no app offers 100% protection, so remain vigilant and practise good cyber hygiene.

及时更新软件

软件和应用程序更新包含重要的安全修补程序，有助于保障设备安全。

了解更多

扫描此处了解如何启用自动更新！

下载 ScamShield 和防病毒 (Anti-Virus) 应用程序

ScamShield 是一套协助防范诈骗的产品与工具。下载应用程序可拦截和过滤诈骗电话及讯息。

防病毒应用程序可以检测恶意软件和钓鱼链接的防病毒应用程序，是保障设备和账户安全的重要工具。

如何选择防病毒应用程序

不同品牌的防病毒应用程序在功能和能力方面各有不同。以下是选择防病毒应用程序时的建议：

- **切勿从非官方来源下载应用。**仅使用 Google Play Store (Android) 或 Apple App Store (iOS) 等官方应用商店。
- **下载前查看应用评价，**包括开发者信誉、评分及下载次数。
- **选择具备侦测及清除功能的应用程序，**尤其是提供实时恶意软件侦测 (仅限安卓设备) 及移除功能的应用。

了解更多

扫描此处了解更多有关 ScamShield 的信息。

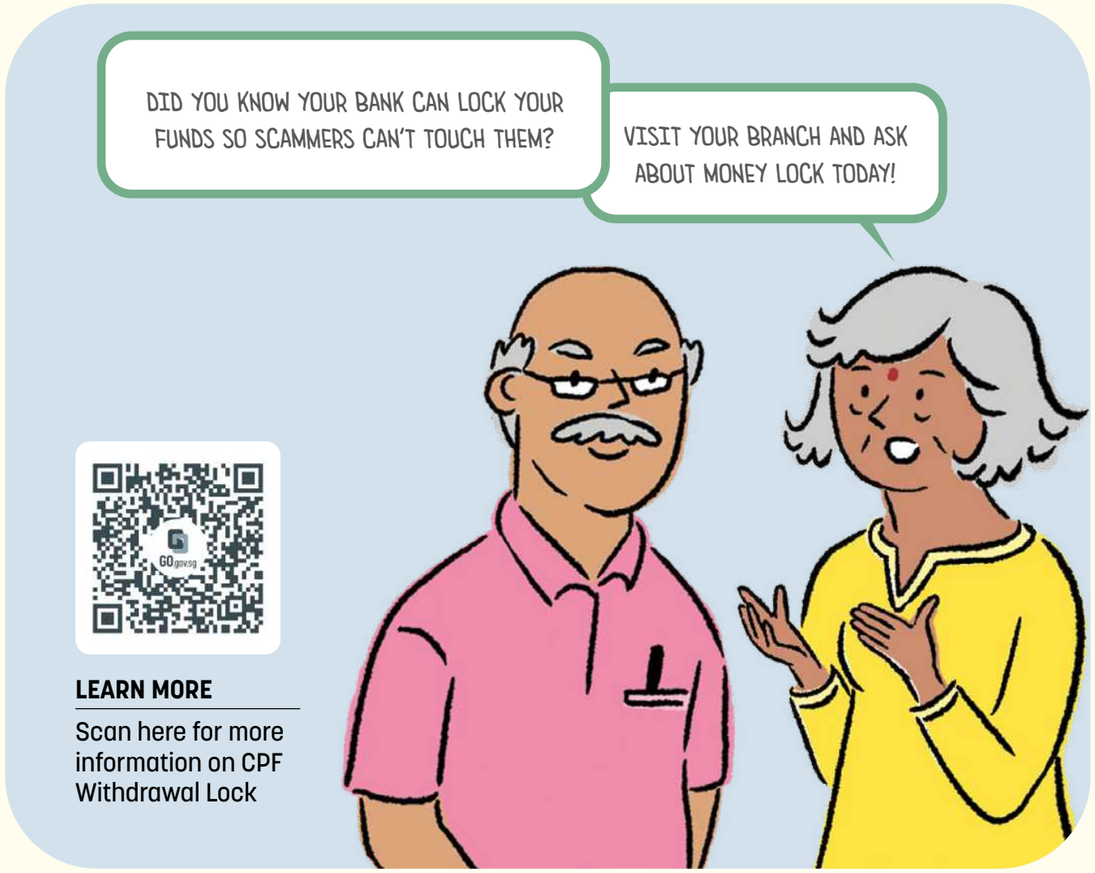
在此查看新加坡网络安全局推荐的防病毒应用程序。

请记住，没有任何应用程序能提供百分之百保障，务必保持警惕并养成良好的网络卫生习惯。

What else can you do to protect yourself?

Besides practising good cyber hygiene, there are additional security features you can enable in your apps to protect your savings and reduce potential losses in the event of a scam.

- **Money Lock** was introduced by the local banks to safeguard your bank account and guard against scams by allowing funds to be 'locked' so they cannot be transferred digitally. Check with your bank on how to activate this feature.
- The **CPF Withdrawal Lock** feature allows members aged 55 and above to instantly disable online CPF withdrawals. You can activate this feature at any time through your CPF account settings and set your Daily Withdrawal Limit to safeguard your savings.



LEARN MORE

Scan here for more information on CPF Withdrawal Lock

您还能做些什么来保护自己?

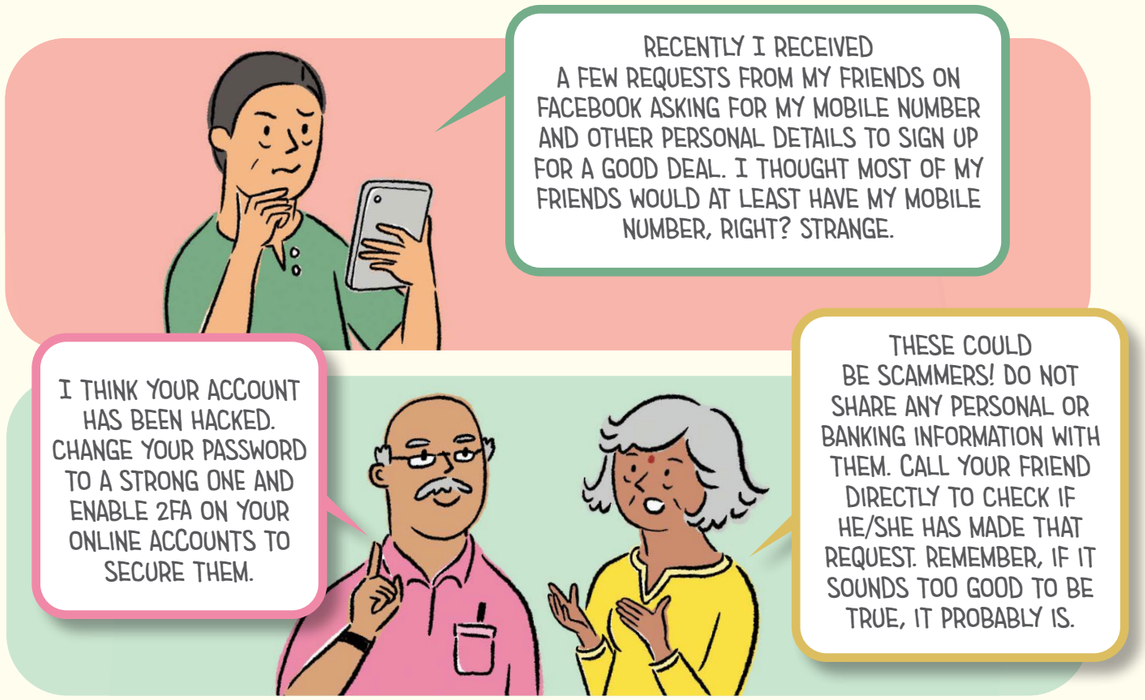
除了养成良好的网络卫生习惯外，您也可启用应用程序中的额外安全功能，以保障存款，并在遭遇诈骗时减少潜在损失。

- 本地银行推出 **Money Lock** 功能，可将部分资金锁定，防止通过电子方式转账，以保障银行账户安全。请向您的银行查询如何启用此功能。
- **公积金局（CPF）提款锁**功能允许55岁及以上会员即时关闭网上提款功能。您可随时通过公积金账户设置启用此功能，并设定每日提款限额，以保障存款安全。

了解更多

扫描此处了解更多有关公积金提款锁的信息。

WHAT SHOULD YOU DO IF YOU'VE FALLEN PREY TO A PHISHING SCAM?



If you still have access to your account,

- **Log out of this account from all devices** connected to the account
- **Change your password immediately** and enable 2FA if available

If you do not have access to your account,

- **Contact the platform** e.g. bank or social media platform, to report the issue and request assistance to retrieve your account
- **Report any fraudulent credit/debit card charges** to your bank and cancel your card immediately
- **Make a police report** at the nearest Neighbourhood Police Centre or Neighbourhood Police Post or online at www.police.gov.sg/e-services if monetary loss is involved
- **Go to CSA's SingCERT Webpage** www.csa.gov.sg/singcert/reporting if you wish to submit an incident report
- Should your account be compromised, the impersonator could reach out to your contacts. **Warn your family and friends** to ignore any request and not to share their personal details.

如果您落入网络钓鱼诈骗陷阱，该怎么办？

如果您还能进入自己的账户，

- **在所有**连接到账户的**电子设备上登出账户。**
- **立即更换密码**及启用2FA（如有）。

如果您不能进入自己的账户，

- **联系**银行或社交媒体等**相关平台，**告知您遇到的问题，并寻求协助恢复您的账户。
- 如果信用卡/借记卡有任何不实的消费记录，应立即**通知银行，**并注销您的卡。
- 如果涉及金钱损失，应到最靠近的邻里警局或邻里警岗，或上网 www.police.gov.sg/e-services **报案。**
- 如果您想提交事件报告，**请到新加坡网络紧急应变组 (SingCERT) 网页** www.csa.gov.sg/singcert/reporting 。
- 如果账户被盗，冒充者可能会联系您认识的人。您应**通知家人和朋友**不要理会任何要求，也不要泄露他们的个人资料。

I'M WORRIED I WILL GET SCAMMED. MAYBE I SHOULD NOT RESPOND TO ANY MESSAGES OR CALLS.

DON'T WORRY. WE JUST HAVE TO STAY VIGILANT. STOP AND CHECK AND CALL A FAMILY MEMBER OR FRIEND FOR ADVICE.

YES. AND REMEMBER, DO NOT SHARE YOUR PASSWORDS OR OTPS WITH ANYONE. NOT EVEN ME, OKAY?

我担心自己会被骗。也许我不应该回复任何短信或接听来电。

不要担心。我们只须保持警惕。停一停，检查一下，并向家人或朋友求助。

是的，请牢记不要向任何人透露个人密码和OTP，即使是我也不例外，OK?

Better cyber safe than sorry

For more information, visit CSA's SG Cyber Safe Seniors webpage or ScamShield website.

欲知更多详情，请到新加坡网络安全局年长者网络安全网页或浏览ScamShield网站查询。

www.csa.gov.sg **www.scamshield.gov.sg**

Get more cyber tips at:

安全贴士请扫描QR码:

For the latest scam info, visit:

更多有关诈骗的最新详情，请扫描QR码: