BE CYBER SAFE

A GUIDE TO STAYING SAFE ONLINE

இணையத்தில் பாதுகாப்பாக இருங்கள்

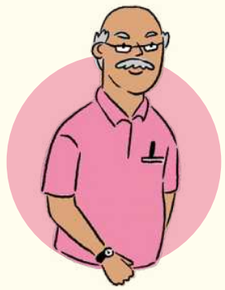
இணையத்தில் பாதுகாப்பாக இருக்க ஒரு வழிகாட்டி

CSA SINGAPORE
Cyber Security Agency of Singapore

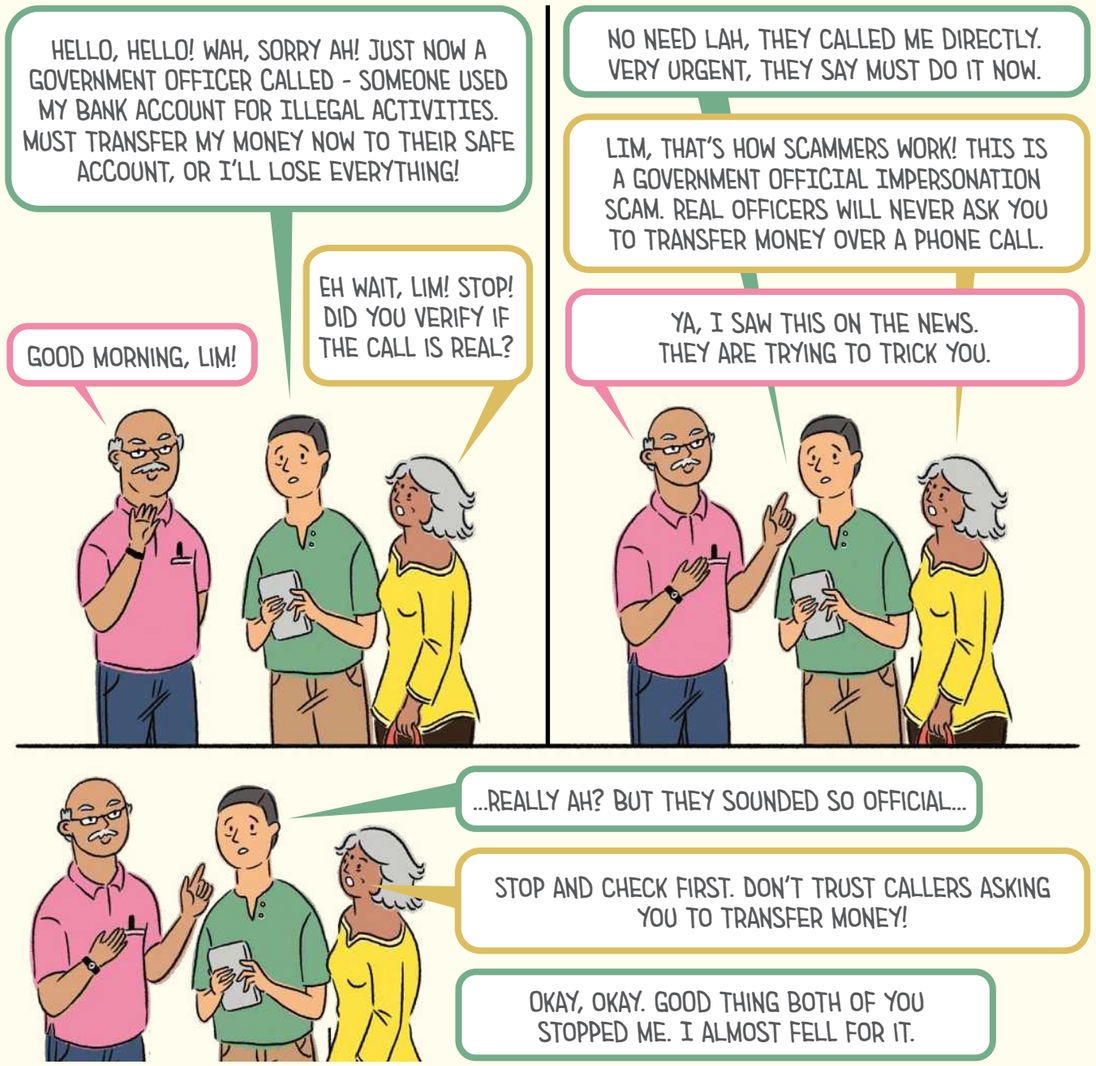
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

LIM
Taxi Driver

RANI
Administrative Assistant



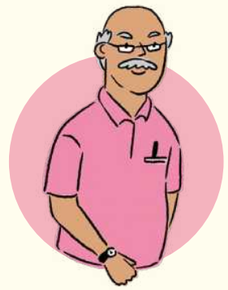
MUHAMMAD
Retired Teacher



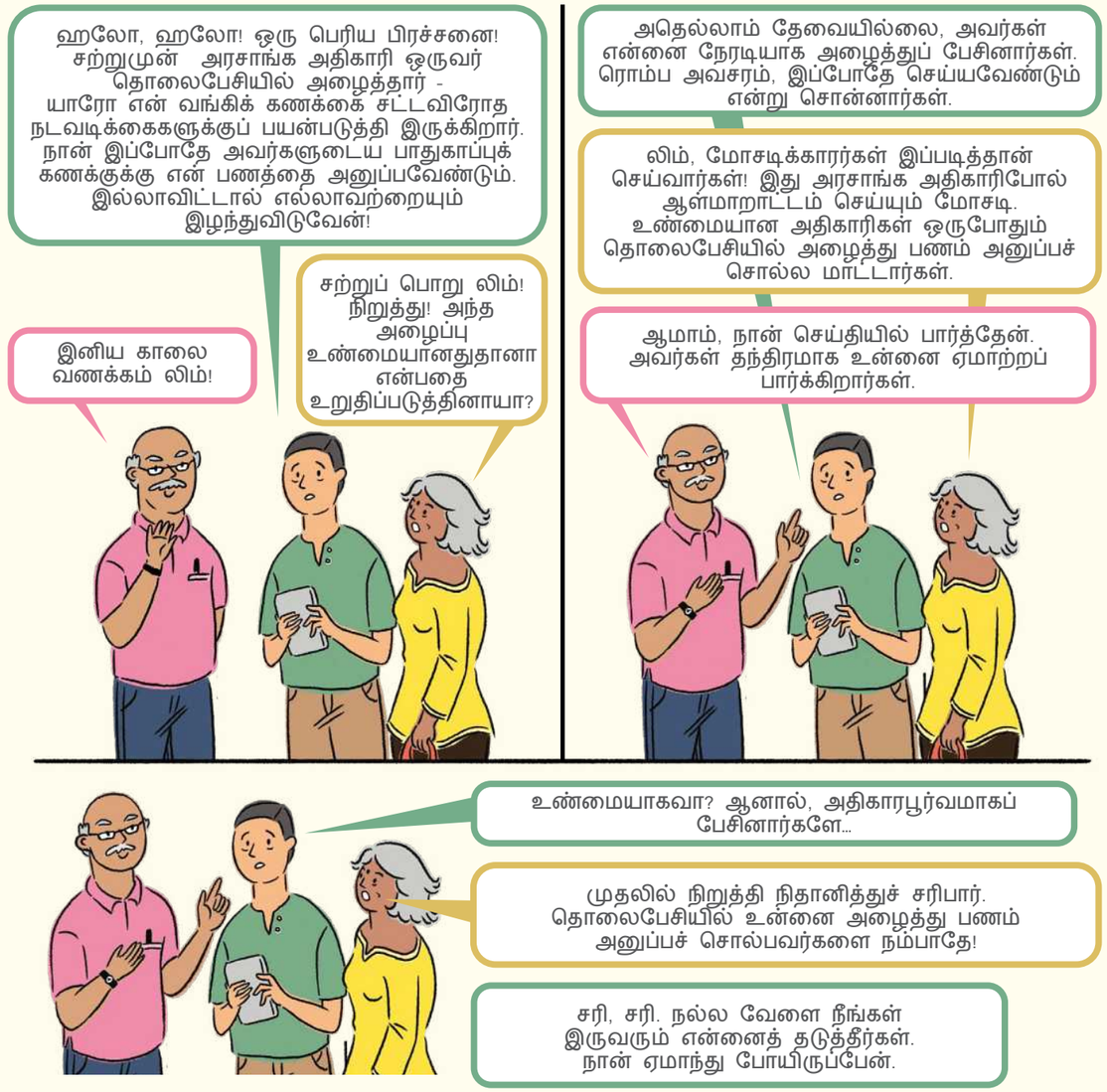
Smartphones and smart devices have made life more convenient. However, this has also created more opportunities for cybercriminals to carry out cybercrimes. This handbook will arm you with the information you need to protect yourself and your loved ones online.

லிம்
டாக்சி ஓட்டுநர்

ராணி
நிர்வாக உதவியாளர்



முகமது
ஓய்வுபெற்ற ஆசிரியர்



திறன்பேசிகளும் அறிவார்ந்த சாதனங்களும் வாழ்க்கையை அதிக வசதியாக்கியுள்ளன. இருந்தாலும், இணையம்வழிக் குற்றங்கள் புரிவதற்கும் அதிகமான வாய்ப்புகளை உருவாக்கியுள்ளன. இந்தக் கையேடு, இணையத்தில் உங்களையும் உங்கள் அன்புக்குரியவர்களையும் பாதுகாத்துக் கொள்வதற்குத் தேவைப்படும் தகவல்களை உங்களுக்கு வழங்கும்.

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.

நாம் என்னென்ன ஆபத்துகளுக்கு உள்ளாகக்கூடும்?

நாம் வங்கிச் சேவைக்காக அல்லது பொருள் வாங்குவதற்காக இணையத்தை அதிகமாகப் பயன்படுத்துவதால், இணைய மோசடிகள், தகவல் திருட்டு போன்ற இணைய மிரட்டல்களை எதிர்நோக்குகிறோம்.

தகவல் திருட்டு என்பது என்ன?

தகவல் திருட்டு (phishing) என்பது கடவுச்சொற்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் (OTPs) அல்லது வங்கிக் கணக்கு எண்கள் போன்ற தனிப்பட்ட நிதித் தகவல்களைத் தந்திரமாக உங்களிடமிருந்து தெரிந்துகொள்ள இணையம்வழிக் குற்றம் புரிவோர் பயன்படுத்தும் ஓர் உத்தி.

இணையம்வழிக் குற்றம் புரிவோர், அரசாங்க, வங்கி அல்லது நிறுவன அதிகாரிபோல் ஆள்மாறாட்டம் செய்து, நீங்கள் உடனடியாகக் கவனிக்க வேண்டிய சில அவசர விவகாரங்கள் இருப்பதாகச் சொல்லக்கூடும். அவர்கள் சமூக ஊடகம், செயலிவழித் தகவல்கள், தொலைபேசி அழைப்புகள் வாயிலாக உங்களைத் தொடர்புகொண்டு, உங்களது தனிப்பட்ட, வங்கி விவரங்களைத் தந்திரமாக வெளியிட வைக்கக்கூடும். அனுமதியின்றி பணப் பரிவர்த்தனைகள் செய்வதற்கு இந்த விவரங்கள் பயன்படுத்தப்படலாம்.

நிறுத்தி நிதானித்துச் சரிபாருங்கள்!

இணையம்வழிக் குற்றம் புரிவோர் உங்களை அவசர அவசரமாக முடிவெடுக்கச் செய்வதற்காகப் பயமுறுத்திப் பதற்றமடையச் செய்வார்கள்.

நீங்கள் சற்று நேரம் நிறுத்தி நிதானித்து, அதிகாரப்பூர்வத் தகவல் தளங்கள், குடும்பத்தினர், நண்பர்கள் ஆகியோரிடம் கேட்டுச் சரிபார்ப்பதன்வழி, பாடுபட்டுச் சம்பாதித்த பணத்தையும் உங்கள் விவரங்களையும் இணையம்வழிக் குற்றம் புரிவோரிடம் பறிகொடுக்காமல் உங்களைப் பாதுகாத்துக் கொள்ள முடியும்.

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.

பொதுவான இணைய மோசடிகள்

அரசாங்க அதிகாரிபோல் ஆள்மாறாட்டம் செய்யும் மோசடிகள்

இணையம்வழிக் குற்றம் புரிவோர் வழக்கமாக அரசாங்க அதிகாரிபோல் ஆள்மாறாட்டம் செய்து, தந்திரமாக உங்களது தனிப்பட்ட, வங்கி விவரங்களை வெளியிட வைப்பார்கள் அல்லது அவர்கள் கூறும் வங்கிக் கணக்குகளுக்குப் பணம் அனுப்பச் சொல்வார்கள்.

நீங்கள் கவனிக்க வேண்டியவை:

அதிகாரிகள் ஒருபோதும் உங்களைத் தொலைபேசியில் அழைத்துப் பின்வருமாறு செய்யச் சொல்ல மாட்டார்கள்:

- பணம் அனுப்பச் சொல்லுதல்
- வங்கி விவரங்களைக் கூறச் சொல்லுதல்
- அதிகாரபூர்வமற்ற செயலி விநியோகத் தளங்களிலிருந்து கைப்பேசிச் செயலிகளைப் பதிவிறக்கம் செய்யச் சொல்லுதல்
- உங்களுக்குச் செய்த தொலைபேசி அழைப்பைக் காவல்துறைக்கு நேரடியாக மாற்றிவிடுதல்

வங்கிப் பிரதிநிதிகளைப்போல் ஆள்மாறாட்டம்

இணையம்வழிக் குற்றம் புரிவோர் வங்கி ஊழியர்களைப் போலவும் ஆள்மாறாட்டம் செய்து, உங்கள் வங்கிக் கணக்கில் பிரச்சனைகள் இருப்பதாகச் சொல்லக்கூடும். நீங்கள் பதறிவிடாதீர்கள். உங்கள் வங்கியின் அதிகாரப்பூர்வத் தொலைபேசி எண்ணை அழைத்துப் பிரச்சனை இருக்கிறதா என்பதை உறுதிப்படுத்துங்கள். ஒன்றை மட்டும் எப்போதும் நினைவில் கொள்ளுங்கள். வங்கிகள் "கிளிக்" செய்யக்கூடிய இணைப்புகளைக் குறுந்தகவல்வழி அனுப்பவோ அல்லது உங்கள் அழைப்பைக் காவல்துறைக்கு மாற்றிவிடவோ மாட்டார்கள்.

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

முதலீட்டு மோசடிகள்

இணையம்வழிக் குற்றம் புரிவோர் சமூக ஊடகத்தையும் தகவல் தளங்களையும் பயன்படுத்தி முதலீட்டு மோசடிகள் செய்வார்கள். அதிக ஆதாயம் கிடைக்குமென உத்தரவாதம் தரும் போலி முதலீடுகளை விளம்பரம் செய்வார்கள், அல்லது அரட்டைக் குழுக்களில் உங்களைச் சேர்ப்பார்கள். அந்த அரட்டைக் குழுக்களில் உள்ள அவர்களது உடந்தையாளர்கள், போலியான வெற்றிக் கதைகளை அல்லது பணம் கிடைத்த சான்றுகளின் படங்களைப் பகிர்ந்து, மோசடியை உண்மையென்று நம்ப வைப்பார்கள். சிலர் ஆரம்பத்தில் நட்பாகப் பழகி உங்கள் நம்பிக்கையைப் பெற்ற பிறகு, ஏமாற்றிப் பணம் அனுப்ப வைப்பார்கள்.

வேலை மோசடிகள்

இணைய மோசடிக்காரர்கள் வாட்ஸ்ஆப் அல்லது டெலிகிராம் குழுக்கள் வாயிலாக ஹோட்டல்களை விமர்சித்தல் அல்லது ஆய்வுகளில் பங்கெடுத்தல் போன்ற எளிய பணிகளுக்குப் பணம் தருவதாகச் சொல்வார்கள். உங்கள் நம்பிக்கையைப் பெறுவதற்காகச் சிறு தொகைகள் வழங்கப்படும். அதன்பின், அதிகப் பணம் கிடைக்கும் மற்றப் பணிகளைச் செய்யுமாறு உங்களை ஊக்குவிப்பார்கள். வங்கிக் கணக்குகள் தொடங்கி, தெரியாத வங்கிக் கணக்குகளுக்குப் பெரும் பணத்தை மாற்றிவிடுவது அந்தப் பணிகளில் உள்ளடங்கும்.

இணைய விற்பனை மோசடிகள்

இணையம்வழிக் குற்றம் புரிவோர் அருமையான சலுகைகளுடன் ஆசைகாட்டி, பொருளை அனுப்பி வைப்பதற்குமுன் உடனடியாகப் பணம் கட்டச் சொல்லி நெருக்குதல் தருவார்கள். பணத்தைக் கட்டியவுடன், அவர்களுடன் தொடர்புகொள்ள முடியாமல் போய்விடும். சில சம்பவங்களில், பணம் கட்டுவதற்கு அல்லது பணத்தைத் திரும்பப் பெறுவதற்கு நச்சுநிரல் செயலியைப் பதிவிறக்கம் செய்யச் சொல்வார்கள். அந்தச் செயலியைப் பதிவிறக்கம் செய்தால், உங்களது கைப்பேசிச் சாதனம், வங்கிச்சேவை, சமூக ஊடகக் கணக்குகள் அனைத்தும் அவர்களின் வசமாகிவிடும்.

கவனிக்க வேண்டியவை:

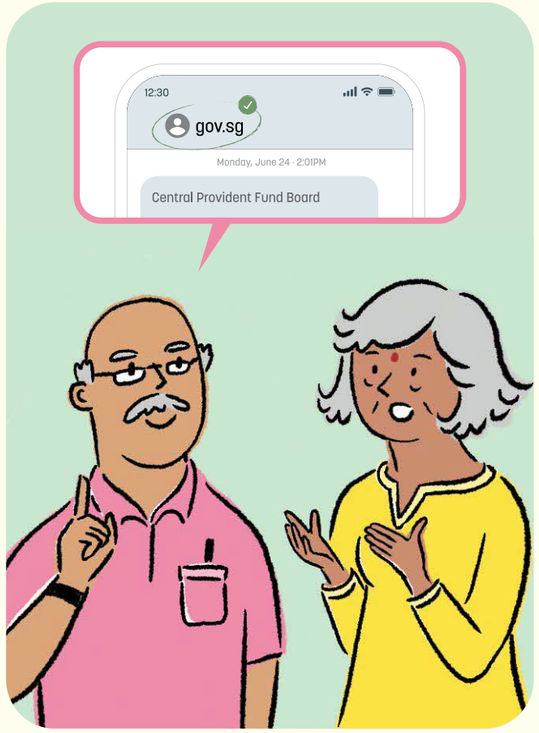
நீங்கள் கவனிக்க வேண்டிய தகவல் திருட்டு அறிகுறிகள் இவை. இணையம்வழிக் குற்றம் புரிவோர் பின்வரும் வழிகளில் உங்களை ஏமாற்றக்கூடும்:

- எதிர்பார்க்காத அல்லது வரவேற்கப்படாத மின்னஞ்சல்கள், குறுந்தகவல்கள் அனுப்புவார்கள் அல்லது தொலைபேசியில் அழைப்பார்கள்
- அருமையான வெகுமதிகள் தருவதாக உத்தரவாதம் அளிப்பார்கள் அல்லது பிரத்யேகச் சலுகைகளை வழங்குவார்கள்
- அவசரமான அல்லது மிரட்டலான முறையில் பேசி, உடனடியாகச் செயல்பட நெருக்குதல் தருவார்கள்
- தனிப்பட்ட மற்றும்/அல்லது வங்கித் தகவல்களைக் கேட்பார்கள்
- சந்தேகத்திற்குரிய இணைப்புகளை இணைத்து அனுப்புவார்கள்

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.

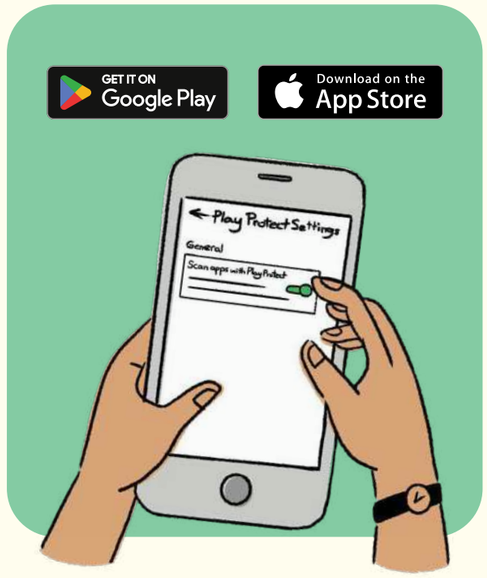
MALWARE-ENABLED SCAMS

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:

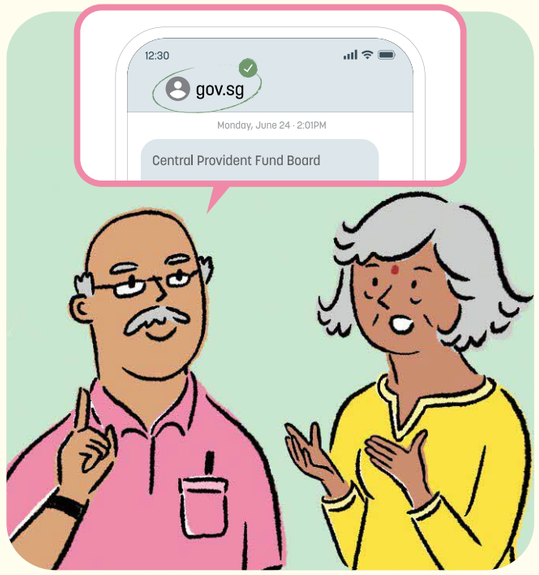
Be cautious if someone asks you to download an app from unofficial sources for discounts or free services. Cybercriminals may also pressure you and give step-by-step instructions on how to download the app.



நீங்கள் என்ன செய்ய முடியும்:

நிறுத்தி நிதானித்துப், பின்வரும் வழிமுறைகளைப் பயன்படுத்திச் சரிபாருங்கள்:

- **எதிர்பார்க்காத அழைப்புகளை அல்லது குறுந்தகவல்களைச் சரிபார்க்க** அதிகாரபூர்வத் தொலைபேசி எண்ணை அழையுங்கள் அல்லது அதிகாரபூர்வ செயலியை அல்லது இணையத்தளத்தை நேரடியாகத் திறந்து பாருங்கள். நண்பரிடமிருந்து வரும் குறுந்தகவல்களை அல்லது அழைப்புகளை உறுதிப்படுத்த, நீங்கள் ஏற்கனவே சேமித்து வைத்திருக்கும் எண்ணை அழைத்துப் பாருங்கள்.
- விலை அல்லது முதலீட்டு ஆதாயம் உண்மையென நம்ப முடியாத அளவுக்கு அருமையாக இருந்தால் **மறுபடியும் யோசித்துப் பாருங்கள்**
- **தொலைபேசியில் அழைத்து ஆலோசனை கேளுங்கள்.** உங்கள் குடும்பத்தினரிடம் அல்லது நண்பர்களிடம் கேட்டு, அல்லது 1799 எனும் ஸ்கேம்ஷீல்டு உதவித் தொலைபேசிச் சேவையை அழைத்து உறுதிப்படுத்திக் கொள்ளுங்கள்
- சட்டபூர்வமான கோரிக்கைதான் என உறுதியாகத் தெரிந்திருந்தாலொழிய, உங்களது தனிப்பட்ட வங்கி விவரங்களைப் **பகிராதீர்கள்**
- தகவலில் உள்ள எந்தவோர் இணைப்பின்மீதும் **“கிளிக்” செய்யாதீர்கள்.** அதனை அழித்துவிடுங்கள்
- மூன்றாம் தரப்பு இணையத்தளத்தில் இருந்து தெரியாத செயலிகளை அல்லது மென்பொருளைப் **பதிவிறக்கம் செய்யாதீர்கள்**



நச்சுநிரல் என்பது என்ன?

நச்சுநிரல் என்பது தீங்கு செய்யும் ஒரு வகை மென்பொருளைக் (“malicious software”) குறிக்கிறது. இந்த மென்பொருள், உங்கள் சாதனங்களில் நச்சைப் பரப்பி, உங்களது தகவல்களைத் திருடி, சாதனத்தில் உள்ள தரவுகளைக் கெடுத்து அழித்துவிடும்.

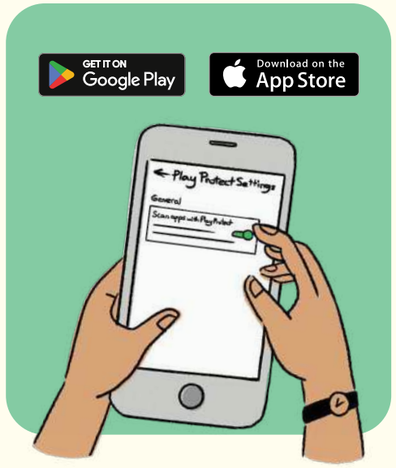
நச்சுநிரலைப் பயன்படுத்திச் செய்யப்படும் மோசடிகள்

இணையம்வழிக் குற்றம் புரிவோர், இலவசமாகப் பொருளை அனுப்பிவைக்க அல்லது தள்ளுபடிகள் பெறத் தங்களது செயலியைப் பதிவிறக்கம் செய்யச் சொல்லி தந்திரமாக நச்சுநிரலை உங்கள் சாதனத்தில் நிறுவ வைக்கக்கூடும்.

நச்சுநிரல் நிறுவப்பட்டவுடன், அவர்கள் உங்கள் சாதனத்தில் ஊடுருவி உங்களது வங்கி விவரங்களையும் கடவுச்சொற்களையும் ஒருமுறை பயன்படுத்தும் கடவுச்சொற்களையும் (OTPs) திருடி, அனுமதியின்றி பரிவர்த்தனைகள் செய்யமுடியும்.

கவனிக்க வேண்டியவை:

தள்ளுபடிகளுக்காக அல்லது இலவசச் சேவைகளுக்காக அதிகாரப்பூர்வமற்ற தளங்களிலிருந்து செயலியைப் பதிவிறக்கம் செய்யும்படி யாராவது உங்களிடம் சொன்னால் எச்சரிக்கையாக இருங்கள். இணையம்வழிக் குற்றம் புரிவோர் உங்களுக்கு நெருக்குதல் தரக்கூடும். செயலியைப் பதிவிறக்கம் செய்யப் படிப்படியாக வழிகாட்டவும் கூடும்.



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?

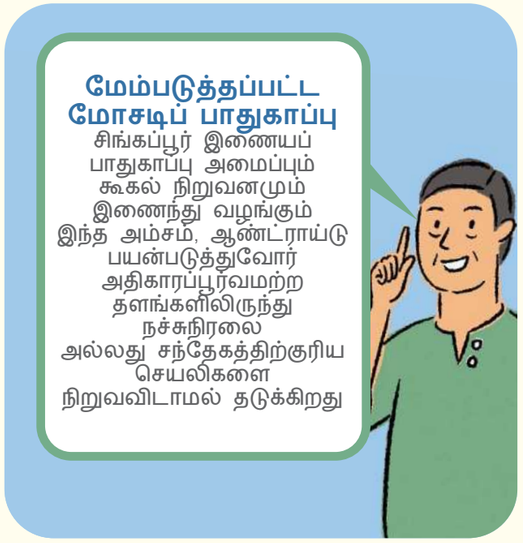
- Excessive and unexplained data use
- Random pop-ups or new apps not installed by you
- Noticeably slower responses or performance
- Battery drains unusually
- Unexpected or suspicious behaviours from the device such as auto-activation of camera or microphone

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.

நீங்கள் என்ன செய்ய முடியும்:

- தெரியாத செயலிகளுக்கு **அணுகல் அனுமதி வழங்காதீர்கள்**
- கூகல் பிளே ஸ்டோர் (ஆண்ட்ராய்டு) அல்லது ஆப்பிள் ஆப் ஸ்டோர் (ஐஓஎஸ்) போன்ற **அதிகாரப்பூர்வச் செயலி விநியோகத் தளங்களிலிருந்து மட்டுமே செயலிகளைப் பதிவிறக்கம் செய்யுங்கள்.** ஏனெனில், இந்தத் தளங்களால் நச்சுநிரல் உள்ள செயலிகளைக் கண்டுபிடித்து நீக்கமுடியும்



உங்கள் கைப்பேசியில் நச்சுநிரல் பரப்பப்பட்டிருக்கிறதா என்பதை எப்படித் தெரிந்துகொள்வது?

- தரவுப் பயன்பாடு காரணமின்றி வெகு அதிகமாக இருக்கிறது
- நீங்கள் நிறுவாத பாப்-அப் அல்லது புதிய செயலிகள் இருக்கின்றன
- இயக்கம் அல்லது செயலாற்றல் குறிப்பிடத்தக்க அளவு மெதுவாக இருக்கிறது
- வழக்கத்திற்கு மாறாக மின்சக்தி விரைவில் முடிந்துவிடுகிறது
- கைப்பேசி எதிர்பாராமல் அல்லது சந்தேகம் தரும் வகையில் செயல்படுகிறது.
- புகைப்படக் கருவி அல்லது ஒலிவாங்கி தாமாகச் செயல்படுகிறது

உங்கள் கைப்பேசியில் நச்சுநிரல் பரப்பப்பட்டிருந்தால் நீங்கள் என்ன செய்ய வேண்டும்?

- கைப்பேசியில் “airplane mode” செயல்படுத்தி, அருகலை இணைப்பை (Wi-Fi) அடைத்து வைத்திருங்கள்
- புதுப்பிக்கப்பட்ட நச்சுநிரல் தடுப்புச் செயலியைப் பயன்படுத்தி உங்கள் கைப்பேசியிலிருந்து நச்சுநிரலை நீக்குங்கள்
- வேறொரு நம்பகமான சாதனத்தைப் பயன்படுத்தி, வங்கி, சிங்பாஸ் அல்லது மத்திய சேம நிதிப் பரிவர்த்தனைகள் ஏதாவது அனுமதியின்றி செய்யப்பட்டிருக்கிறதா என்பதைச் சரிபாருங்கள்
- அனுமதியின்றி பரிவர்த்தனைகள் செய்யப்பட்டிருந்தால், உடனடியாக வங்கியிடமும் காவல்துறையிடமும் புகார் செய்யுங்கள்
- இவை அனைத்தையும் செய்த பிறகு, உங்கள் கைப்பேசியில் நச்சுநிரல் இல்லை என நீங்கள் நம்பினால், மீண்டும் கைப்பேசியைப் பயன்படுத்துங்கள். ஒரு முன்னெச்சரிக்கையாக, “factory reset” செய்து, முக்கியமான கடவுச்சொற்களை மாற்றலாம். அதற்குமுன் உங்கள் தரவுகளுக்குக் காப்புப்பிரதி எடுங்கள்

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!

ஆழ்நிலைப் போலிகள்

ஆழ்நிலைப் போலிகள் (deepfakes) என்பது ஆக்கமுறை செயற்கை நுண்ணறிவைப் (AI) பயன்படுத்தி மின்னிலக்க முறையில் உருவாக்கப்படும் அல்லது மாற்றியமைக்கப்படும் புகைப்படங்கள், காணொளிகள் அல்லது ஒலிப்பதிவுகளைக் குறிக்கிறது. தொழில்நுட்ப முன்னேற்றத்துடன், ஆழ்நிலைப் போலிகளும் அதிகம் நம்பும் அளவுக்கு உருவாகி வருகின்றன. இணைய மோசடிகளில், அதிகாரிகளையும் பிரபலங்களையும் போல் ஆள்மாறாட்டம் செய்து உங்களது தனிப்பட்ட விவரங்களை வெளியிட வைப்பதற்கு அல்லது மோசடியான பணப் பரிவர்த்தனைக்கு அனுமதி தரச் செய்வதற்கு இந்தத் தொழில்நுட்பம் பயன்படுத்தப்படுகிறது. இது திரும்பப் பெறமுடியாத பண இழப்புக்கு இட்டுச்செல்லக்கூடும்.

கவனிக்க வேண்டியவை:

- உள்ளடக்கங்கள் அதிகாரபூர்வமான அல்லது நம்பகமான தரப்பிலிருந்து வந்திருக்கிறதா என்பதைச் சரிபாருங்கள்
- பின்வரும் உள்ளடக்கம் குறித்து கூடுதல் கவனமாக இருங்கள்:
  - அவசரமான சொற்களின் பயன்பாடு ("உடனே அனுப்பு", "கடைசி வாய்ப்பு")
  - முக்கிய விவரங்களைக் கேட்டல் (அடையாள அட்டை எண், வங்கிக் கணக்கு, OTP)
  - பணம் அனுப்பச் சொல்லுதல்
- காணொளிகளில்/ஒலிப்பதிவுகளில் இயல்புக்கு மாறான அறிகுறிகள் இருக்கிறதா என்பதைக் கவனியுங்கள்:
  - முகத்தின் ஓரப்பகுதிகள் மங்கலாக இருப்பது
  - இயல்புக்கு மாறான கண் சிமிட்டல் அல்லது முக அசைவுகள்
  - உதட்டின் அசைவும் பேச்சும் பொருந்தாதிருப்பது

நீங்கள் என்ன செய்ய முடியும்:

- **நிதானித்துச், சிந்தித்துப் பாருங்கள்.** அவசரப்படாதீர்கள், குறிப்பாகக் குறுந்தகவல் அவசரமானதாக, பாதுகாப்பற்றதாக, அல்லது வழக்கத்திற்கு மாறானதாக இருந்தால்
- **தரப்பின் மூலத்தைச் சரிபாருங்கள்.** குறுந்தகவலில் கொடுக்கப்பட்டுள்ள தொலைபேசி எண்ணுக்குப் பதிலாக, உங்களுக்கு ஏற்கனவே தெரிந்த தொலைபேசி எண்ணை அல்லது வழியைப் (எ.கா. அதிகாரப்பூர்வத் தொலைபேசிச் சேவை, சேமித்து வைத்திருக்கும் தொலைபேசி எண்) பயன்படுத்தி குறுந்தகவல் அனுப்பியவரை அல்லது அமைப்பைத் தொடர்பு கொள்ளுங்கள்
- **முக்கிய விவரங்களைப் பகிராதீர்கள்.** உங்களது கடவுச்சொற்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள், முழுமையான வங்கி விவரங்கள் எதனையும் தொலைபேசி அழைப்பில், குறுந்தகவலில் அல்லது காணொளியில் வெளியிடாதீர்கள்
- **பணம் அனுப்பாதீர்கள்.** குடும்பத்தினர், நண்பர்களுடன் முதலில் கலந்து பேசுங்கள்

மேலும் தெரிந்து கொள்ளுங்கள்

ஆக்கமுறை செயற்கை நுண்ணறிவு, ஆழ்நிலைப் போலிகள் பற்றிய மேல்விவரங்களுக்கு QR குறியீட்டை ஸ்கேன் செய்யுங்கள்!

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.

இணையத்தில் பாதுகாப்பாக இருப்பது எப்படி

சிறந்த இணையப் பழக்கங்களைக் கடைப்பிடிப்பது, இணைய மோசடிகளில் நீங்கள் சிக்கிவிடாமல் பாதுகாக்க உதவும். மூன்று இணைய உதவிக்குறிப்புகளைக் கடைப்பிடித்து உங்களைப் பாதுகாத்துக் கொள்ளுங்கள்:

இரட்டை மறைசொல் முறையையும் வலுவான கடவுச் சொற்றொடரையும் பயன்படுத்துங்கள்

இரட்டை மறைசொல் முறையுடன் (2FA) வலுவான கடவுச் சொற்றொடரையும் சேர்த்துப் பயன்படுத்தும்போது, உங்களது இணையக் கணக்குகளுக்குக் கூடுதல் பாதுகாப்பு கிடைக்கும்.

இரட்டை மறைசொல் முறை, உங்கள் அடையாளத்தை உறுதிப்படுத்துவதற்கும் இணையக் கணக்குகளைப் பயன்படுத்துவதற்கும் ஒன்றுக்கு மேற்பட்ட விவரங்களைப் பயன்படுத்துகிறது.

வலுவான கடவுச் சொற்றொடரை உருவாக்குவது எப்படி:

படிநிலை 1: தனிப்பட்ட ஞாபகத்தில் இருந்து **5 வெவ்வேறு சொற்களைக் கோர்வையாகச் சேருங்கள்**

Bread → ihadbread**at8am**

படிநிலை 2: **பேரெழுத்துகள், சிற்றெழுத்துகள், எண்கள், சின்னங்கள் ஆகியவற்றைக் கலந்து பயன்படுத்துங்கள்** (குறைந்தது 12 எழுத்துருக்கள்)

ihadBREADat8am!

உங்கள் பெயர், அடையாள அட்டை எண் அல்லது பிறந்த தேதி போன்ற **எளிதில் பெறக்கூடிய தகவல்களைப் பயன்படுத்தாதீர்கள்.**

உங்களது கடவுச்சொற்களை யாருடனும் **பகிரவோ அல்லது எழுதி வைக்கவோ கூடாது.**

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.

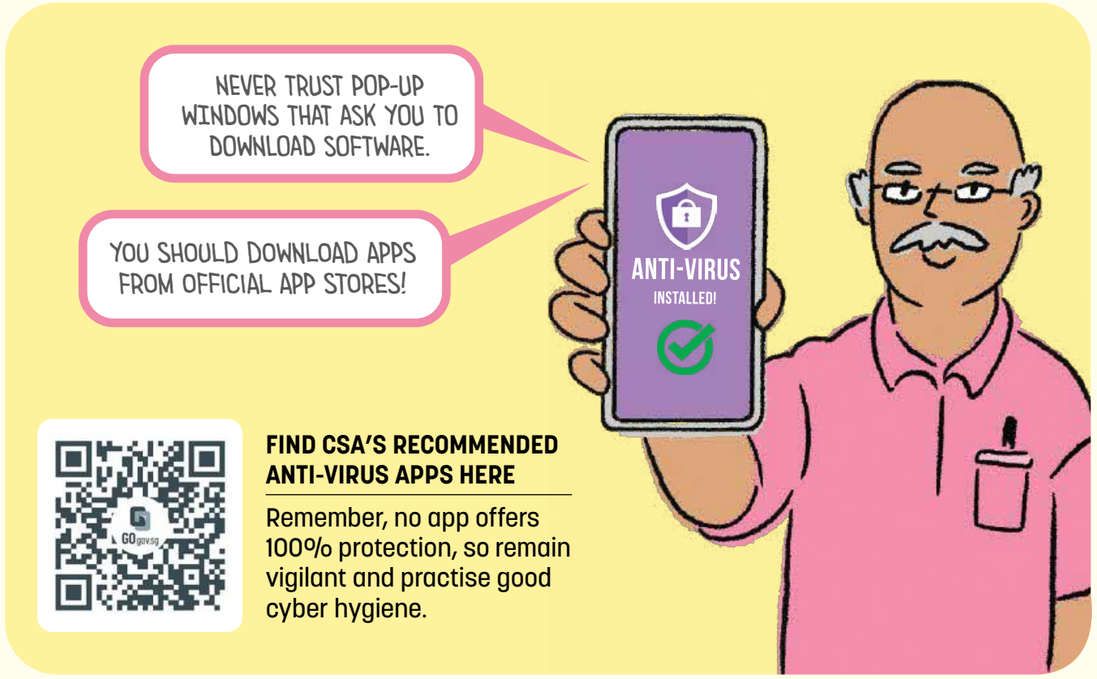
How to choose an Anti-Virus App

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.

மென்பொருளை உடனுக்குடன் புதுப்பித்திடுங்கள்

மென்பொருள் மற்றும் செயலிப் புதுப்பிப்புகளில் முக்கியமான பாதுகாப்புச் சீரமைப்புகள் இருக்கும். அவை உங்களது சாதனங்களைப் பாதுகாப்பாக வைத்திருக்க உதவும்.

மேலும் தெரிந்து கொள்ளுங்கள்

தானியக்கப் புதுப்பிப்புகளைச் செயல்படுத்தும் வழிமுறையைக் கண்டறிய இங்கே ஸ்கேன் செய்யுங்கள்!

ஸ்கேம்ஷீல்டு, நச்சுநிரல் தடுப்புச் செயலிகளை நிறுவுங்கள்

ஸ்கேம்ஷீல்டு என்பது மோசடிகளிலிருந்து தற்காத்துக் கொள்ள உதவும் தயாரிப்புகள் மற்றும் கருவிகளின் தொகுப்பாகும். மோசடி அழைப்புகளையும் குறுந்தகவல்களையும் கண்டுபிடித்துத் தடுப்பதற்கு இந்தச் செயலியைப் பதிவிறக்கம் செய்யுங்கள்.

நச்சுநிரல் தடுப்புச் செயலிகள் நச்சுநிரலையும் தகவல் திருடும் இணைப்புகளையும் கண்டுபிடிக்க உதவுகின்றன. உங்களது சாதனங்களையும் கணக்குகளையும் பாதுகாக்க அவை முக்கியம்.

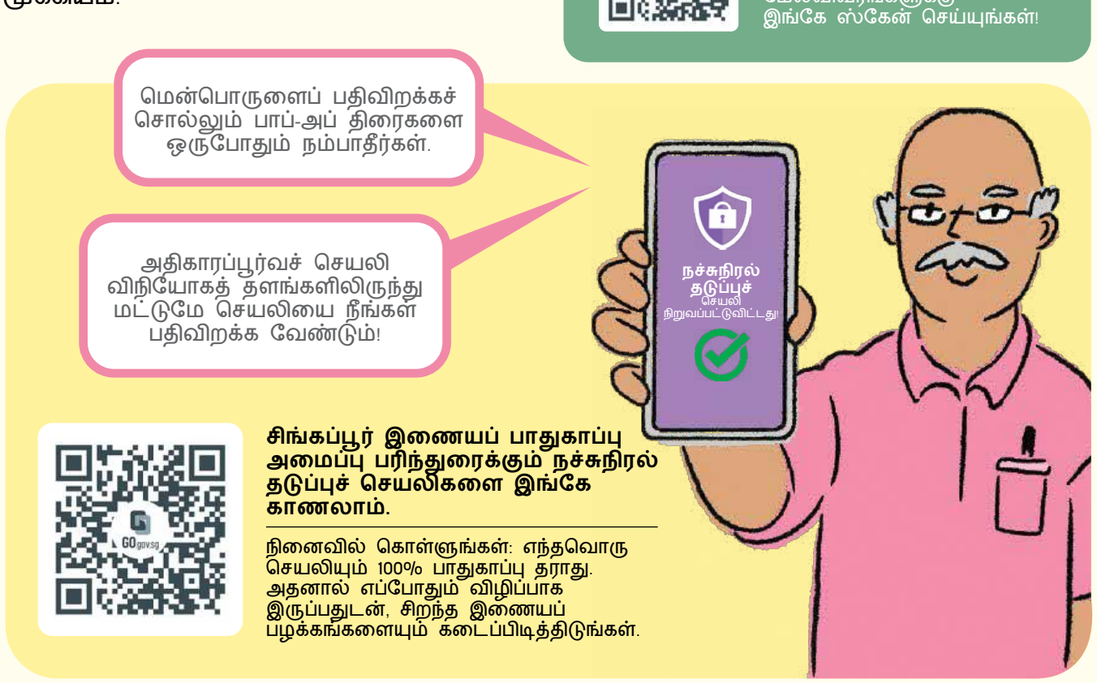
நச்சுநிரல் தடுப்புச் செயலியைத் தேர்ந்தெடுப்பது எப்படி

வெவ்வேறு வர்த்தகப் பெயர்களிலான நச்சுநிரல் தடுப்புச் செயலிகளின் இயக்கங்களும் ஆற்றல்களும் மாறுபட்டிருக்கும். நச்சுநிரல் தடுப்புச் செயலிகளைத் தேர்ந்தெடுப்பதற்கான சில உதவிக்குறிப்புகள்:

- கூகல் பிளே ஸ்டோர் (ஆண்ட்ராய்டு) அல்லது ஆப்பிள் ஆப் ஸ்டோர் (ஐஓஎஸ்) போன்ற **அதிகாரப்பூர்வச் செயலி விநியோகத் தளங்களிலிருந்து பதிவிறக்கம் செய்யுங்கள்**
- **பதிவிறக்கம் செய்வதற்குமுன் செயலியைப் பற்றிய கருத்துரைகளைப் படித்துப் பாருங்கள்.** செயலியைத் தயாரித்தவரின் நன்மதிப்பு, செயலியின் மதிப்பீடு, பதிவிறக்கங்களின் எண்ணிக்கை ஆகியவற்றைக் கவனத்தில் கொள்ளுங்கள்
- **கண்டுபிடித்து அகற்றும் ஆற்றல் கொண்ட செயலிகளைத் தேர்ந்தெடுங்கள்.** நிகழ்நேரத்தில் நச்சுநிரலைக் கண்டுபிடித்து (ஆண்ட்ராய்டு சாதனங்களுக்கு மட்டும்) அகற்றக்கூடிய ஆற்றல் கொண்ட செயலிகளைத் தேடுங்கள்

மேலும் தெரிந்து கொள்ளுங்கள்

ஸ்கேம்ஷீல்டு பற்றிய மேல்விவரங்களுக்கு இங்கே ஸ்கேன் செய்யுங்கள்!



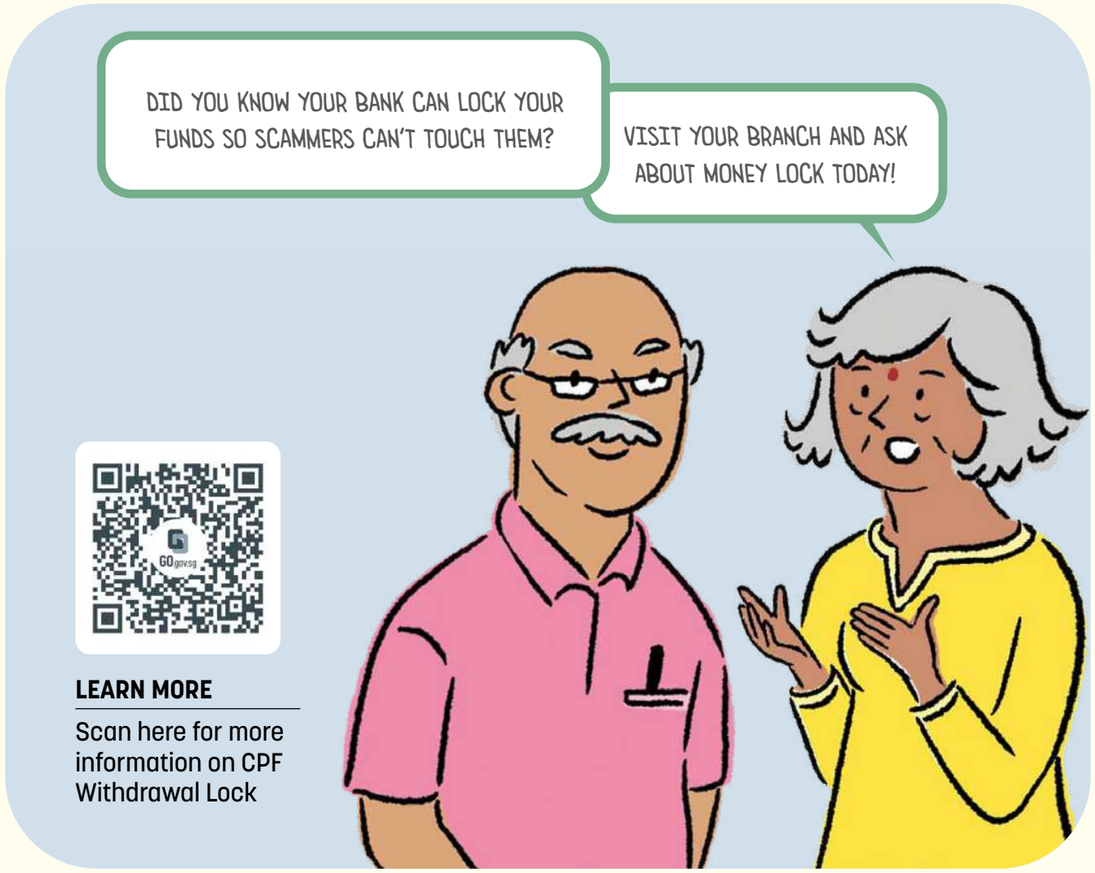
சிங்கப்பூர் இணையப் பாதுகாப்பு அமைப்பு பரிந்துரைக்கும் நச்சுநிரல் தடுப்புச் செயலிகளை இங்கே காணலாம்.

நினைவில் கொள்ளுங்கள்: எந்தவொரு செயலியும் 100% பாதுகாப்பு தராது. அதனால் எப்போதும் விழிப்பாக இருப்பதுடன், சிறந்த இணையப் பழக்கங்களையும் கடைப்பிடித்திடுங்கள்.

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.

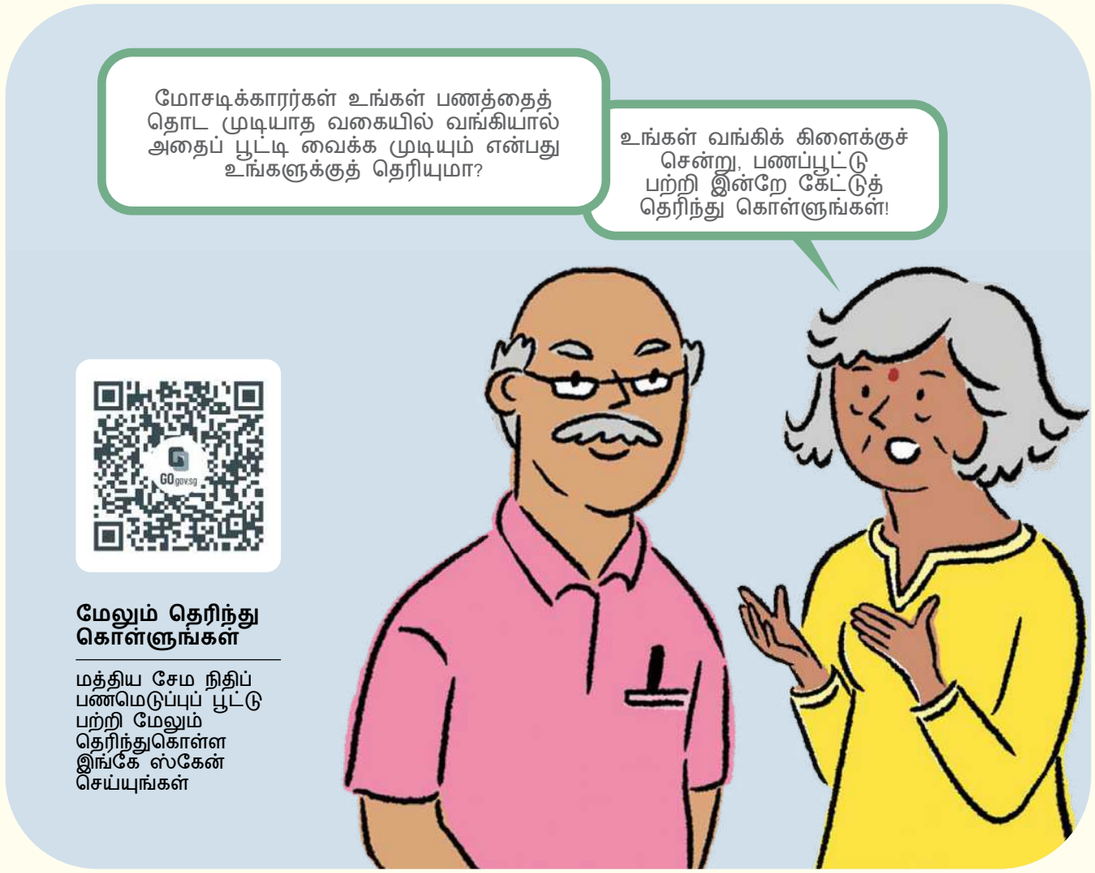
- **Money Lock** was introduced by the local banks to safeguard your bank account and guard against scams by allowing funds to be 'locked' so they cannot be transferred digitally. Check with your bank on how to activate this feature.
- The **CPF Withdrawal Lock** feature allows members aged 55 and above 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.



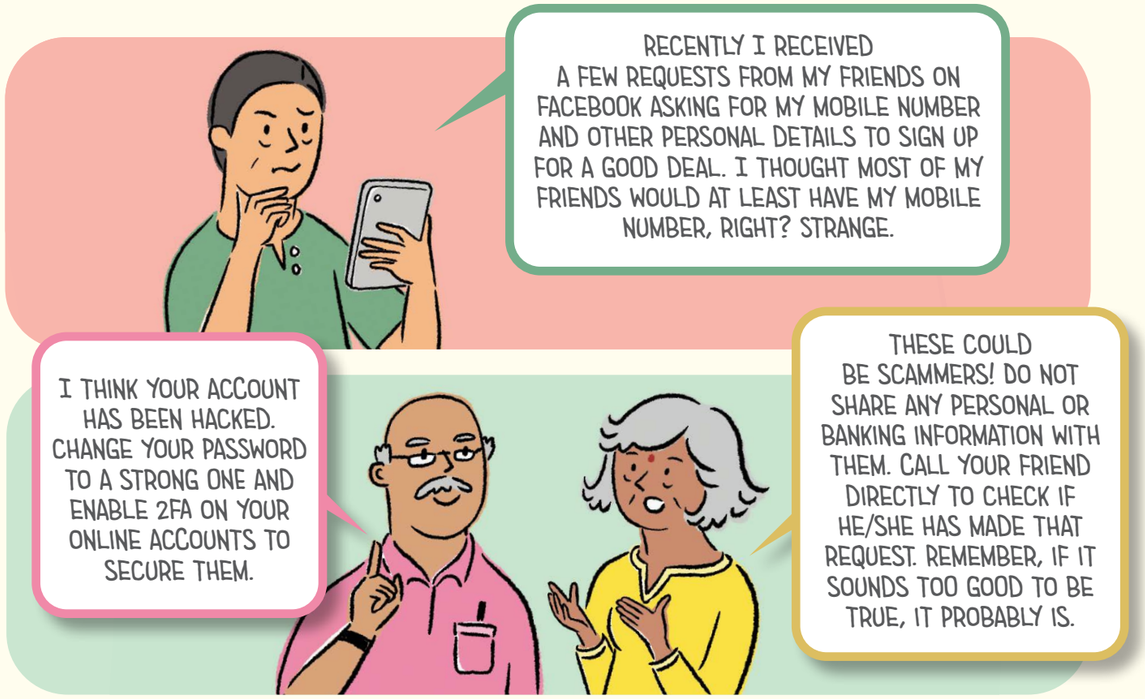
உங்களைப் பாதுகாத்துக் கொள்ள நீங்கள் வேறு என்னவெல்லாம் செய்யமுடியும்?

சிறந்த இணையப் பழக்கங்களைக் கடைப்பிடிப்பதோடு, நீங்கள் உங்களது செயலிகளில் செயல்படுத்த கூடுதல் பாதுகாப்பு அம்சங்களும் இருக்கின்றன. மோசடிச் சம்பவம் நேரும்போது உங்களது சேமிப்புகளைப் பாதுகாத்து, உத்தேச இழப்புகளைக் குறைப்பதற்கு இந்த அம்சங்கள் துணைபுரியும்.

- உங்கள் வங்கிக் கணக்கைப் பாதுகாக்கவும், **பணத்தைப் "பூட்டிவைத்து"** மோசடிகளைத் தடுக்கவும் உள்ளூர் வங்கிகள் பணப்பூட்டை ("Money Lock") அறிமுகப்படுத்தின. நீங்கள் "பூட்டிவைக்கும்" பணத்தை மின்னிலக்க முறையில் வேறொரு கணக்குக்கு மாற்றமுடியாது. இந்தப் பாதுகாப்பு அம்சத்தை எவ்வாறு செயல்படுத்துவது என்பதை உங்கள் வங்கியிடம் கேட்டுத் தெரிந்து கொள்ளுங்கள்.
- **மத்திய சேம நிதிப் பணமெடுப்புப் பூட்டுடன்**, 55 வயதுக்கு மேற்பட்ட உறுப்பினர்கள் இணையம்வழி மத்திய சேம நிதிக் கணக்கிலிருந்து பணம் எடுப்பதை உடனடியாக முடக்கலாம். உங்களது மத்திய சேம நிதிக் கணக்கின் மூலம் இந்தப் பூட்டை நீங்கள் எப்போது வேண்டுமானாலும் செயல்படுத்தலாம். அதோடு, உங்களது சேமிப்பைப் பாதுகாக்க அன்றாடப் பணமெடுப்பு வரம்பையும் நிர்ணயிக்கலாம்.



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



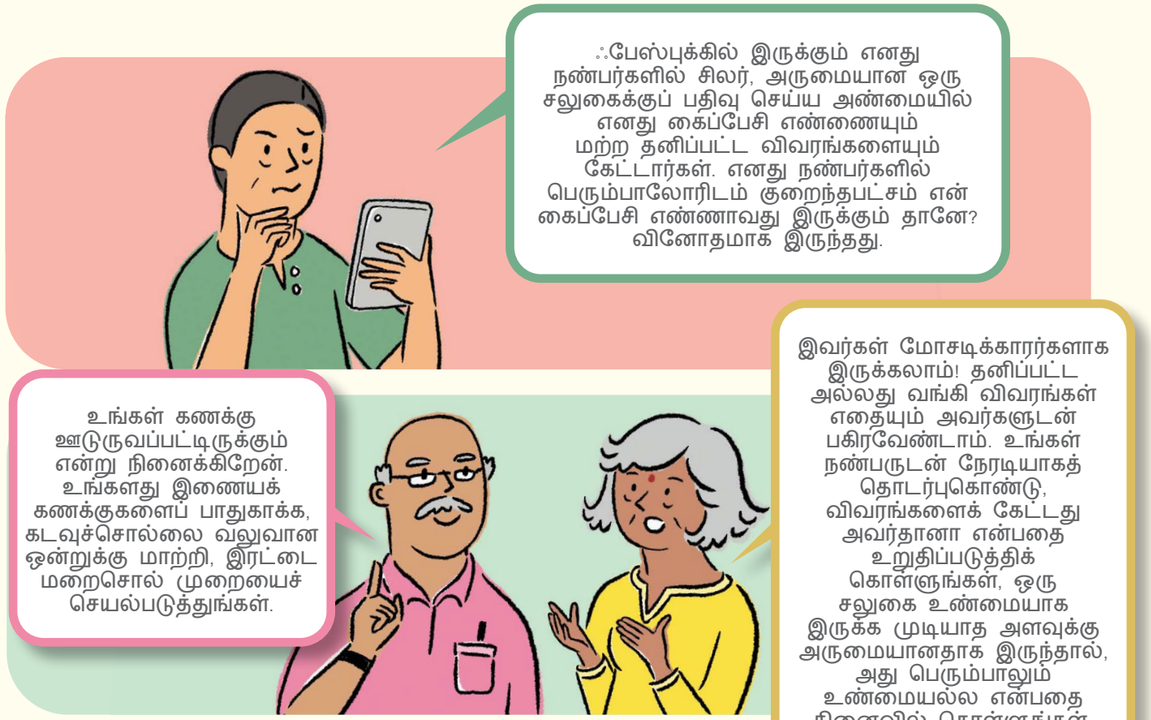
If you still have access to your account,

- **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.

நீங்கள் தகவல் திருட்டு மோசடிக்கு உள்ளானால் என்ன செய்யவேண்டும்?



உங்கள் கணக்கை உங்களால் இன்னமும் பயன்படுத்த முடிந்தால்,

- அந்தக் கணக்குடன் இணைக்கப்பட்ட **அனைத்து சாதனங்களிலும் கணக்கிலிருந்து வெளியேறிவிடுங்கள்**
- **உங்களது கடவுச்சொல்லை உடனடியாக மாற்றிவிட்டு,** இரட்டை மறைசொல் முறையைச் செயல்படுத்துங்கள்

உங்கள் கணக்கை உங்களால் பயன்படுத்த முடியாவிட்டால்,

- **சம்பந்தப்பட்ட தளத்துடன்,** எடுத்துக்காட்டாக வங்கி அல்லது சமூக ஊடகத் தளத்துடன், **தொடர்புகொண்டு,** பிரச்சனையைப் புகார் செய்து, உங்கள் கணக்கை மீட்பதற்கு உதவி கேளுங்கள்
- உங்களது **கடன் / பண அட்டையைப் பயன்படுத்தி மோசடி செய்யப்பட்டிருந்தால்,** உடனடியாக வங்கியிடம் **தெரியப்படுத்தி,** அட்டையை ரத்து செய்யுங்கள்.
- பண இழப்பு ஏற்பட்டிருந்தால், அருகிலுள்ள அக்கம் பக்கக் காவல் நிலையத்தில் அல்லது அக்கம் பக்கக் காவல் சாவடியில் அல்லது www.police.gov.sg/e-services இணையத்தளத்தில் **புகார் செய்யுங்கள்**
- நீங்கள் சம்பவம் பற்றி புகார் அளிக்க விரும்பினால், www.csa.gov.sg/singcert/reporting எனும் **CSA SingCERT இணையப்பக்கத்திற்குச் செல்லுங்கள்**
- உங்கள் கணக்கு அத்துமீறப்பட்டிருந்தால், உங்களைப் போல் பாசாங்கு செய்பவர் உங்களது தொடர்புகளுடன் தொடர்பு கொள்ளக்கூடும். எனவே, உங்களிடமிருந்து ஏதாவது கோரிக்கைகள் கிடைத்தால் புறக்கணிக்கும்படியும், தனிப்பட்ட விவரங்களைப் பகிர வேண்டாம் என்றும் **உங்கள் குடும்பத்தாரையும் நண்பர்களையும் எச்சரித்திடுங்கள்.**

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?

நான் மோசடிக்கு உள்ளாகி விடுவேனோ எனக் கவலையாக இருக்கிறது. பேசாமல் தகவல்கள் அல்லது அழைப்புகள் எதற்கும் பதில் அளிக்காமல் இருக்கலாம் என்று நினைக்கிறேன்.

கவலை வேண்டாம். நாம் விழிப்பாக இருந்தாலே போதும். நிறுத்தி நிதானித்துச் சரிபாருங்கள். குடும்பத்தினரை அல்லது நண்பரை அழைத்து ஆலோசனை கேளுங்கள்.

ஆமாம், அதோடு கடவுச்சொற்களையும் ஒருமுறை பயன்படுத்தும் கடவுச்சொற்களையும் யாரிடமும் சொல்லாதீர்கள். என்னிடம் கூடத்தான், சரியா?

Better cyber safe than sorry

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

மேல்விவரம் அறிய, சிங்கப்பூர் இணையப் பாதுகாப்பு அமைப்பின் எஸ்ஜி இணையப் பாதுகாப்புமிக்க மூத்தோர் இணையப்பக்கத்தை அல்லது ஸ்கேம்ஷீல்டு இணையப்பக்கத்தை நாடுங்கள்.

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

Get more cyber tips at:

இன்னும் பல இணையக் குறிப்புகளுக்கு:

For the latest scam info, visit:

மோசடி பற்றிய அண்மைத் தகவலுக்கு, நாடுங்கள்: