BETTER CYBER SAFE THAN SORRY

A GUIDE TO STAYING SAFE ONLINE

பின்னர் வருந்தாமல் இப்போதே இணையத்தில் பாதுகாப்பாக இருப்பதே நல்லது

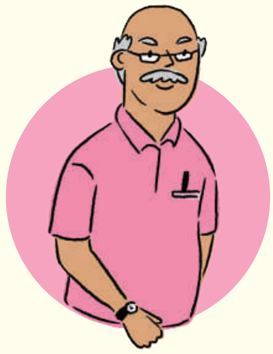
இணையத்தில் பாதுகாப்பாக இருக்க ஒரு வழிகாட்டி

CSA SINGAPORE

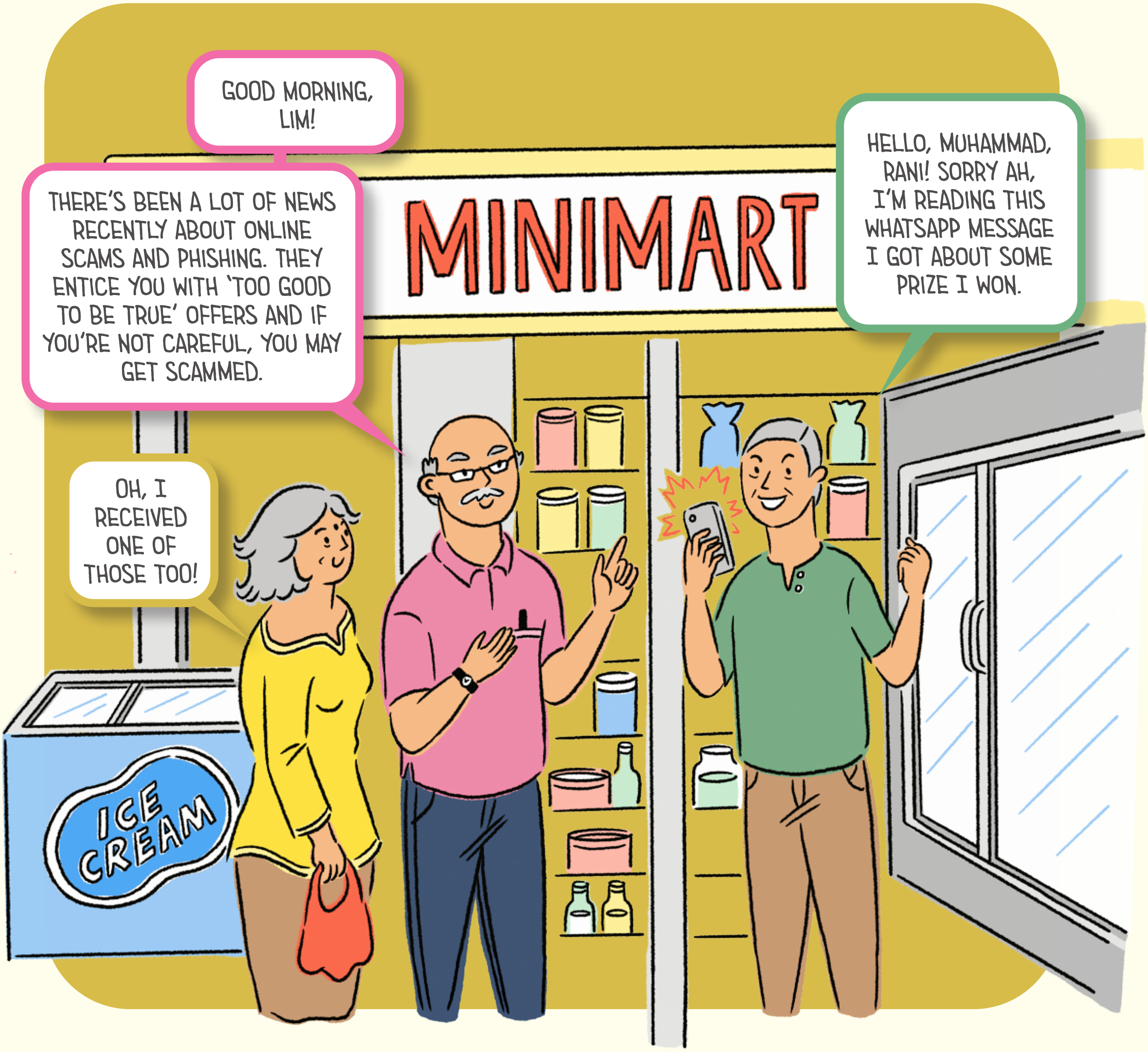
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

LIM
Taxi Driver

RANI
Administrative Assistant



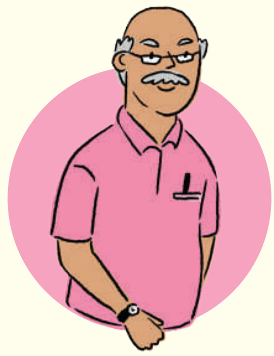
MUHAMMAD
Retired Teacher



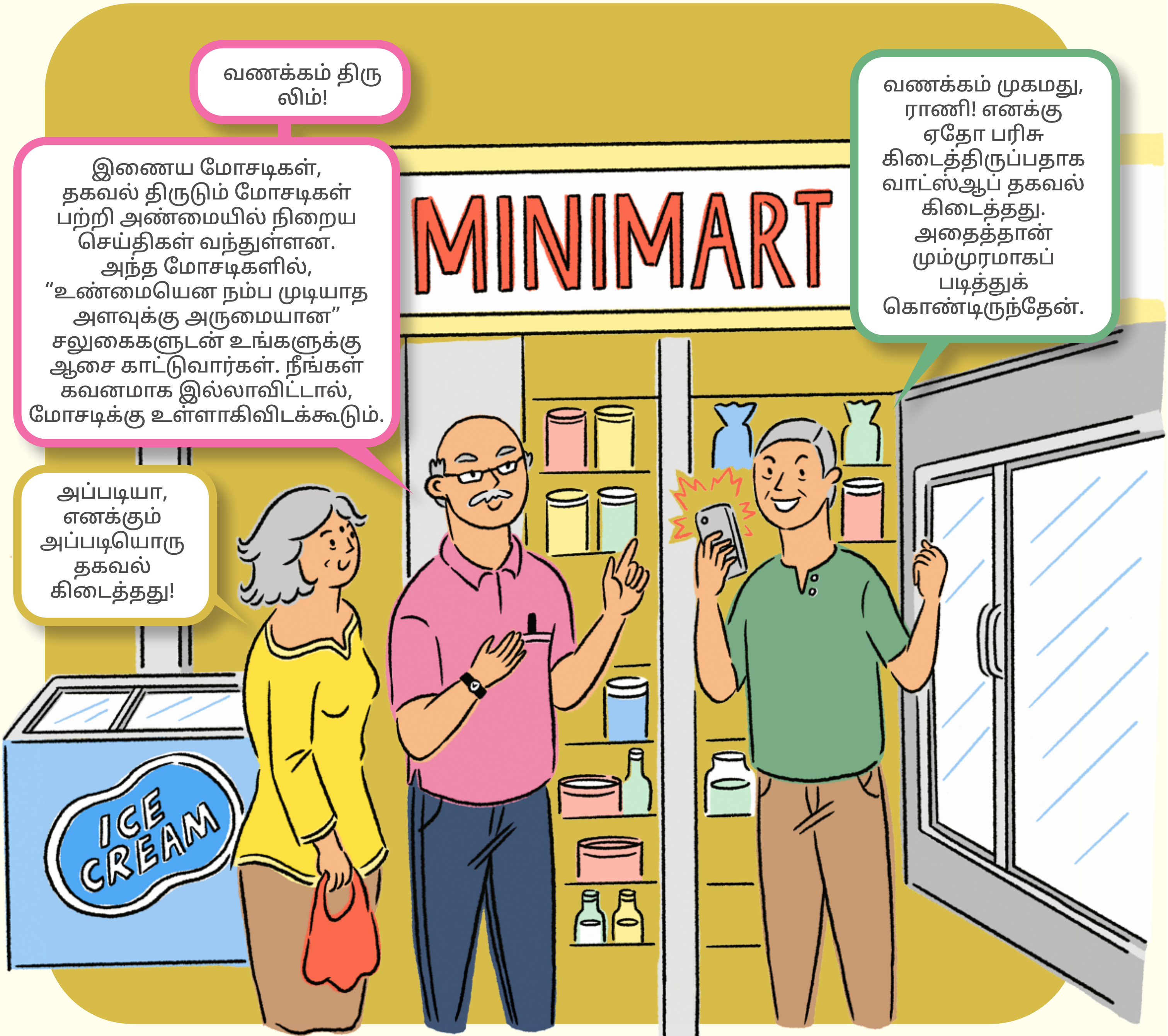
The increased use of smartphones and other smart devices has made life more convenient but at the same time, there are also cybercrimes which we need to be aware of. This handbook will arm you with the information you need to protect yourselves from cyber threats.

திரு லிம்
டாக்சி ஓட்டுநர்

ராணி
நிர்வாக உதவியாளர்



முகமது
ஓய்வுபெற்ற ஆசிரியர்



திறன்பேசிகளும் மற்ற அறிவார்ந்த சாதனங்களும் அதிகமாகப் பயன்படுத்தப்படுவதால் வாழ்க்கை அதிக வசதியாக இருந்தாலும், இணையக் குற்றச்செயல்கள் நடப்பதால் நாம் விழிப்பாக இருப்பது அவசியம். இணைய மிரட்டல்களிலிருந்து உங்களைப் பாதுகாத்துக் கொள்வதற்குத் தேவைப்படும் தகவல்களை இந்தக் கையேடு வழங்குகிறது.

WHAT DANGERS ARE WE EXPOSED TO?

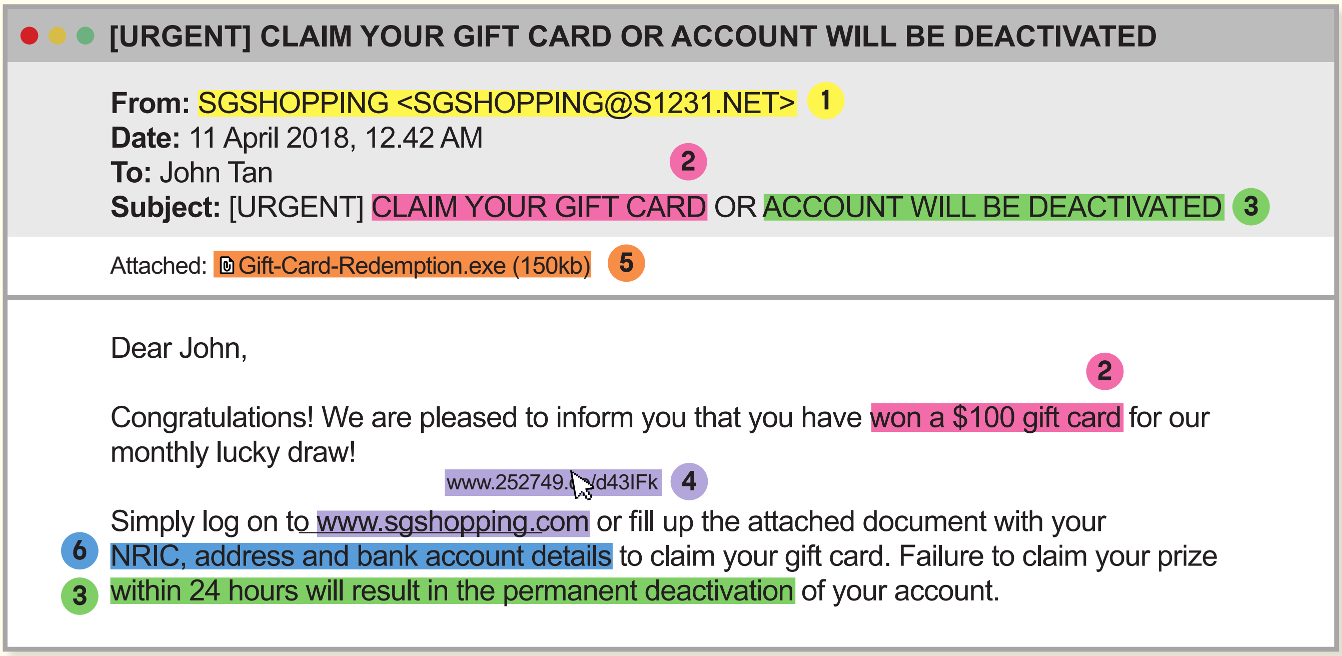
As we go online more often to do banking or shopping at our own convenience, we are at risk from cyber threats in the form of online scams and data theft.

WHAT IS PHISHING?

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

Cyber criminals may impersonate organisations such as the government or banks and contact you, claiming that there are issues requiring your immediate attention. They may do so via calls, SMSes, messaging apps, emails or pop-up ads.

How to spot phishing attempts



1

Unexpected emails & text messages via Whatsapp, SMS

2

Promise of attractive rewards which sound too good to be true

3

Use of urgent or threatening language

4

Mismatched & misleading information

5

Suspicious links or attachments

6

Request for confidential information e.g. personal or banking information, passwords or One-Time Password (OTP)

நாம் என்னென்ன ஆபத்துகளுக்கு உள்ளாகக்கூடும்?

வங்கிச்சேவைக்காக அல்லது பொருள் வாங்குவதற்காக நாம் இணையத்தை அதிகமாகப் பயன்படுத்துவதால், இணைய மோசடிகள், தகவல் திருட்டுகள் போன்ற இணைய மிரட்டல்களை எதிர்நோக்குகிறோம்.

தகவல் திருட்டு என்பது என்ன?

தகவல் திருட்டு (phishing) என்பது இணையக் குற்றச்செயல்கள் புரிவோர் பயன்படுத்தும் ஓர் உத்தி. இதைப் பயன்படுத்தி கடவுச்சொற்கள், ஒருமுறை பயன்படுத்தும் கடவுச்சொற்கள் (OTPs) அல்லது வங்கிக் கணக்கு எண்கள் போன்ற தனிப்பட்ட, நிதித் தகவல்களை வெளியிட வைப்பார்கள்.

இணையம்வழி குற்றம் புரிவோர், அரசாங்கம் அல்லது வங்கிகள் போன்ற அமைப்புகளைச் சேர்ந்த அதிகாரிகள்போல் ஆள்மாறாட்டம் செய்து உங்களுடன் தொடர்பு கொள்ளக்கூடும். நீங்கள் உடனடியாகக் கவனிக்க வேண்டிய சில விவகாரங்கள் இருப்பதாக அவர்கள் உங்களிடம் சொல்லக்கூடும். தொலைபேசி அழைப்புகள், குறுந்தகவல்கள், செயலிவழித் தகவல்கள், மின்னஞ்சல்கள் அல்லது பாப்-ஆப் விளம்பரங்கள் மூலம் அவர்கள் அவ்வாறு செய்யக்கூடும்.

தகவல் திருடும் முயற்சிகளை எப்படி கண்டுகொள்வது

[அவசரம்] உங்களது அன்பளிப்பு அட்டையைப் பெற்றுக் கொள்ளுங்கள் அல்லது கணக்கு துண்டிக்கப்பட்டுவிடும்

அனுப்புநர்: SGSHOPPING <SGSHOPPING@S1231.NET> 1
தேதி: 11 ஏப்ரல் 2018, காலை 12.42 மணி
பெறுநர்: ஜான் டான் 2
தலைப்பு: [அவசரம்] உங்களது அன்பளிப்பு அட்டையைப் பெற்றுக் கொள்ளுங்கள் அல்லது கணக்கு துண்டிக்கப்பட்டுவிடும் 3

இணைப்பு: Gift-Card-Redemption.exe (150kb) 5

அன்பார்ந்த ஜான்,

2 வாழ்த்துக்கள்! எங்களது மாதாந்தர அதிர்ஷ்டக் குலுக்கலில் நீங்கள் $100 பெறுமானமுள்ள அன்பளிப்பு அட்டையை வென்றிருப்பதாகத் தெரிவிப்பதில் மகிழ்ச்சி அடைகிறோம்!

www.252749.co/d43IFk 4

6 உங்களது அன்பளிப்பு அட்டையைப் பெற்றுக்கொள்ள www.sgshopping.com இணையத்தளத்திற்குச் செல்லுங்கள் அல்லது இணைக்கப்பட்டுள்ள படிவத்தில் உங்கள் அடையாள அட்டை எண், முகவரி, வங்கிக் கணக்கு விவரங்களை நிரப்புங்கள். உங்களது பரிசை 24 மணி நேரத்திற்குள் பெற்றுக்கொள்ளாவிட்டால் உங்கள் கணக்கு நிரந்தரமாகத் துண்டிக்கப்பட்டுவிடும். 3

1

வாட்ஸ்ஆப், குறுந்தகவல் வழியாக எதிர்பாராமல் வரும் மின்னஞ்சல்கள் அல்லது குறுந்தகவல்கள்

2

நம்பமுடியாத அளவுக்கு அருமையான வெகுமதிகள் வழங்கப்படும் என வாக்குறுதியளிப்பது

3

அவசரப்படுத்தும் அல்லது மிரட்டும் வார்த்தைகளைப் பயன்படுத்துதல்

4

பொருந்தாத மற்றும் தவறாக வழிநடத்தக்கூடிய தகவல்கள்

5

சந்தேகத்தை உண்டாக்கும் இணைப்புகள்

6

இரகசியத்தன்மை வாய்ந்த தகவல்களைக் கோருதல் - எடுத்துக்காட்டாக, தனிப்பட்ட அல்லது வங்கி விவரம், கடவுச்சொற்கள் அல்லது ஒருமுறை பயன்படுத்தும் கடவுச்சொல் (OTP) போன்றவற்றைக் கேட்பது

QR CODE PHISHING

Cyber criminals may also trick you to scan a QR code that leads to a website requesting for your information. They may also embed QR codes with malware* to steal information from your mobile device.

- DO NOT SHARE any personal or financial information, unless you are sure that it is a legitimate request.
- DO NOT SCAN QR codes that are in the form of stickers or flyers placed randomly in public places (especially if they offer vouchers or discounts), or look like they have been tampered with.

When making e-payments with QR codes:

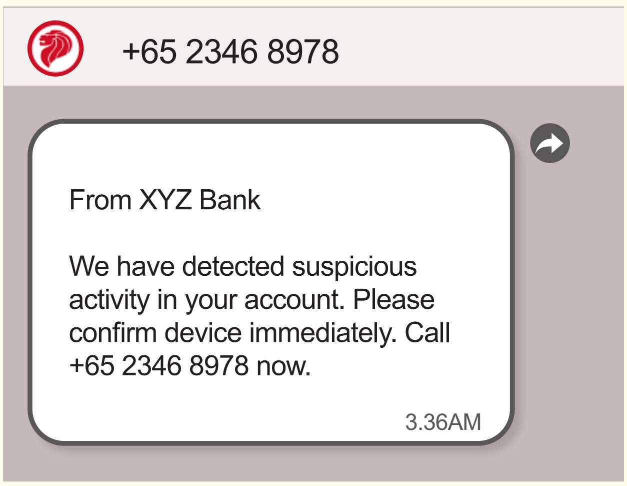
- USE ONLY OFFICIAL E-payment apps (e.g. DBS Paylah!, GrabPay).
- SET UP BANK TRANSACTION ALERTS by setting up email or SMS notifications to help you keep track of transactions.
- CHECK that the QR code for payment is not tampered with.

** Malware is a type of software that infects your devices and causes damage, including stealing your information, corrupting and even deleting your data.*

HOW TO SPOT PHISHING/ONLINE SCAMS

IMPERSONATION SCAMS

- In TECH SUPPORT SCAMS, scammers may claim to be officers from CSA, the Police or a telco investigating suspicious activity on your network.
- In BANK PHISHING SCAMS, scammers pretend to be bank employees, asking you to follow urgent instructions in order to address some bank account or technical issues or provide personal particulars for a non-existent offer.
- In SOCIAL MEDIA IMPERSONATION SCAMS, scammers may pretend to be your friends, family or colleagues and contact you on social media, asking for your personal details or OTPs sent to you 'by mistake'.
- In WHATSAPP ACCOUNT TAKEOVER SCAMS, scammers may pretend to be your contacts and request for a six-digit verification code to be sent to them.



QR குறியீட்டுடன் தகவல் திருட்டு

இணையம்வழி குற்றம் புரிவோர், உங்களை ஏமாற்றி ஒரு QR குறியீட்டை ஸ்கேன் செய்யவும் வைக்கக்கூடும். அந்தக் குறியீடு ஓர் இணையப்பக்கத்திற்கு இட்டுச்செல்லும். அந்த இணையப்பக்கம் உங்கள் தகவல்களைக் கேட்கும். அதுமட்டுமன்றி, உங்கள் சாதனத்திலிருந்து தகவல் திருடுவதற்காக, QR குறியீட்டில் நச்சுநிரலையும்* அவர்கள் பதித்து வைத்திருக்கக்கூடும்.

- உண்மையான கோரிக்கையா என உங்களுக்கு உறுதியாகத் தெரியாவிட்டால், தனிப்பட்ட அல்லது நிதித் தகவல்கள் எதனையும் பகிராதீர்கள்.
- பொது இடங்களில் ஆங்காங்கே வைக்கப்பட்டிருக்கும் அல்லது திருத்தம் செய்யப்பட்டிருப்பதுபோல் தோன்றும் ஒட்டுவில்லைகளில் அல்லது சிற்றேடுகளில் உள்ள QR குறியீடுகளை ஸ்கேன் செய்யாதீர்கள் (குறிப்பாக, அவை பற்றுச்சீட்டுகள் அல்லது தள்ளுபடிகள் வழங்கினால்).

QR குறியீடுகளுடன் மின்னியல் முறையில் கட்டணம் செலுத்தும்போது:

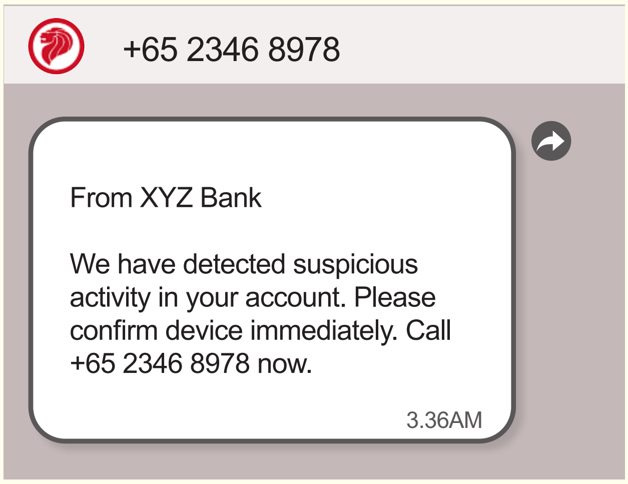
- அதிகாரபூர்வமான மின்கட்டணச் செயலிகளை மட்டுமே பயன்படுத்துங்கள் (எ.கா. டிபிஎஸ் பேலா!, கிராப்பே).
- பரிவர்த்தனைகளைக் கண்காணிப்பதற்கு உதவியாக, வங்கிப் பரிவர்த்தனைகள் பற்றி மின்னஞ்சல்வழி அல்லது குறுந்தகவல்வழி தகவல் பெறுவதற்கு ஏற்பாடு செய்யுங்கள்.
- கட்டணம் செலுத்துவதற்கான QR குறியீட்டில் ஏதாவது திருத்தம் செய்யப்பட்டிருக்கிறதா என்பதைக் கவனித்திடுங்கள்.

** நச்சுநிரல் என்பது உங்களது சாதனங்களைச் சேதப்படுத்தி, உங்களது தகவல்களைத் திருடி, சாதனத்தின் செயல்பாட்டைப் பாதிப்பதோடு, தகவல்களையும் அழித்துவிடக்கூடிய ஒரு வகையான மென்பொருள்.*

தகவல் திருட்டு / இணைய மோசடிகளை எப்படி கண்டுகொள்வது

ஆள்மாறாட்ட மோசடிகள்

- தொழில்நுட்ப ஆதரவு மோசடிகளில், இணையப் பாதுகாப்பு அதிகாரி, காவல்துறை அதிகாரி, அல்லது உங்கள் கட்டமைப்பில் சந்தேகத்திற்குரிய நடவடிக்கைகளை விசாரிக்கும் தொலைத்தொடர்பு நிறுவன அதிகாரி என மோசடிக்காரர்கள் சொல்லிக் கொள்ளக்கூடும்.
- வங்கி தகவல் திருட்டு மோசடிகளில், வங்கி ஊழியர்களைப் போல் பாசாங்கு செய்யும் மோசடிக்காரர்கள், வங்கிக் கணக்கு அல்லது தொழில்நுட்பப் பிரச்சனைகளுக்குத் தீர்வு காண அவசரமாகச் சில வழிமுறைகளைப் பின்பற்றுமாறு அல்லது இல்லாத ஒரு சலுகைக்காகத் தனிப்பட்ட விவரங்களைத் தெரிவிக்குமாறு சொல்வார்கள்.
- சமூக ஊடக ஆள்மாறாட்ட மோசடிகளில், மோசடிக்காரர்கள் உங்களது நண்பர்கள், குடும்பத்தினர் அல்லது சக ஊழியர்களைப் போல் பாசாங்கு செய்து, சமூக ஊடகத்தில் உங்களுடன் தொடர்பு கொண்டு, தனிப்பட்ட விவரங்களை அல்லது “தவறுதலாக” உங்களுக்கு அனுப்பப்பட்ட ஒருமுறை பயன்படுத்தும் கடவுச்சொல்லைக் கேட்பார்கள்.
- வாட்ஸ்ஆப் கணக்கைக் கைப்பற்றும் மோசடிகளில், மோசடிக்காரர்கள் உங்களது தொடர்புகளில் ஒருவரைப் போல் பாசாங்கு செய்து, ஆறு இலக்கச் சரிபார்ப்புக் குறியீட்டைத் தங்களுக்கு அனுப்பி வைக்கச் சொல்வார்கள்.

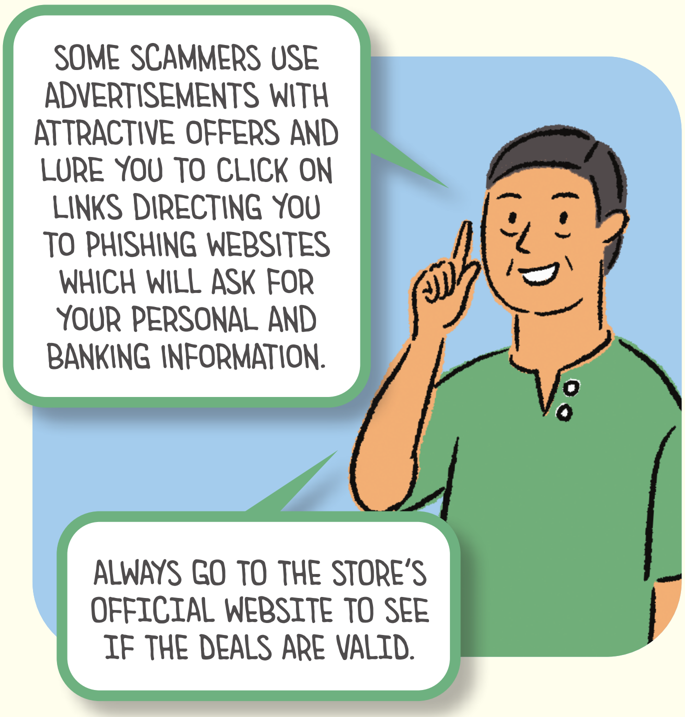


E-COMMERCE SCAM

Using huge discounts and offers, these scammers will insist on immediate payment or bank transfers before delivery. Once they have received the money, they will be uncontactable.

What can you do?

- PURCHASE ONLY FROM REPUTABLE SITES.
- PAY THROUGH THE SHOPPING PLATFORM. This way, the seller receives payment only after you receive your goods.
- BE ON YOUR GUARD always, and rethink the purchase if the deal is too good to be true.



If you or someone you know has received a phishing message...

- DO NOT PANIC. Call your family members or friends, or call the Anti-Scam helpline at 1800-722-6688 for advice.
- DO NOT ANSWER incoming calls showing a '+' sign if you are not expecting overseas calls.
- DO NOT INSTALL any software if you are 'advised' to.
- DO NOT SHARE YOUR PASSWORD, OTP or personal and banking information.
- DO NOT SEND MONEY to anyone.
- DO NOT CLICK on any attachment or link in the message. Delete it.
- ENABLE TWO-STEP VERIFICATION IN WHATSAPP as an additional layer of security.
- VERIFY SUSPICIOUS CALLS OR MESSAGES by calling government/ business' official hotline or official app/website directly. Do not contact the organisation via the contact details provided in the call or message.
- NOTE that government officials will never demand immediate payment online or instruct you to transfer money to any local or foreign bank account, or disallow you from hanging up a call.
- REFER to the list of trusted government-related websites at **www.gov.sg/trusted-sites** if the link or email address does not have "**.gov.sg**" in them.

இணைய விற்பனை மோசடி

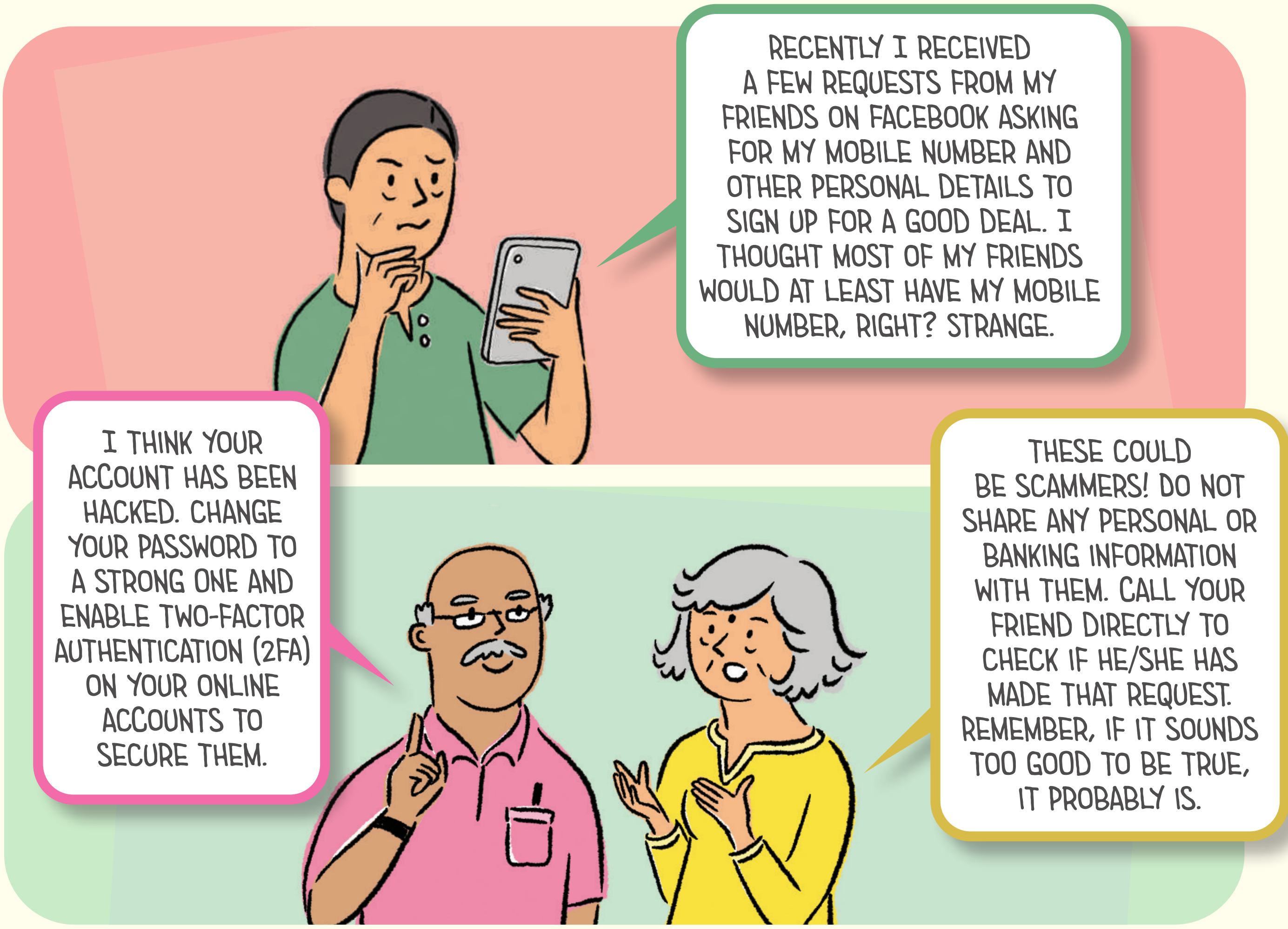
மாபெரும் விலைத் தள்ளுபடிகளையும் சலுகைகளையும் பயன்படுத்தும் இந்த மோசடிக்காரர்கள், உடனடியாக அல்லது பொருளை அனுப்பி வைப்பதற்கு முன்பாகப் பணத்தைச் செலுத்தியாக வேண்டும் என வற்புறுத்துவார்கள். பணம் கைக்குக் கிடைத்ததும், அவர்களுடன் தொடர்புகொள்ள இயலாமல் போய்விடும்.

நீங்கள் என்ன செய்யமுடியும்?

- நம்பகமான இணையத்தளங்களில் மட்டுமே வாங்குங்கள்.
- பொருள் வாங்கும் இணையத்தளத்தின் வழியாகப் பணம் செலுத்துங்கள். இதன்வழி, பொருள் உங்களுக்குக் கிடைத்த பிறகுதான் விற்பனையாளருக்குப் பணம் கிடைக்கும்.
- எப்போதும் விழிப்பாக இருங்கள். ஒரு விற்பனைச் சலுகை நம்ப முடியாத அளவுக்கு அருமையாக இருந்தால், வாங்குவதா இல்லையா என மீண்டும் யோசித்துப் பாருங்கள்.

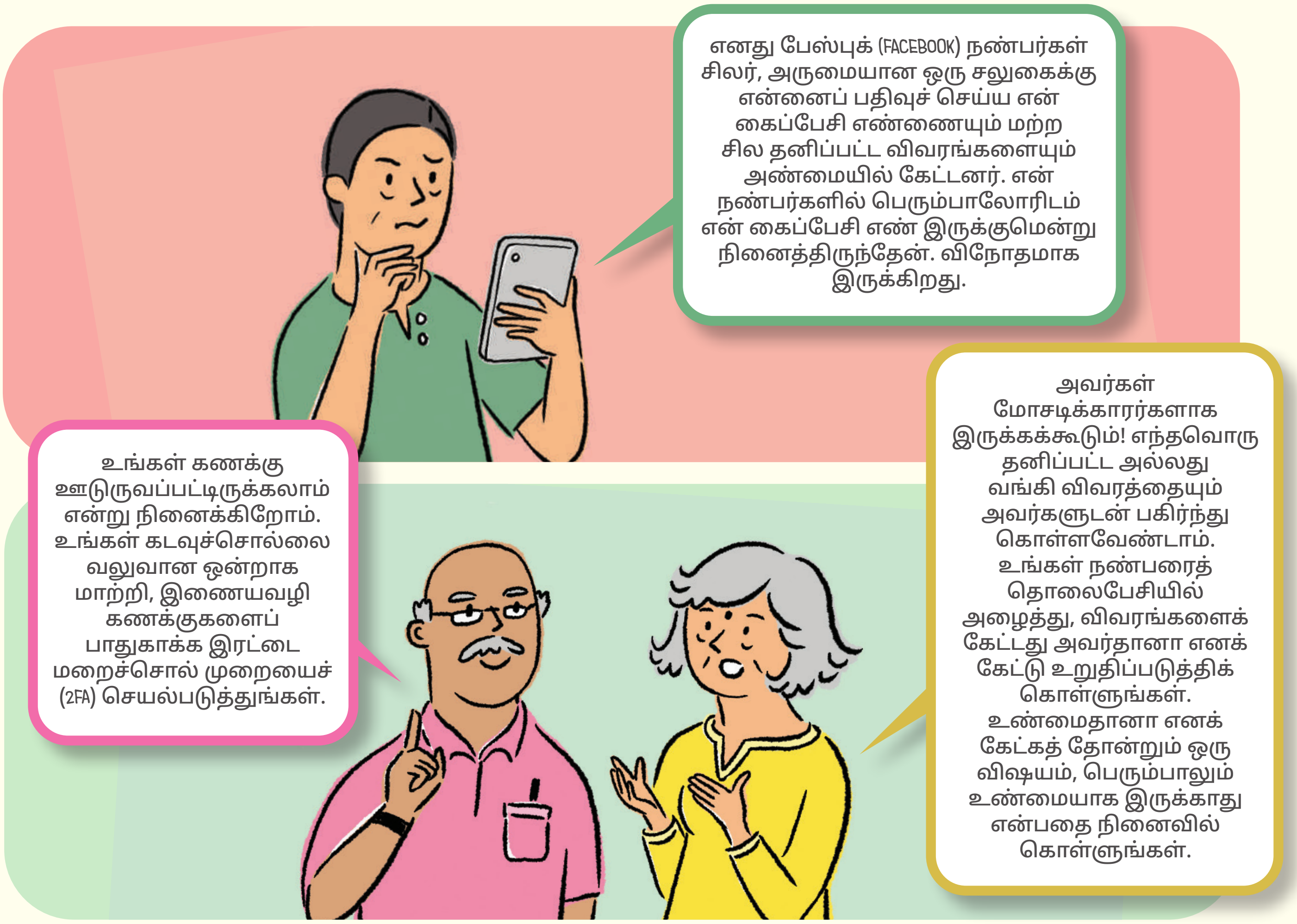
உங்களுக்கு அல்லது உங்களுக்குத் தெரிந்த யாருக்காவது தகவல் திருடும் மோசடித் தகவல் கிடைத்தால்...

- பதற்றம் அடையாதீர்கள். உங்கள் குடும்பத்தினரை அல்லது நண்பர்களை அழையுங்கள், அல்லது மோசடித் தடுப்பு உதவித் தொலைபேசி சேவையை 1800-722-6688 என்ற எண்ணில் அழைத்து ஆலோசனை கேளுங்கள்.
- நீங்கள் வெளிநாட்டிலிருந்து அழைப்புகளை எதிர்பார்க்காவிட்டால், “+” குறியைக் காட்டும் உள்வரும் அழைப்புகளுக்குப் பதில் அளிக்காதீர்கள்.
- உங்களுக்கு “ஆலோசனை” அளிக்கப்படும் எந்தவொரு மென்பொருளையும் நிறுவாதீர்கள்.
- உங்களது கடவுச்சொல், OTP தனிப்பட்ட மற்றும் வங்கித் தகவல் எதனையும் பகிராதீர்கள்.
- யாருக்கும் பணம் அனுப்பாதீர்கள்.
- தகவலில் உள்ள எந்தோர் இணைப்பின்மீதும் “கிளிக்” செய்யாதீர்கள். அதனை அழித்துவிடுங்கள்.
- கூடுதல் பாதுகாப்புக்காக, வாட்ஸ்ஆப் செயலியில் இரட்டை மறைச்சொல் முறையைச் செயல்படுத்துங்கள்.
- சந்தேகத்திற்குரிய அழைப்புகளை அல்லது தகவல்களைச் சரிபார்க்க, அரசாங்கத்தின் / தொழில்நிறுவனத்தின் அதிகாரபூர்வ தொலைபேசி சேவையை அழையுங்கள் அல்லது அதிகாரபூர்வ செயலிக்கு / இணையப்பக்கத்திற்கு நேரடியாகச் சென்று பாருங்கள். அழைப்பில் அல்லது தகவலில் வழங்கப்படும் தொடர்பு விவரங்களைப் பயன்படுத்தி அமைப்புடன் தொடர்பு கொள்ளாதீர்கள்.
- அரசாங்க அதிகாரிகள் ஒருபோதும் உடனடியாக இணையம்வழி கட்டணம் செலுத்தச் சொல்லவோ, உள்நாட்டு அல்லது வெளிநாட்டு வங்கிக் கணக்குக்குப் பணம் அனுப்பச் சொல்லவோ, தொலைபேசி அழைப்பை நீங்கள் துண்டிக்க விடாமல் தடுக்கவோ மாட்டார்கள் என்பதைக் கவனத்தில் கொள்ளுங்கள்.
- இணைப்பில் அல்லது மின்னஞ்சல் முகவரியில் “**.gov.sg**” இல்லாவிட்டால், நம்பகமான அரசாங்க இணையப்பக்கங்களின் பட்டியலை **www.gov.sg/trusted-sites** இணையப்பக்கத்தில் பாருங்கள்.



If you inadvertently provided your personal and/or banking details, here's what you should do straight away:

- CHANGE THE PASSWORD for your account (Singpass or bank) immediately, including all other accounts using this password.
- ALERT YOUR BANK if you have revealed credit card details.
- MONITOR YOUR ACCOUNT for unauthorised withdrawals or purchases.
- MAKE A POLICE REPORT if any funds are missing.
- USE AN ANTI-VIRUS SOFTWARE to scan your system for any malware. Malware infects your devices and causes damage, including stealing, corrupting and even deleting your data.
- GO TO CSA'S SingCERT WEBPAGE **www.csa.gov.sg/singcert/reporting** if you wish to submit an incident report.



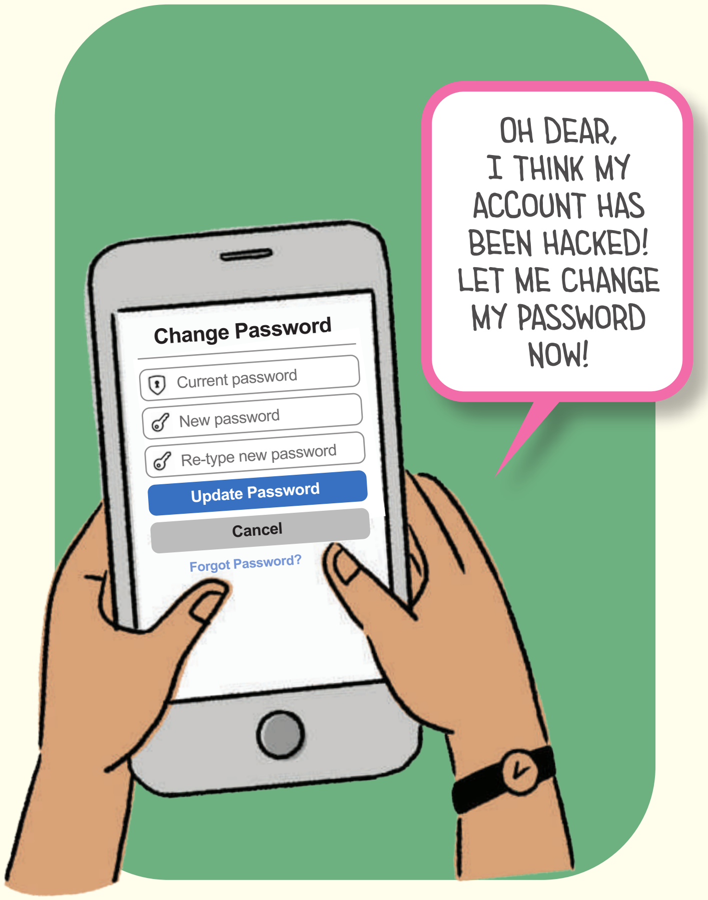
நீங்கள் சரியாகக் கவனிக்காமல் உங்களது தனிப்பட்ட மற்றும்/அல்லது வங்கி விவரங்களைத் தெரிவித்திருந்தால், உடனடியாகப் பின்வருமாறு செய்யுங்கள்:

- உங்கள் கணக்கின் (சிங்பாஸ் அல்லது வங்கி) கடவுச்சொல்லையும், அதனைப் பயன்படுத்தும் மற்ற எல்லா கணக்குகளின் கடவுச்சொற்களையும் உடனடியாக மாற்றுங்கள்.
- நீங்கள் கடன் அட்டை விவரங்களை வெளியிட்டிருந்தால், உங்கள் வங்கியிடம் தெரியப்படுத்துங்கள்.
- உங்கள் கணக்கிலிருந்து அனுமதியின்றி பணம் எடுக்கப்படுகிறதா அல்லது பொருட்கள் வாங்கப்படுகிறதா என்பதைக் கண்காணித்திடுங்கள்.
- பணம் ஏதாவது காணாமல் போனால் காவல்துறையில் புகார் செய்யுங்கள்.
- நச்சுநிரல் எதிர்ப்பு மென்பொருளைப் பயன்படுத்தி உங்களது சாதனங்களைச் சோதனையிடுங்கள். நச்சுநிரல் சாதனங்களைச் சேதப்படுத்தும். உங்களது தகவல்களைத் திருடி, சாதனத்தின் செயல்பாட்டைப் பாதிப்பதோடு, தகவல்களையும் அது அழித்துவிடக்கூடும்.
- நீங்கள் சம்பவத்தைப் புகார் செய்ய விரும்பினால், இணையப் பாதுகாப்பு அமைப்பின் **www.csa.gov.sg/singcert/reporting** இணையப்பக்கத்திற்குச் செல்லுங்கள்.

KEEP TABS ON YOUR ONLINE ACCOUNT

How can you protect your online accounts?

- CREATE PASSWORDS that are unique to you. Have at least 12 characters. Use words that relate to a memory unique to you to form a phrase, e.g. IhadKAYAtoastAT8AM!
- USE uppercase and lowercase letters, numbers and symbols.
- ENABLE TWO-FACTOR AUTHENTICATION (2FA) where available. Besides internet banking, 2FA is available for social media, email, shopping, and government accounts.



What should you do if you think you have been hacked?

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 **https://eservices.police.gov.sg** if monetary loss is involved.
- Should your account be compromised, your impersonator could reach out to your contacts. WARN YOUR FAMILY AND FRIENDS to ignore any request and not to share their personal details.

ACTIVITY

Want to find out if a password is strong? Use the Password Checker to find out now!

உங்கள் இணையக் கணக்கைக் கண்காணித்திடுங்கள்

உங்களது இணையக் கணக்குகளை எப்படி பாதுகாப்பது?

- உங்களுக்கே உரிய தனித்துவமான **கடவுச்சொற்களை உருவாக்குங்கள்.** அவற்றில் குறைந்தது 12 எழுத்துகளும் எண்களும் இருக்கவேண்டும். உங்கள் மனதில் பதிந்த ஒரு ஞாபகத்துடன் தொடர்புடைய சொற்களைப் பயன்படுத்தி ஒரு சொற்றொடரை உருவாக்குங்கள். எடுத்துக்காட்டாக, IhadKAYAtoastAT8AM!

- பேரெழுத்துகள் மற்றும் சிற்றெழுத்துகளின் கலவை, எண்கள், சின்னங்கள் ஆகியவற்றைப் **பயன்படுத்துங்கள்.**

- சாத்தியமானபோது **இரட்டை மறைச்சொல் முறையை (2FA) செயல்படுத்துங்கள்.** இணைய வங்கிச்சேவை தவிர, சமூக ஊடகம், மின்னஞ்சல், விற்பனைத் தளங்கள், அரசாங்கக் கணக்குகள் ஆகியவற்றுக்கும் இரட்டை மறைச்சொல் முறை கிடைக்கும்.

உங்கள் கணக்கு ஊடுருவப்பட்டிருப்பதாக நீங்கள் நினைத்தால் என்ன செய்யவேண்டும்?

- அந்தக் கணக்கை உங்களால் இன்னமும் பயன்படுத்த முடிந்தால், அந்தக் கணக்குடன் இணைக்கப்பட்ட **அனைத்து சாதனங்களிலும் கணக்கிலிருந்து வெளியேறிவிடுங்கள்.**

- **உங்களது கடவுச்சொல்லை உடனடியாக மாற்றிவிட்டு,** இரட்டை மறைச்சொல் முறையைச் செயல்படுத்துங்கள்.

- **சம்பந்தப்பட்ட தளத்துடன்,** எ.கா. வங்கி அல்லது சமூக ஊடகத் தளத்துடன், **தொடர்புகொண்டு,** ஊடுருவலைப் புகார் செய்து, உங்கள் கணக்கை மீட்பதற்கு உதவி கேளுங்கள்.

- உங்களது கடன்பற்று / ரொக்கக்கழிவு அட்டையைப் பயன்படுத்தி மோசடி செய்யப்பட்டிருந்தால், உடனடியாக வங்கியிடம் **தெரியப்படுத்தி,** அட்டையை ரத்து செய்யுங்கள்.

- பண இழப்பு ஏற்பட்டிருந்தால், அருகிலுள்ள அக்கம்பக்கப் போலிஸ் நிலையத்தில் அல்லது அக்கம்பக்கப் போலிஸ் சாவடியில் அல்லது **https://eservices.police.gov.sg** இணையப்பக்கத்தில் **போலிஸ் புகார் செய்யுங்கள்.**

- உங்கள் கணக்கு அத்துமீறப்பட்டால், உங்களைப் போல் ஆள்மாறாட்டம் செய்பவர் உங்களது தொடர்புகளுடன் தொடர்பு கொள்ளக்கூடும். எனவே, உங்களிடமிருந்து ஏதாவது கோரிக்கைகள் கிடைத்தால் புறக்கணிக்கும்படியும், தனிப்பட்ட விவரங்களைப் பகிர வேண்டாமென்றும் **உங்கள் குடும்பத்தாரையும் நண்பர்களையும் எச்சரித்திடுங்கள்.**

நடவடிக்கை

ஒரு கடவுச்சொல் வலுவானதா என்பதைத் தெரிந்து கொள்ள வேண்டுமா? இப்போதே கடவுச்சொல் சரிபார்ப்புக் கருவியைப் பயன்படுத்தி தெரிந்து கொள்ளுங்கள்!

MALWARE. WHAT EXACTLY IS IT?

Malware is a type of software that infects your devices and causes damage, including stealing your information, corrupting and even deleting your data.

How can you protect your devices from Malware?

- **DO DOWNLOAD AN ANTI-VIRUS APP** from official app stores to protect your device.
- **DO UPDATE YOUR SOFTWARE** regularly and promptly to keep your device safe. These updates will fix the weak points in your device.
- **DO ENABLE AUTOMATIC UPDATES** over Wi-Fi, or schedule updates to install overnight when your device is plugged in.

நச்சுநிரல். அது என்ன?

நச்சுநிரல் என்பது உங்களது சாதனங்களைச் சேதப்படுத்தி, உங்களது தகவல்களைத் திருடி, சாதனத்தின் செயல்பாட்டைப் பாதிப்பதோடு, தகவல்களையும் அழித்துவிடக்கூடிய ஒரு வகையான மென்பொருள்.

உங்கள் சாதனங்களை நச்சுநிரலிலிருந்து எப்படி பாதுகாப்பது?

- உங்கள் சாதனத்தைப் பாதுகாக்க, அதிகாரபூர்வ செயலிக் கடைகளிலிருந்து **நச்சுநிரல் எதிர்ப்புச் செயலியைப் பதிவிறக்கம் செய்யுங்கள்.**

- உங்கள் சாதனத்தின் **மென்பொருளை உடனுக்குடன் புதுப்பித்து**, சாதனத்தைப் பாதுகாப்பாய் வைத்திருங்கள். உங்கள் சாதனத்திலுள்ள பலவீனங்களை இந்தப் புதுப்பிப்புகள் சரிசெய்துவிடும்.

- அருகலை (Wi-Fi) வழியாகத் **தானாகப் புதுப்பிக்கும் இயக்கத்தைச் செயல்படுத்துங்கள்**, அல்லது இரவில் சாதனத்தை மின்விசையுடன் இணைத்திருக்கும்போது புதுப்பிப்பதற்கு ஏற்பாடு செய்யுங்கள்.

WITH OUR SMARTPHONES AND DEVICES, LIFE IS MUCH EASIER, BUT CAN BE MORE WORRYING.

DON'T WORRY. WE JUST HAVE TO STAY ALERT, AND BE MORE VIGILANT WITH OUR DEVICES AND ONLINE ACCOUNTS.

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

நம்முடைய திறன்பேசிகளும் சாதனங்களும் வாழ்க்கையை மிகவும் எளிதாக்கி இருந்தாலும், அதிக கவலையும் தருகின்றன.

கவலைப்படாதீர்கள். நாம் விழிப்புடன் இருந்தாலே போதும். சாதனங்களையும் இணையக் கணக்குகளையும் அதிக கவனமாகப் பயன்படுத்துங்கள்.

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

Better cyber safe than sorry

For more information, visit CSA's SG Cyber Safe Seniors webpage or the Scam Alert webpage of the National Crime Prevention Council.

மேல்விவரம் அறிய, CSA எஸ்ஜி இணையப் பாதுகாப்புமிக்க மூத்தோர்கள் இணையப்பக்கத்திற்கு அல்லது தேசிய குற்றத்தடுப்பு மன்றத்தின் மோசடி எச்சரிக்கை இணையப்பக்கத்திற்குச் செல்லுங்கள்.

www.csa.gov.sg www.scamalert.sg

Get more cyber tips at:
இன்னும் பல இணையக்குறிப்புகளுக்கு:

For the latest scam info, visit:
மோசடி பற்றிய அண்மைத் தகவலுக்கு, பாருங்கள்: