BETTER CYBER SAFE THAN SORRY

A GUIDE TO STAYING SAFE ONLINE

பின்னர் வருந்தாமல் இப்போதே இணையத்தில் பாதுகாப்பாக இருங்கள்

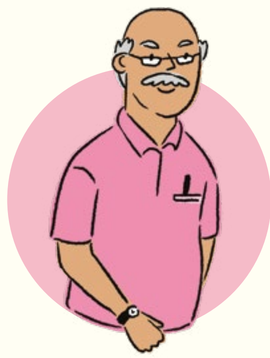
இணையத்தில் பாதுகாப்பாக இருக்க ஒரு வழிகாட்டி

CSA SINGAPORE

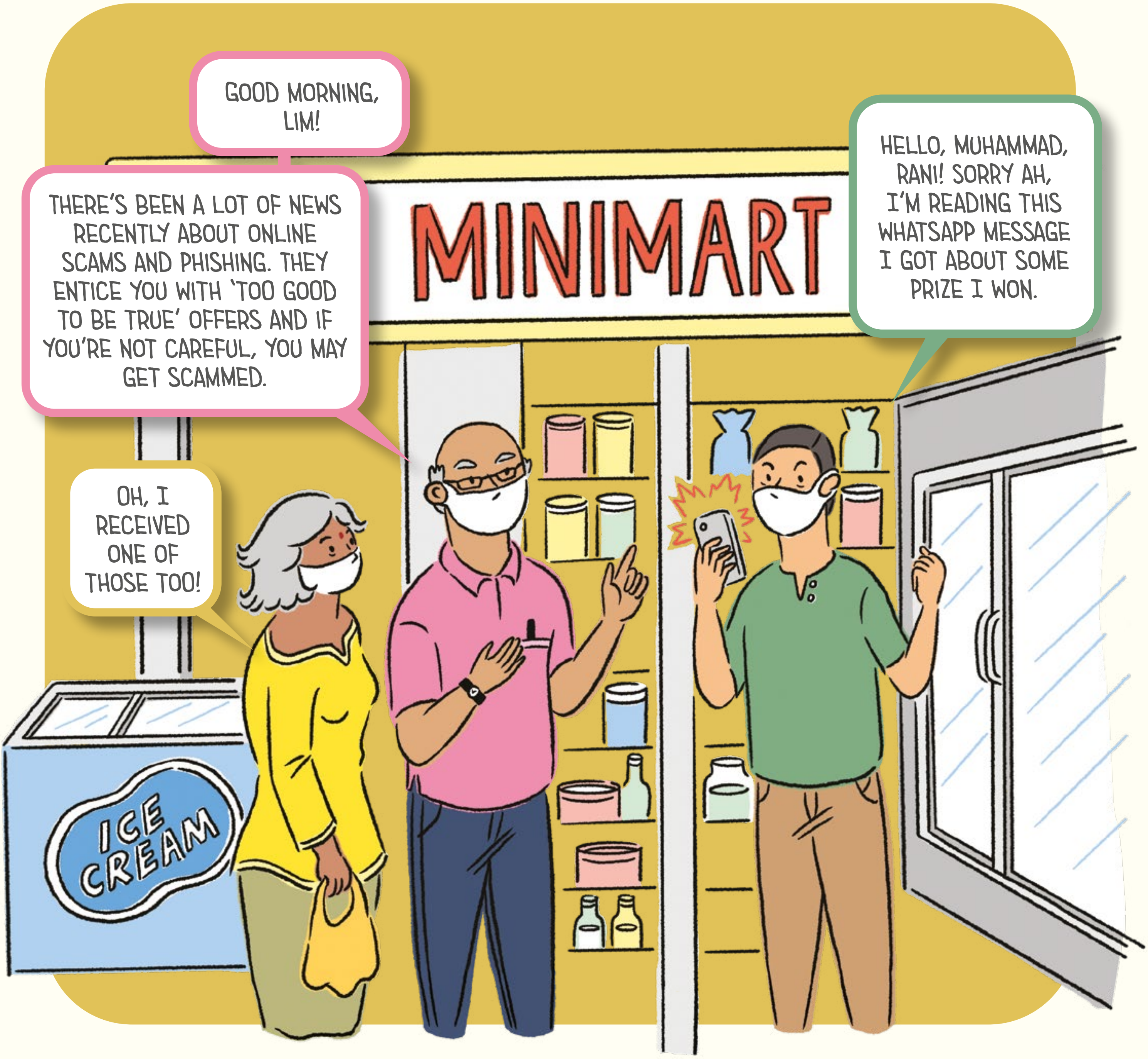
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

LIM
Taxi Driver

RANI
Administrative Assistant



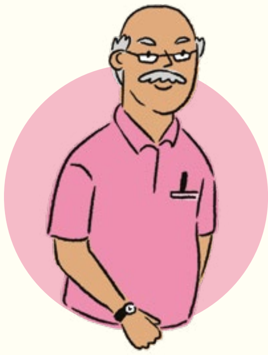
MUHAMMAD
Retired Teacher



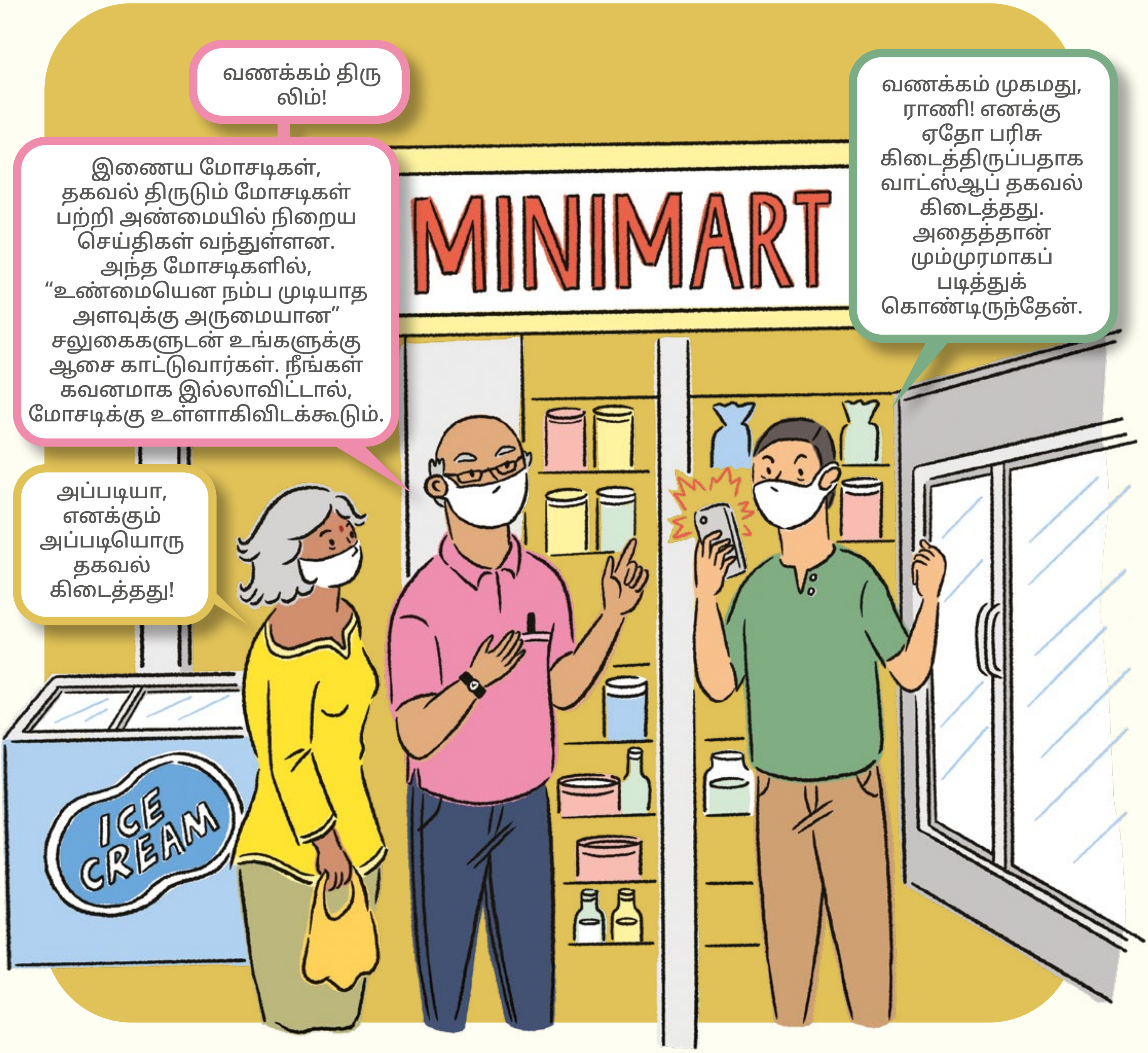
Does this sound familiar? The increased use of smartphones and other smart devices has made life more convenient but there are also cybercrimes which we need to be aware of. So what are the telltale signs and how can we protect ourselves against cyber threats? This handbook will arm you with the information you need to navigate this bold new world.

திரு லிம்
டாக்சி ஓட்டுநர்

ராணி
நிர்வாக உதவியாளர்



முகமது
ஓய்வுபெற்ற ஆசிரியர்



இதை எங்கோ கேட்டதுபோல இருக்கிறதா? திறன்பேசிகளும் மற்ற அறிவார்ந்த சாதனங்களும் அதிகமாகப் பயன்படுத்தப்படுவதால் வாழ்க்கை அதிக வசதியாகியுள்ளது. ஆனால், இணையக் குற்றச்செயல்களும் நடப்பதால், நாம் விழிப்பாக இருக்கவேண்டும். இத்தகைய இணைய மிரட்டல்களின் அறிகுறிகள் என்ன? இவற்றிலிருந்து நம்மை நாம் எப்படி பாதுகாத்துக் கொள்வது? துணிச்சலான புதிய உலகில் பாதுகாப்பாக வலம்வர உங்களுக்குத் தேவைப்படும் தகவல்களை இந்தக் கையேடு வழங்குகிறது.

WHAT ARE CYBER THREATS?

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 victims into giving out your personal and financial information such as passwords, One-Time Passwords (OTPs) or bank account numbers.

How to spot phishing attempts

[URGENT] CLAIM YOUR GIFT CARD OR ACCOUNT WILL BE DEACTIVATED

From: SGSHOPPING <SGSHOPPING@S1231.NET> 1
Date: 11 April 2018, 12.42 AM
To: John Tan
Subject: [URGENT] CLAIM YOUR GIFT CARD 2 OR ACCOUNT WILL BE DEACTIVATED 3

Attached: Gift-Card-Redemption.exe (150kb) 4

Dear John,

Congratulations! We are pleased to inform you that you have won a $100 gift card 5 for our monthly lucky draw!

www.252749.co/d43lFk 1

Simply log on to www.sgshopping.com or fill up the attached document with your 6 NRIC, address and bank account details to claim your gift card. Failure to claim your prize within 24 hours will result in the permanent deactivation 3 of your account.

1

Mismatched & Misleading Information

2

Unexpected Emails

3

Use of Urgent or Threatening Language

4

Suspicious Attachments

5

Promise of Attractive Rewards

6

Request for Confidential Information

இணைய மிரட்டல்கள் என்பது என்ன?

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.

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) 4

அன்பார்ந்த ஜான்,

வாழ்த்துக்கள்! எங்களது மாதாந்தர அதிர்ஷ்டக் குலுக்கலில் நீங்கள் $100 பெறுமானமுள்ள அன்பளிப்பு அட்டையை வென்றிருப்பதாகத் தெரிவிப்பதில் மகிழ்ச்சி அடைகிறோம்! 5

www.252749.co/d43IFk 1

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

1

பொருந்தாத மற்றும் தவறாக வழிநடத்தக்கூடிய தகவல்கள்

2

எதிர்பாராத மின்னஞ்சல்கள்

3

அவசரமான அல்லது அச்சுறுத்தும் வகையிலான சொற்களைப் பயன்படுத்துதல்

4

சந்தேகத்திற்குரிய இணைப்புகள்

5

கவர்ச்சிகரமான வெகுமதிகளைத் தருவதாக உத்தரவாதம் அளித்தல்

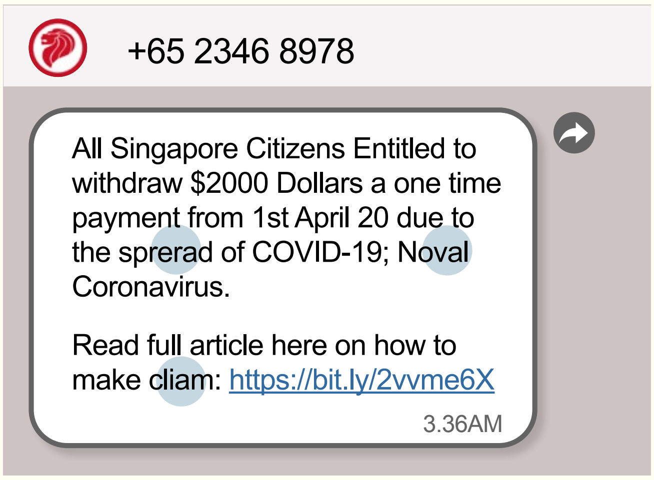
6

இரகசியத்தன்மை வாய்ந்த தகவல்களைக் கோருதல்

HOW TO SPOT PHISHING/ONLINE SCAMS

IMPERSONATION SCAMS

These criminals may call, SMS or WhatsApp you, pretending to be reputable organisations such as a government agency or a bank. They may ask you to follow urgent instructions in order to address some bank account or fake technical issues or provide personal particulars for a non-existent offer.



- **DO 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

- **DO BE SUSPICIOUS** if the message is full of spelling errors and other mistakes

- **DO 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

TECH SUPPORT SCAM

These scammers may claim to be officers from CSA or from a telco investigating suspicious activity on your network.

- **DO NOT INSTALL** any software applications they 'advise' you to

- **DO NOT DISCLOSE** any personal or financial details

BANKING-RELATED PHISHING SCAM

- **DO NOT SHARE YOUR PASSWORDS** or one-time password (OTP) or personal and banking information with anyone

- **DO NOT SEND MONEY** to someone you just met online

- **BE WARY** of incoming calls showing a '+' sign if you are not expecting calls. Local calls will not display the '+' sign

தகவல் திருடும் / இணைய மோசடிகளை எப்படி கண்டுகொள்வது

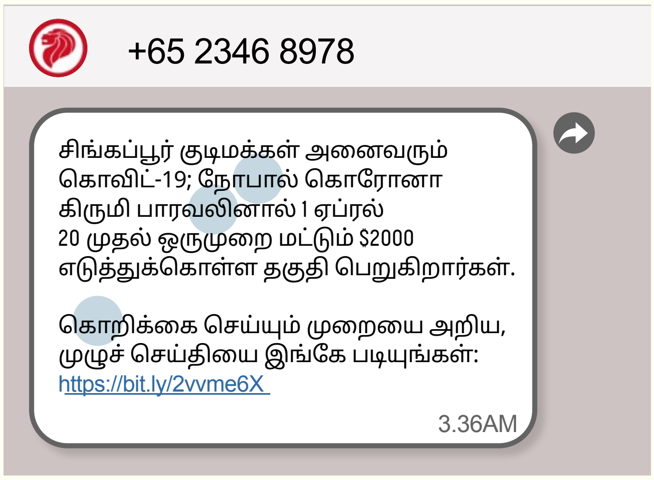
ஆள்மாறாட்ட மோசடிகள்

இந்த மோசடிகளைச் செய்வோர், அரசாங்கம் அல்லது வங்கி போன்ற மதிக்கப்படும் அமைப்புகளைப் போல பாசாங்கு செய்து, தொலைபேசியில் உங்களை அழைக்கக்கூடும், அல்லது குறுந்தகவல் அல்லது வாட்ஸ்ஆப் மூலம் தகவல் அனுப்பக்கூடும். வங்கிக் கணக்கில் ஏற்பட்டுள்ள பிரச்சனைக்கு அல்லது பொய்யான தொழில்நுட்பப் பிரச்சனைக்குத் தீர்வுகாண அவசரமாகச் சில காரியங்களைச் செய்யும்படி, அல்லது இல்லாததொரு சலுகையைப் பெற சுய விவரங்களைத் தெரிவிக்கும்படி அவர்கள் உங்களிடம் கேட்கக்கூடும்.

- அரசாங்க அதிகாரிகள் இணையம்வழி பணம் அனுப்புமாறு தொலைபேசிவழி ஒருபோதும் கேட்க மாட்டார்கள் என்பதைக் **கவனத்தில் கொள்ளுங்கள்**

- தகவலில் ஏகப்பட்ட எழுத்துப் பிழைகளும் மற்ற தவறுகளும் இருந்தால் **சந்தேகப்படுங்கள்**

- இணைப்பில் அல்லது மின்னஞ்சல் முகவரியில் “**gov.sg**” இல்லாவிட்டால், **www.gov.sg/trusted-sites** இணையப்பக்கத்திற்குச் சென்று, நம்பகமான அரசாங்கம் சார்ந்த இணையத்தளங்களின் பட்டியலைப் **பாருங்கள்**



தொழில்நுட்ப ஆதரவு மோசடி

இந்த மோசடிகளைச் செய்வோர், CSA (சிங்கப்பூர் இணையப் பாதுகாப்பு அமைப்பு) அல்லது தொலைத்தொடர்பு நிறுவன அதிகாரிகளைப் போல பாசாங்கு செய்து, உங்கள் கட்டமைப்பில் சந்தேகத்திற்குரிய நடவடிக்கைகளைப் புலனாய்வு செய்வதாகச் சொல்வார்கள்.

- அவர்கள் சொல்லும் “ஆலோசனைப்படி” எந்தவொரு மென்பொருள் செயலியையும் **நிறுவாதீர்கள்**

- தனிப்பட்ட அல்லது நிதித் தகவல்கள் எதனையும் **வெளியிடாதீர்கள்**

- அண்மையில் இணையத்தில் சந்தித்த யாருக்கும் **பணம் அனுப்பாதீர்கள்**

- நீங்கள் தொலைபேசி அழைப்புகளை எதிர்பார்க்காவிட்டால், “+” சின்னத்தைக் காட்டும் உள்வரும் அழைப்புகளிடம் **எச்சரிக்கையாக இருங்கள்**. உள்நாட்டு அழைப்புகளில் “+” சின்னம் இருக்காது

வங்கி தொடர்பான தகவல் திருட்டு

- உங்களது கடவுச்சொல் அல்லது ஒருமுறை பயன்படுத்தும் கடவுச்சொல் (OTP) அல்லது நிதித் தகவல்களை **யாருடனும் பகிர்ந்து கொள்ளாதீர்கள்**

If you or someone you know has received a phishing message, call or email...

- IGNORE and delete it
- DO NOT CLICK on any attachment or link in the message

Should you receive an unsolicited advertisement or message to follow some instructions urgently, do not panic. Call your family members or friends for advice. Visit **www.scamalert.sg** for more info or call the Anti-Scam helpline at **1800-722-6688** for scam-related advice. If you inadvertently clicked on it and provided your personal and/or banking details, here's what you should do straight away:

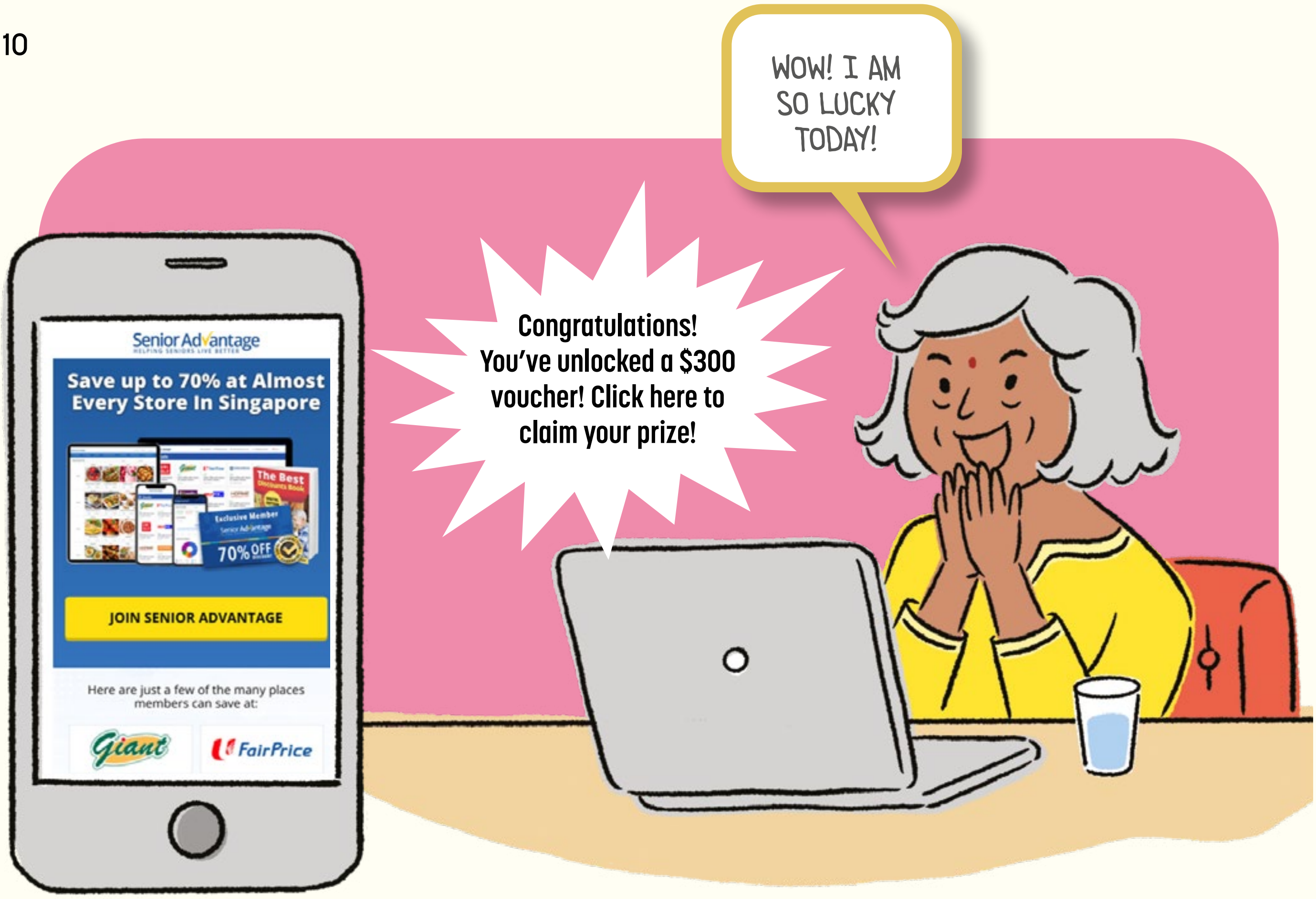
- CHANGE THE PASSWORD FOR YOUR BANKING ACCOUNT IMMEDIATELY, including all other accounts using this password
- ALERT YOUR BANK if you revealed credit card details
- MONITOR YOUR ACCOUNT for unauthorised withdrawals or purchases
- MAKE A POLICE REPORT if any funds are missing
- USE AN ANTI-VIRUS SOFTWARE to scan your system
- GO TO CSA'S SingCERT WEBPAGE **www.csa.gov.sg/singcert/reporting** if you wish to submit an incident report

உங்களுக்கு அல்லது உங்களுக்குத் தெரிந்த யாருக்காவது தகவல் திருடும் மோசடித் தகவல், அழைப்பு அல்லது மின்னஞ்சல் கிடைத்தால்,

- அதைப் **புறக்கணித்துவிட்டு**, அழித்துவிடுங்கள்
- அந்தத் தகவலில் உள்ள எந்தவோர் இணைப்பையும் **கிளிக் செய்யாதீர்கள்**

கேட்கப்படாத விளம்பரம் அல்லது சில அறிவுறுத்தல்களைச் செய்யச் சொல்லும் தகவல் உங்களுக்குக் கிடைத்தால் பதறாதீர்கள். உங்கள் குடும்பத்தினரை அல்லது நண்பர்களை அழைத்து ஆலோசனை கேளுங்கள். மேல்விவரம் அறிய **www.scamalert.sg** இணையத்தளத்தை நாடுங்கள் அல்லது மோசடி தொடர்பான ஆலோசனைக்கு **1800-722-6688** என்ற மோசடித்தடுப்பு தொலைபேசி சேவையை அழையுங்கள். நீங்கள் தெரியாமல் கிளிக் செய்து, உங்களது தனிப்பட்ட மற்றும்/அல்லது வங்கி விவரங்களைத் தெரிவித்திருந்தால், உடனடியாகப் பின்வருமாறு செய்யுங்கள்:

- உங்களது கடவுச்சொல்லையும், அதனைப் பயன்படுத்தும் மற்ற எல்லா கணக்குகளையும் **உடனடியாக மாற்றுங்கள்**
- நீங்கள் கடன் அட்டை விவரங்களை வெளியிட்டிருந்தால், உங்கள் **வங்கியிடம் தெரியப்படுத்துங்கள்**
- உங்கள் கணக்கில் அனுமதியின்றி பணம் எடுக்கப்படுகிறதா அல்லது பொருட்கள் வாங்கப்படுகிறதா என்பதைக் **கண்காணித்திடுங்கள்**
- பணம் ஏதாவது காணாமல் போனால் **காவல்துறையில் புகார் செய்யுங்கள்**
- **நச்சுநிரல் எதிர்ப்பு மென்பொருளைப் பயன்படுத்தி** உங்கள் கணினியைச் சோதனையிடுங்கள்
- நீங்கள் சம்பவத்தைப் புகார் செய்ய விரும்பினால், **இணையப் பாதுகாப்பு அமைப்பின்** **www.csa.gov.sg/singcert/reporting** **SingCERT இணையப்பக்கத்திற்குச்** செல்லுங்கள்



ONLINE SCAMS

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?

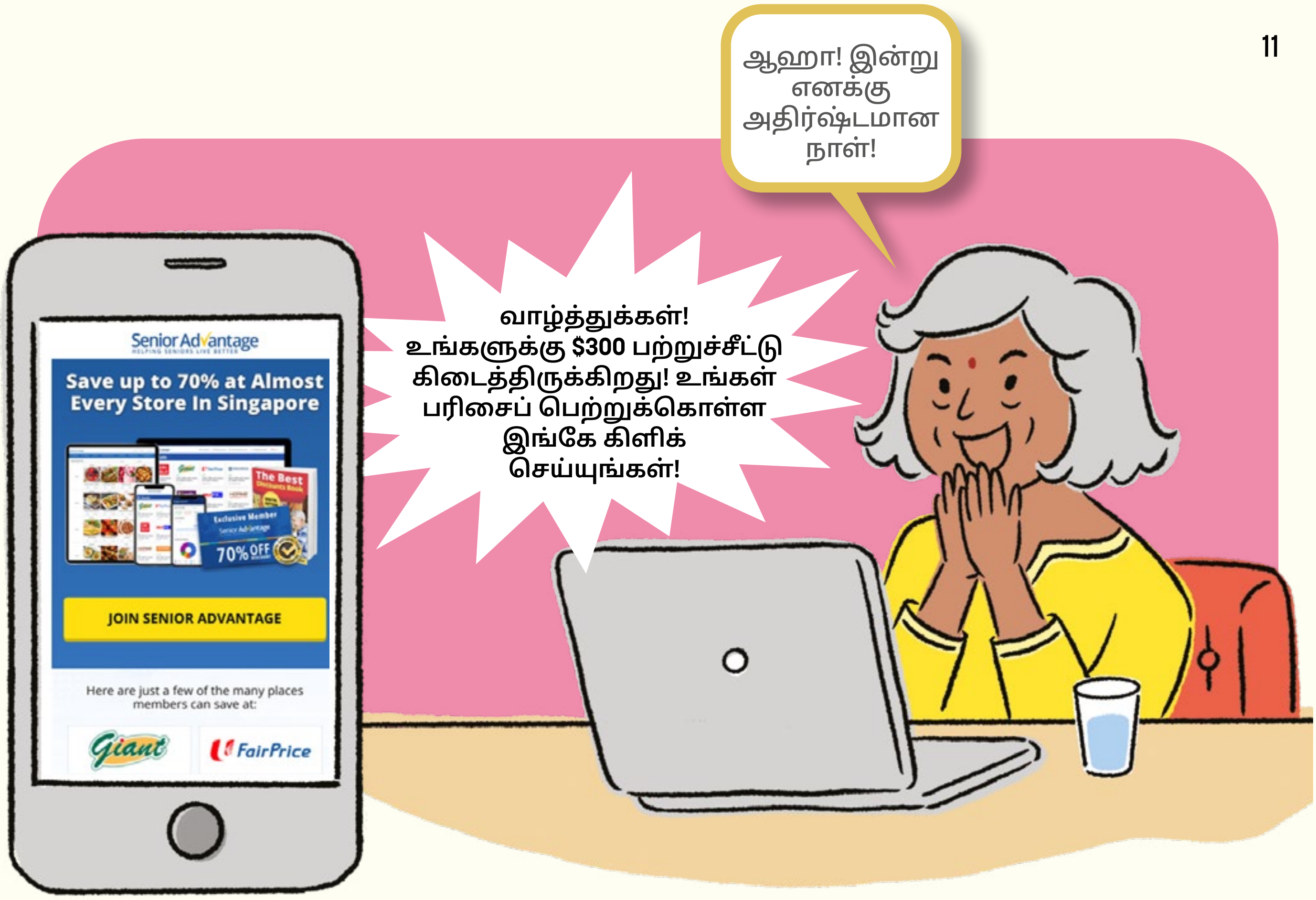
- DO PURCHASE only from reputable sites
- DO PAY through the shopping platform. This way, the seller receives payment only after you receive your goods
- DO BE ON YOUR GUARD always, and rethink the purchase if the deal is too good to be true

SOCIAL MEDIA IMPERSONATION SCAM

Scammers may also 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'.

What can you do?

- DO NOT SHARE personal or banking information or OTPs with anyone, including family or close friends
- BEWARE of unusual requests or offers from anyone, including family or close friends



இணையம்வழி மோசடிகள்

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

சமூக ஊடக ஆள்மாறாட்ட மோசடி

மோசடிக்காரர்கள் உங்களது நண்பர்களை, குடும்பத்தாரை அல்லது சக ஊழியர்களைப் போல பாசாங்கு செய்து, சமூக ஊடகத்தில் உங்களுடன் தொடர்புகொண்டு, உங்களது தனிப்பட்ட விவரங்களை அல்லது "தவறுதலாக" உங்களுக்கு அனுப்பிய ஒருமுறை பயன்படுத்தும் கடவுச்சொல்லைக் கேட்பார்கள்.

நாம் என்ன செய்யமுடியும்?

- உங்களது தனிப்பட்ட அல்லது வங்கி விவரங்களையோ ஒருமுறை பயன்படுத்தும் கடவுச்சொற்களையோ, குடும்பத்தினர் அல்லது நெருங்கிய நண்பர்கள் உட்பட, யாருடனும் பகிர்ந்து கொள்ளாதீர்கள்
- வழக்கத்திற்கு மாறான கோரிக்கைகள் அல்லது சலுகைகள், குடும்பத்தினர் அல்லது நெருங்கிய நண்பர்கள் உட்பட, யாரிடமிருந்து வந்தாலும் கவனமாக இருங்கள்

KEEP TABS ON YOUR ONLINE ACCOUNT

How can you protect your online accounts?

- **DO CREATE PASSWORDS** that are unique to you. Have at least 12 characters. Use words that relate to a memory to you to form a phrase. E.g. IhadKAYAtoastAT8AM!

- **DO USE** uppercase and lowercase letters, numbers and symbols

- **DO 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, **DO LOG OUT OF THIS ACCOUNT FROM ALL DEVICES** connected to this account

- **CHANGE YOUR PASSWORD IMMEDIATELY** and enable 2FA if available

- If you do not have access to your account, **DO 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. If monetary loss is involved, **MAKE A POLICE REPORT** at the nearest Neighbourhood Police Centre or Neighbourhood Police Post or online at **https://eservices.police.gov.sg**

- Should your account be compromised, your impersonator could reach out to your contacts. **DO 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!

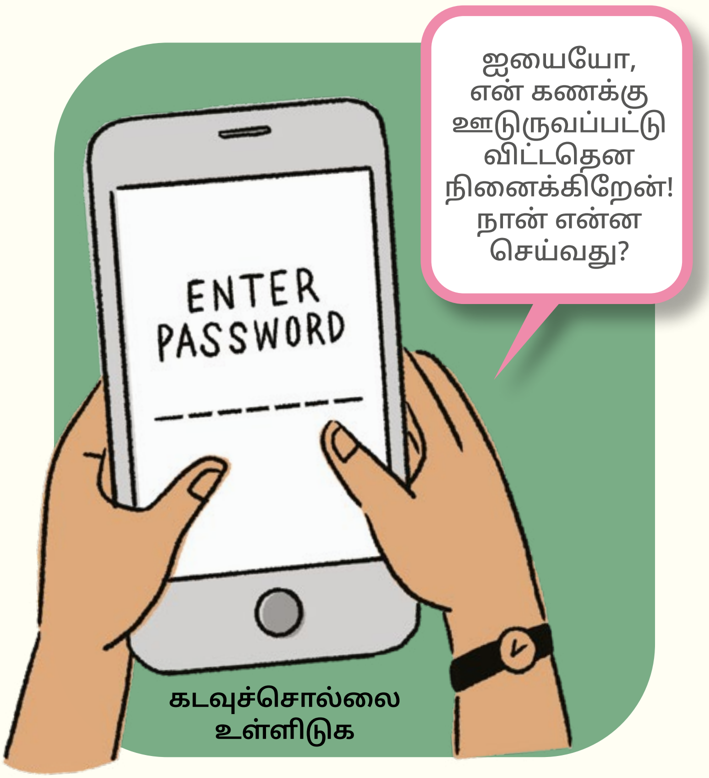
உங்கள் இணையக் கணக்கைக் கண்காணித்திடுங்கள்

உங்களது இணையக் கணக்குகளை எப்படி பாதுகாப்பது?

- உங்களுக்கே உரிய தனித்துவமான **கடவுச்சொற்களை உருவாக்குங்கள்.** அவற்றில் குறைந்தது 12 எழுத்துகளும் எண்களும் இருக்கவேண்டும். மாறாக, உங்களுடன் தொடர்புடைய ஐந்து வெவ்வேறு சொற்களை ஒன்றுசேர்த்து கடவுச்சொல்லை 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 சாதனங்களிலிருந்தும் வெளியேறிவிடுங்கள்**

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

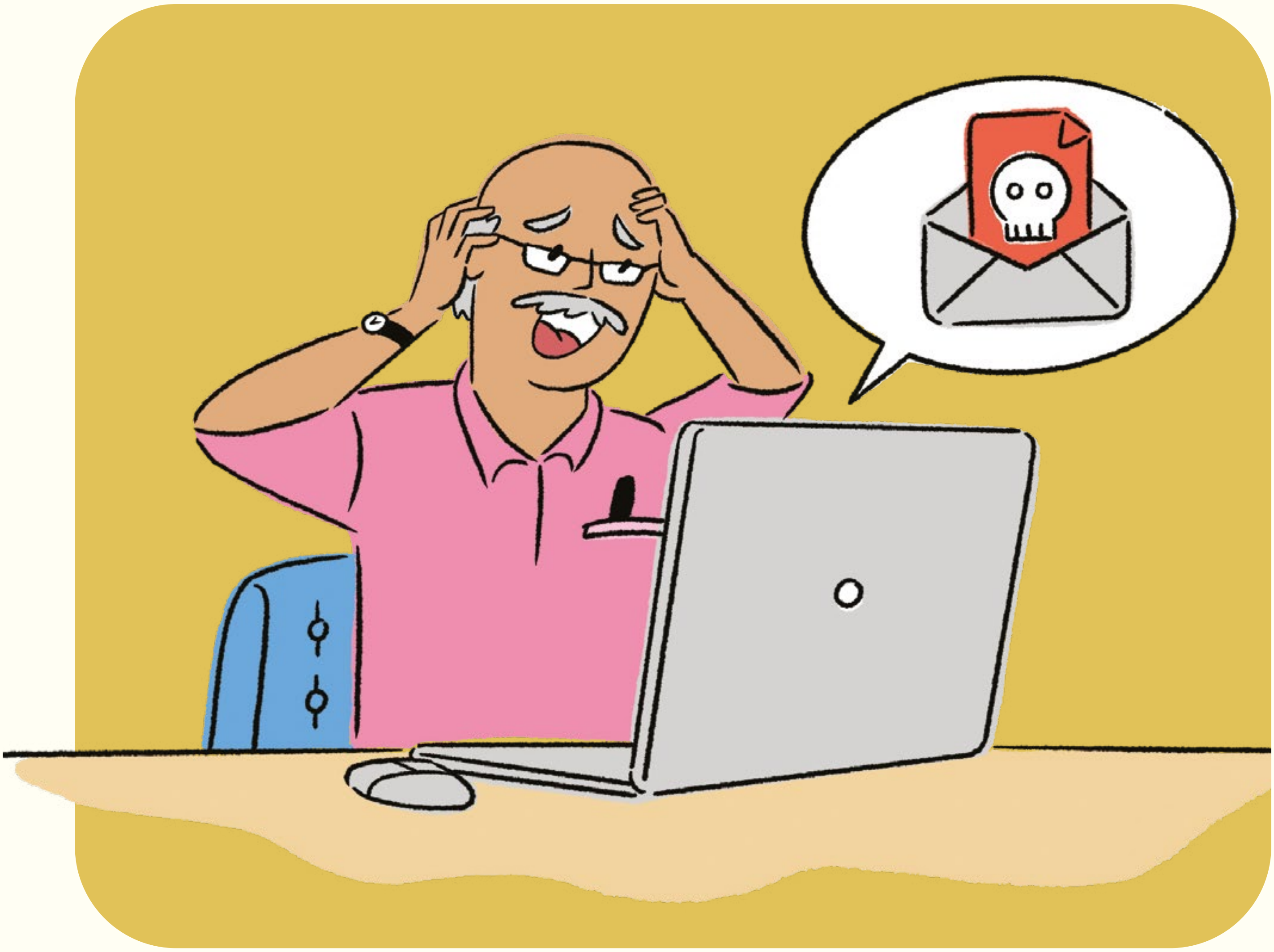
- உங்கள் கணக்கைப் பயன்படுத்த முடியவில்லையா? **சம்பந்தப்பட்ட தளத்துடன், எ.கா. வங்கி அல்லது சமூக ஊடகத் தளத்துடன், தொடர்புகொண்டு,** ஊடுருவலைப் புகார் செய்து, உங்கள் கணக்கை மீட்பதற்கு உதவி கேளுங்கள்

- 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** இணையத்தளத்தில் **போலிஸ் புகார் செய்யுங்கள்**

- உங்கள் கணக்கு அத்துமீறப்படும்போது, உங்களைப் போல ஆள்மாறாட்டம் செய்பவர் உங்களது தொடர்புகளுடன் தொடர்பு கொள்ளக்கூடும். எனவே, 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!

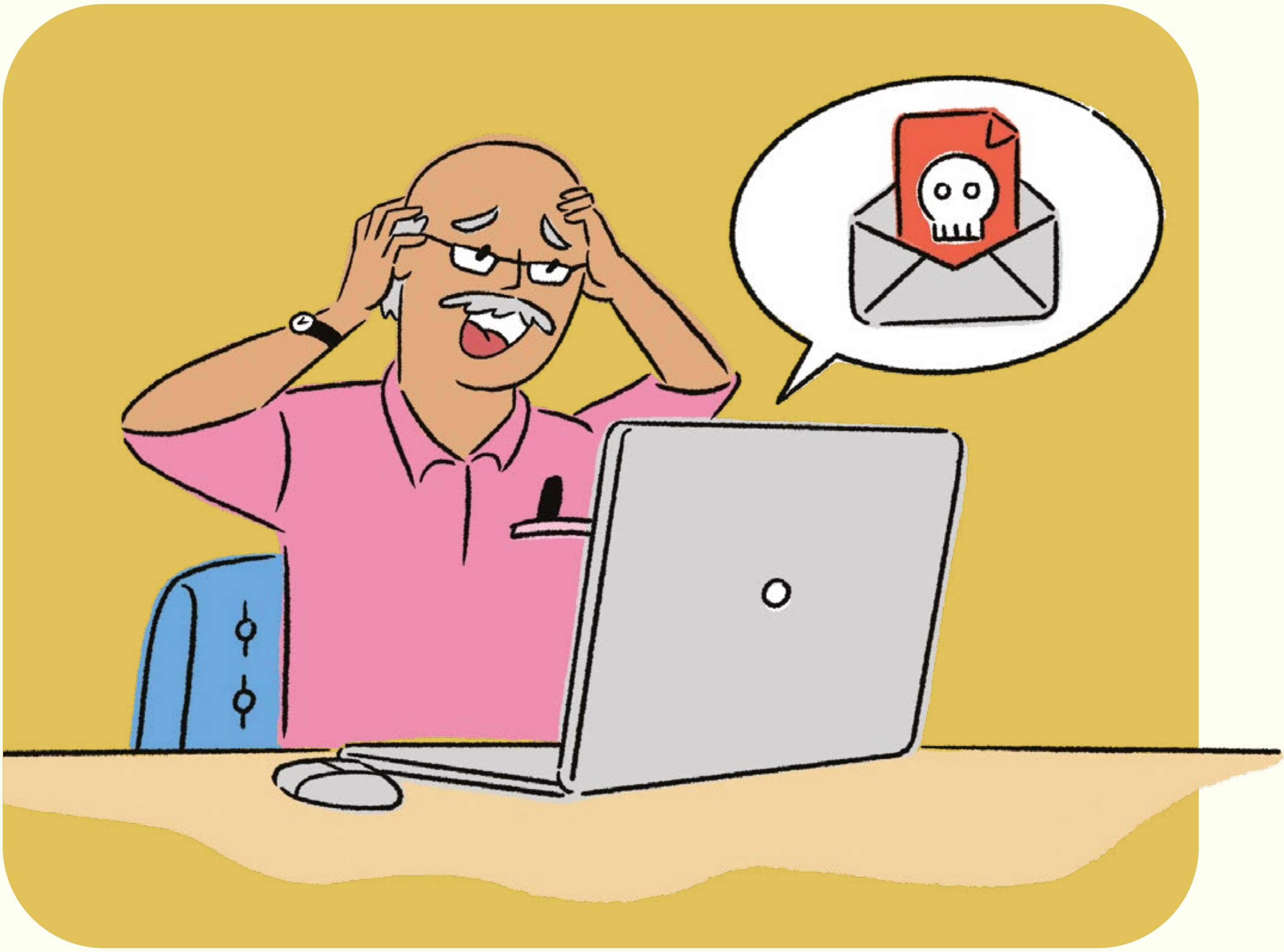


MALWARE. WHAT EXACTLY IS IT?

Malware is a type of software that infects your computer and mobile devices.
They can do much damage, including stealing, 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 (Malware) என்பது நமது கணினிகளையும் கையடக்கச் சாதனங்களையும் பாதிக்கும் தீய மென்பொருளாகும். நச்சுநிரலால் நிறைய சேதம் உண்டாக்க முடியும். நமது தரவுகளைக் களவாடுவதற்காக அல்லது அழிப்பதற்காகத் தரவுகளை அது சிதைக்கக்கூடும்.

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 ALSO SCARIER.

DON'T BE SCARED. 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 எளிதாக்கிவிட்டன, ஆனால் பயத்தையும் தருகின்றன.

பயப்படாதீர்கள். 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, sign up for the Ask the Cyber Experts Series Webinars or visit CSA's SG Cyber Safe Seniors webpage or the Scam Alert webpage of the National Crime Prevention Council

மேல்விவரம் அறிய, இணைய நிபுணர் கூட்டரங்கு தொடருக்குப் பதிவு செய்யுங்கள் அல்லது 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: