BETTER CYBER SAFE THAN SORRY

A GUIDE TO STAYING SAFE ONLINE

做好防范，安心上网

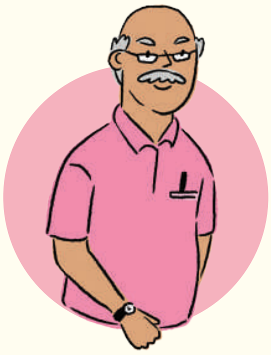
网络安全须知

CSA SINGAPORE

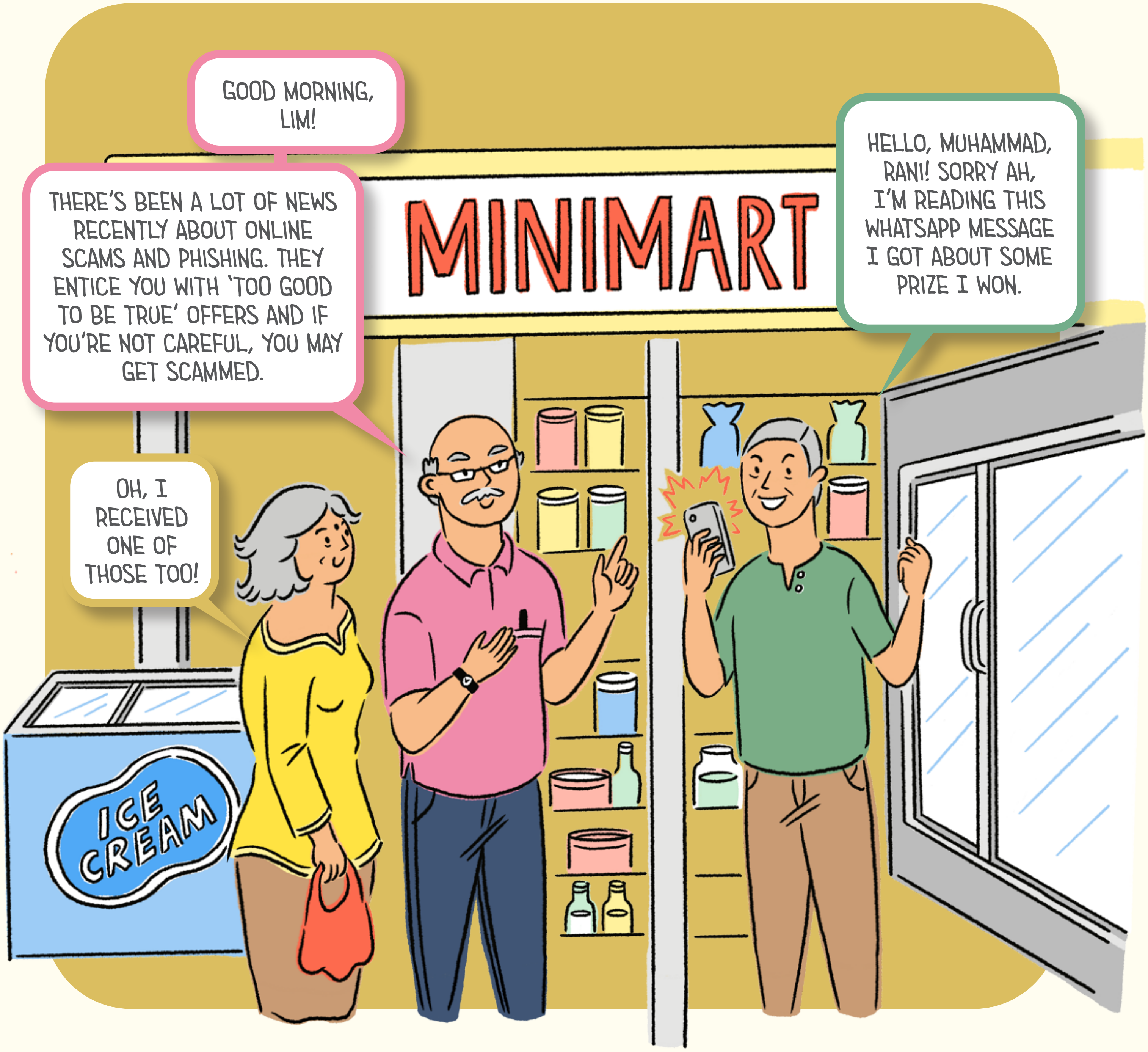
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

LIM
Taxi Driver

RANI
Administrative Assistant



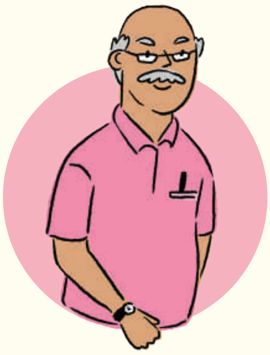
MUHAMMAD
Retired Teacher


GOOD MORNING, LIM!
THERE'S BEEN A LOT OF NEWS RECENTLY ABOUT ONLINE SCAMS AND PHISHING. THEY ENTICE YOU WITH 'TOO GOOD TO BE TRUE' OFFERS AND IF YOU'RE NOT CAREFUL, YOU MAY GET SCAMMED.
HELLO, MUHAMMAD, RANI! SORRY AH, I'M READING THIS WHATSAPP MESSAGE I GOT ABOUT SOME PRIZE I WON.
OH, I RECEIVED ONE OF THOSE TOO!
MINIMART
ICE CREAM

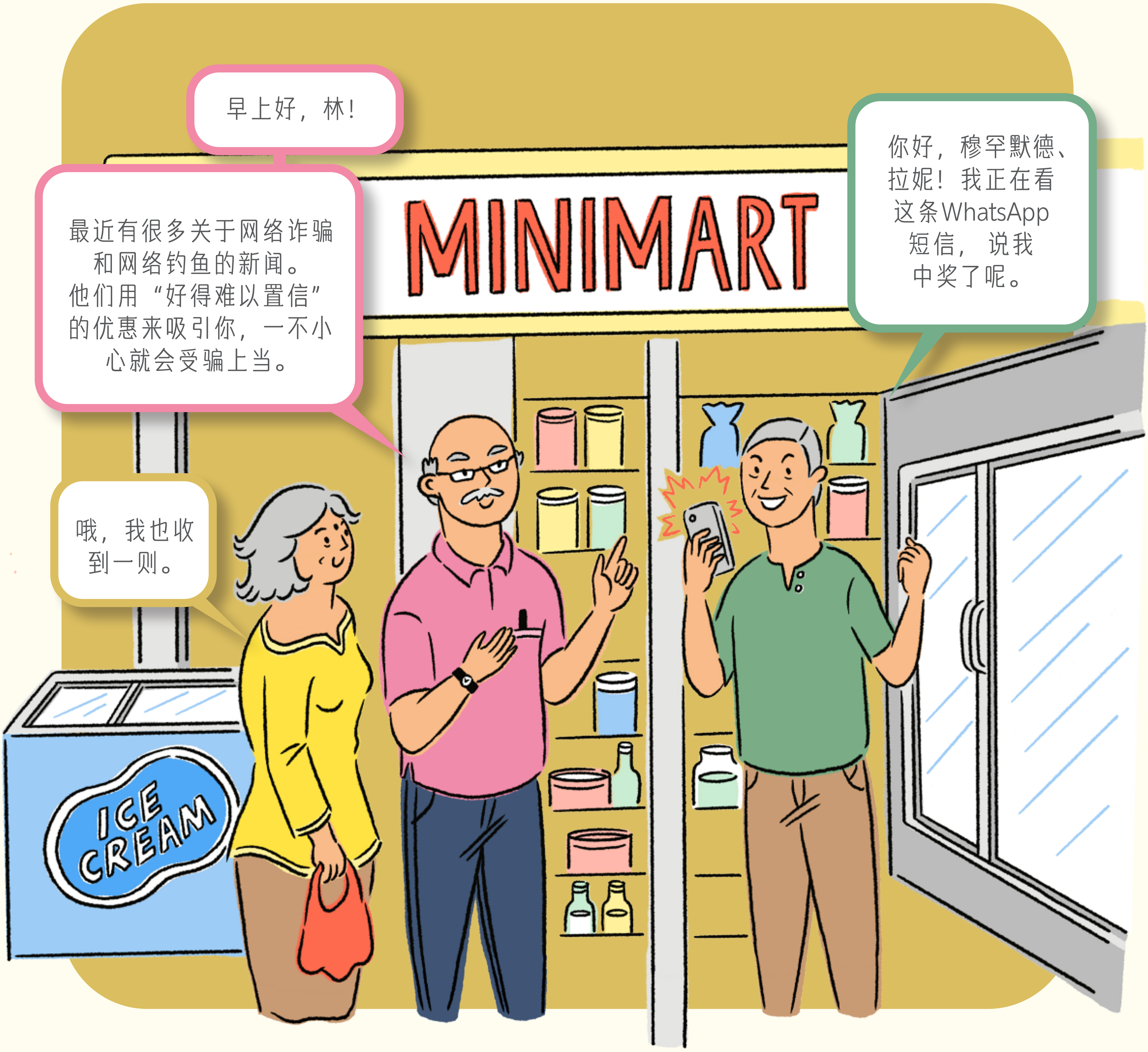
The increased use of smartphones and other smart devices has made life more convenient but at the same time, there are also cybercrimes which we need to be aware of. This handbook will arm you with the information you need to protect yourselves from cyber threats.

林
德士司机

拉妮
行政助理



穆罕默德
退休教师


早上好，林！
你好，穆罕默德、拉妮！我正在看这条WhatsApp短信，说我中奖了呢。
哦，我也收到一则。
最近有很多关于网络诈骗和网络钓鱼的新闻。他们用“好得难以置信”的优惠来吸引你，一不小心就会受骗上当。
MINIMART
ICE CREAM

智能手机和其他智能设备普及，使生活更加便利。但与此同时，我们也更应该小心防范网络罪案。这本手册将为您们提供所需信息，保护年长者们免受网络威胁。

WHAT DANGERS ARE WE EXPOSED TO?

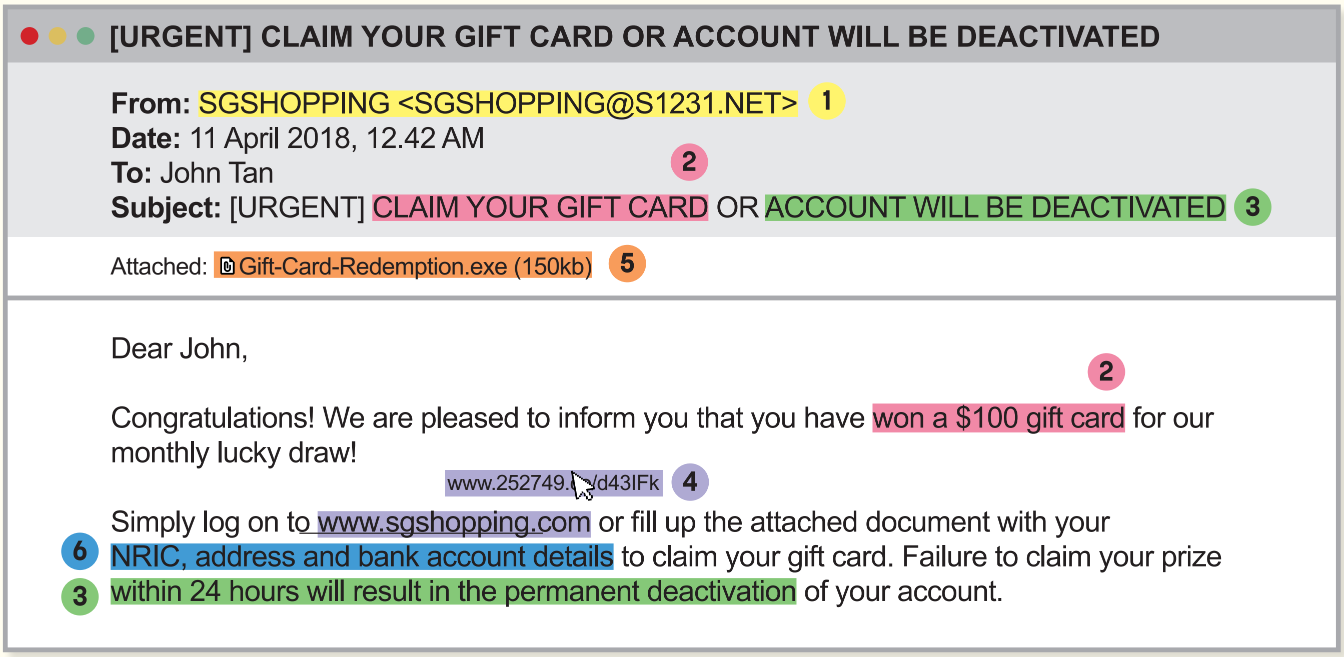
As we go online more often to do banking or shopping at our own convenience, we are at risk from cyber threats in the form of online scams and data theft.

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



[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) 5

Dear John,

Congratulations! We are pleased to inform you that you have won a $100 gift card 2 for our monthly lucky draw!

www.252749.co/d43IFk 4

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 3 within 24 hours will result in the permanent deactivation of your account.

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

www.paypal.com
www.paypa1.com

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)

我们面临怎样的风险？

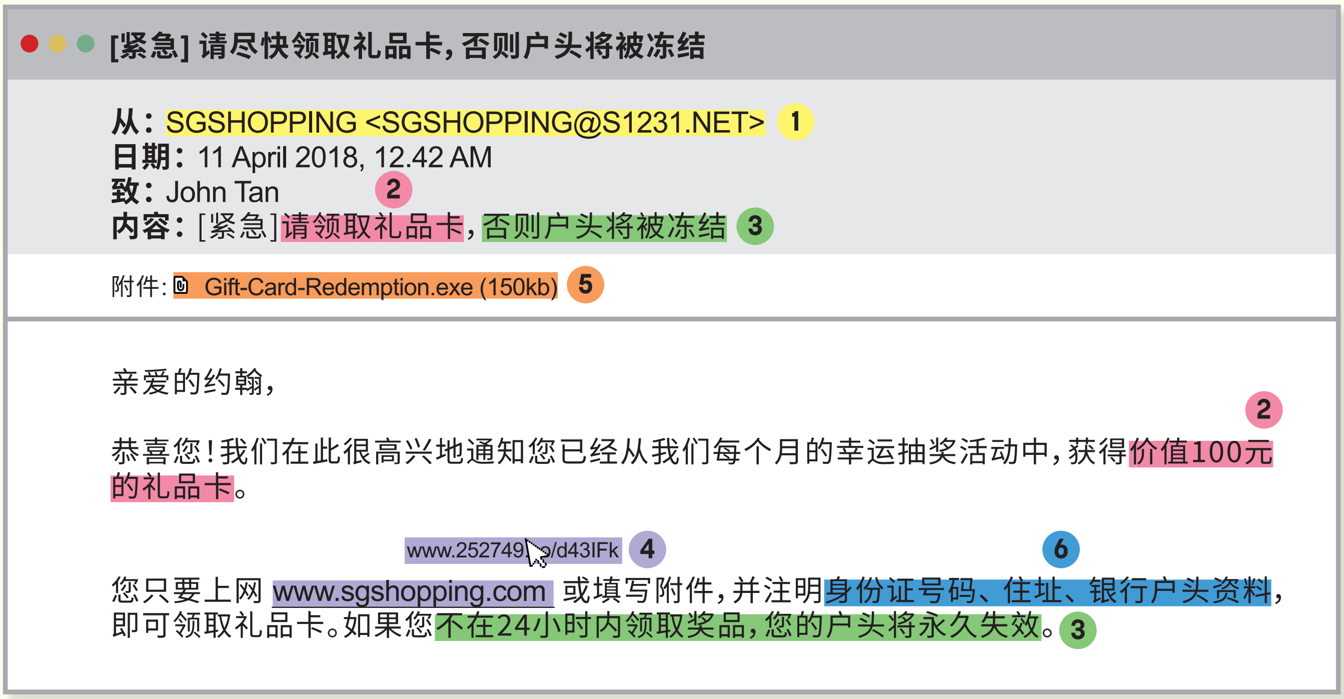
随着网上银行以及网上购物的普及，我们也面临网络诈骗和窃取资料的网络风险。

什么是网络钓鱼？

网络钓鱼是网络罪犯使用的一种手法，目的是诱使受害者提供您的个人和财务信息，如密码、一次性密码（OTP）或银行账户号码。

网络罪犯可能冒充政府或银行等组织联系您，声称有问题需要您立刻注意。他们可能通过电话、短信、通信应用程序、电子邮件或网页弹出广告进行联系。

如何识别电邮中的钓鱼迹象



[紧急] 请尽快领取礼品卡，否则户头将被冻结

从： SGSHOPPING <SGSHOPPING@S1231.NET> 1
日期： 11 April 2018, 12.42 AM
致： John Tan 2
内容： [紧急]请领取礼品卡，否则户头将被冻结 3

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

亲爱的约翰，

2
恭喜您！我们在此很高兴地通知您已经从我们每个月的幸运抽奖活动中，获得价值100元的礼品卡。

www.252749.o/d43IFk 4 6
您只要上网 www.sgshopping.com 或填写附件，并注明身份证号码、住址、银行户头资料，即可领取礼品卡。如果您不在24小时内领取奖品，您的户头将永久失效。3

1

没有预料、突如其来的电邮、WhatsApp或手机简讯

2

承诺提供诱人的奖品

3

使用语调紧急或带威胁性的字眼

4

www.paypal.com
www.paypa1.com

不协调和具误导性的信息

5

含可疑链接或附件

6

索取机密资料，如个人或银行资料、密码或一次性密码（OTP）

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:

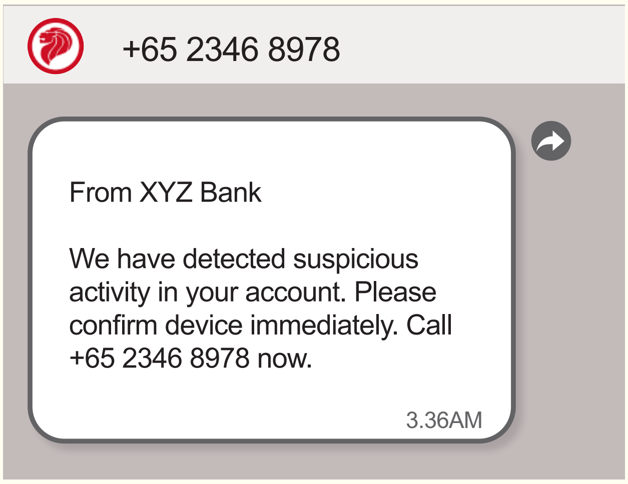
- USE ONLY OFFICIAL E-payment apps (e.g. DBS Paylah!, GrabPay).
- SET UP BANK TRANSACTION ALERTS by setting up email or SMS notifications to help you keep track of transactions.
- CHECK that the QR code for payment is not tampered with.

** 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.



+65 2346 8978

From XYZ Bank

We have detected suspicious activity in your account. Please confirm device immediately. Call +65 2346 8978 now.

3.36AM

QR码网络钓鱼

网络罪犯也可能欺骗您去扫描一个QR码，将您连结到一个要求提供您个人信息的网站。网络罪犯也可能在QR码中嵌入恶意软件*，从受害人的行动通讯设备中窃取信息。

- 除非能确定是合法的要求，否则**不要透露**任何个人或财务信息。
- **不要扫描**随意放置在公共场所的贴纸或传单上的QR码（特别是那些提供优惠券或折扣），或看起来像被篡改过的QR码。

使用QR码进行电子支付时：

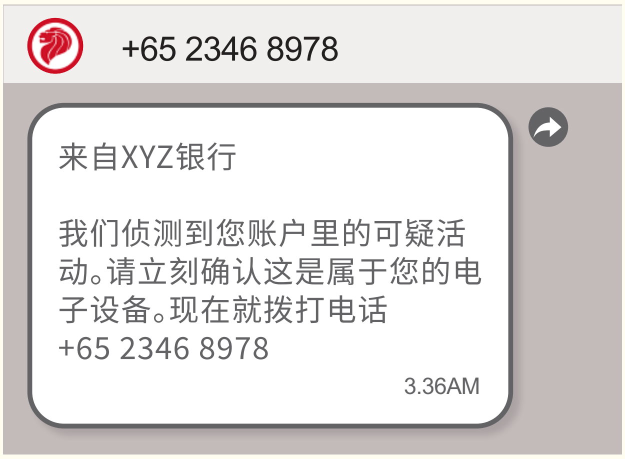
- **只使用官方**的电子支付应用程序（如DBS Paylah!, GrabPay）。
- **设定银行交易提示**的电子邮件或短信通知来追踪支付情况。
- **检查**用于支付的QR码是否被篡改。

**恶意软件是一种入侵您的电子设备并造成损害的软件，这包括窃取个人资料，破坏甚至删除个人数据.*

如何识别网络钓鱼/网上骗局

冒充骗局

- **“技术支援”**
  诈骗者可能声称自己是网络安全局、警方或电信公司的工作人员，正在调查您网络上的可疑活动。
- **“银行钓鱼”**
  诈骗者谎称是银行员工，要求您遵循紧急指示，解决一些银行账户或技术问题，或为一个不存在的优惠要求您提供个人详细资料。
- **“社交媒体冒充”**
  诈骗者可能会冒充为您的朋友、家人或同事，并在社交媒体上与您联系，要求您提供个人资料或“错误”发送给您的一次性密码（OTP）。
- **“WHATSAPP账户劫持”**
  诈骗者可能谎称是您所认识的人或机构，并要求您向他们发一个六位数的验证码。



+65 2346 8978

来自XYZ银行

我们侦测到您账户里的可疑活动。请立刻确认这是属于您的电子设备。现在就拨打电话+65 2346 8978

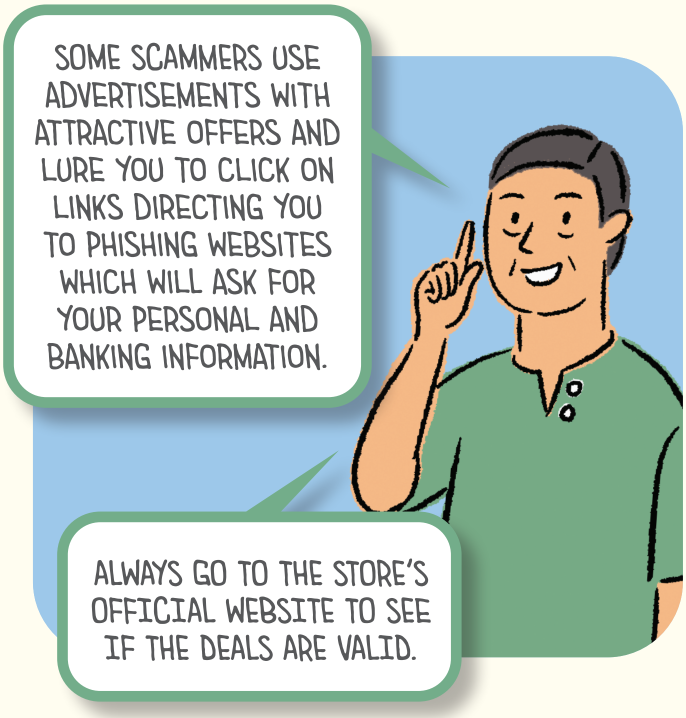
3.36AM

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.


SOME SCAMMERS USE ADVERTISEMENTS WITH ATTRACTIVE OFFERS AND LURE YOU TO CLICK ON LINKS DIRECTING YOU TO PHISHING WEBSITES WHICH WILL ASK FOR YOUR PERSONAL AND BANKING INFORMATION.
ALWAYS GO TO THE STORE'S OFFICIAL WEBSITE TO SEE IF THE DEALS ARE VALID.

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.

电子商务骗局

利用诱人折扣和其他令人难以置信的优惠，骗子会坚持要求在交货前先付款或银行转账。一旦他们收到钱，就再也无法联系。

如何保护自己?

- **只从信誉良好的网站购买商品。**

- **请通过购物平台付款。**这样一来，卖家只有在买方收到货物后才会取得款项。

- **请时刻保持警惕，**如果优惠好得难以置信，请务必三思。

有些诈骗罪犯会以提供诱人优惠的广告来误导你点击钓鱼网站，引诱你提供个人和银行的资料。
为了安全起见，你应该通过商家的官网查看这些优惠有没有效。

如果您或您所认识的人收到了网络钓鱼简讯……

- **不要惊慌。**您可致电给家人或朋友，或拨打反诈骗热线1800-722-6688寻求协助。

- 除非您在等待海外来电，否则**不要接听**显示 “+”号的来电。

- 如果有人“建议”安装任何软件，**不要安装** 。

- **不要透露您的密码、**OTP或个人和银行信息。

- **不要汇款**给任何人。

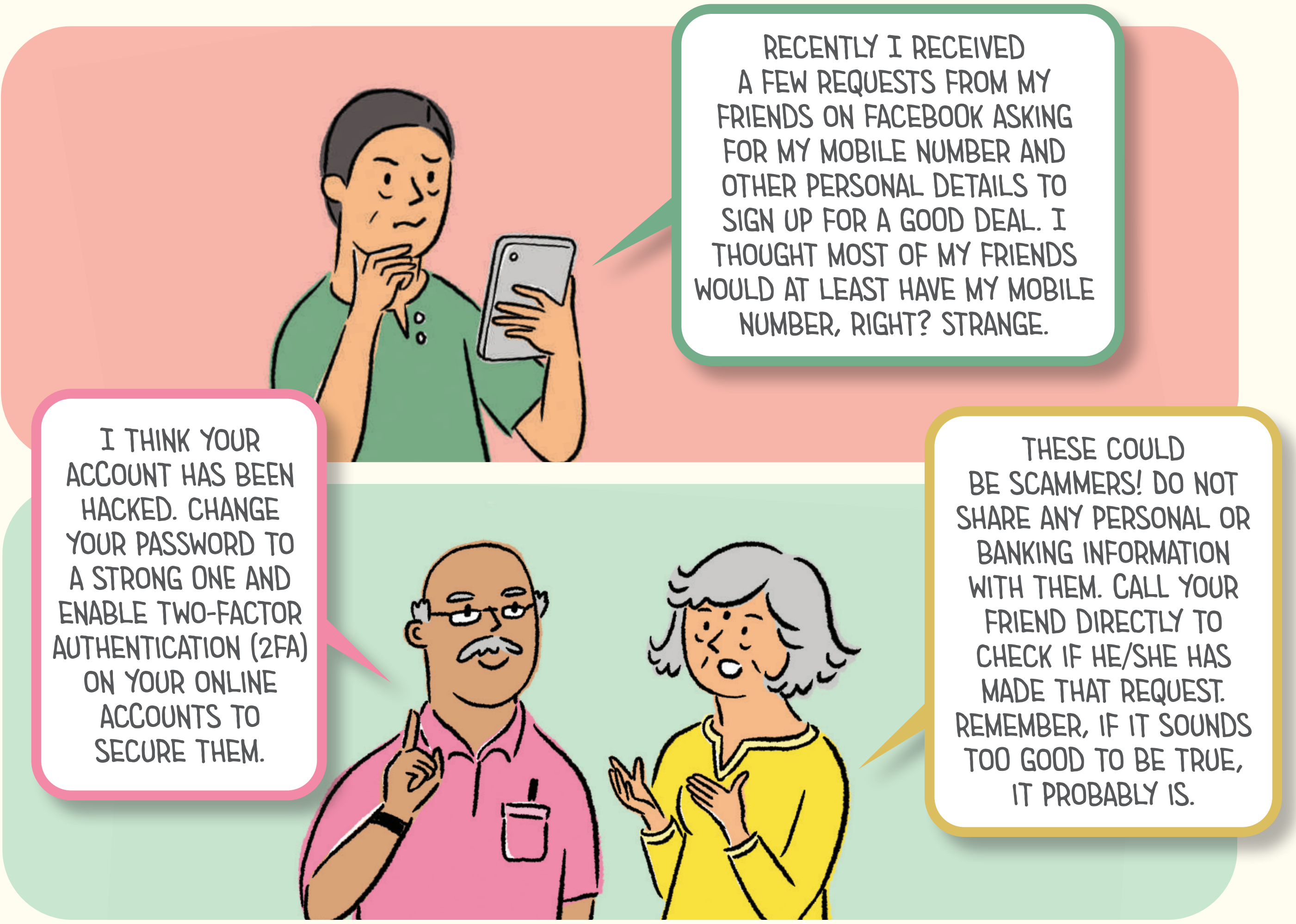
- **不要点击**任何附件或链接，应该直接删除。

- 为了多一层保护，**请启动WHATSAPP中的双重认证功能。**

- 通过直接拨打政府/企业的官方热线或查询官方应用程序/网站来**验证可疑的电话或信息。**不要通过电话或信息中提供的联系方式与该组织联系。

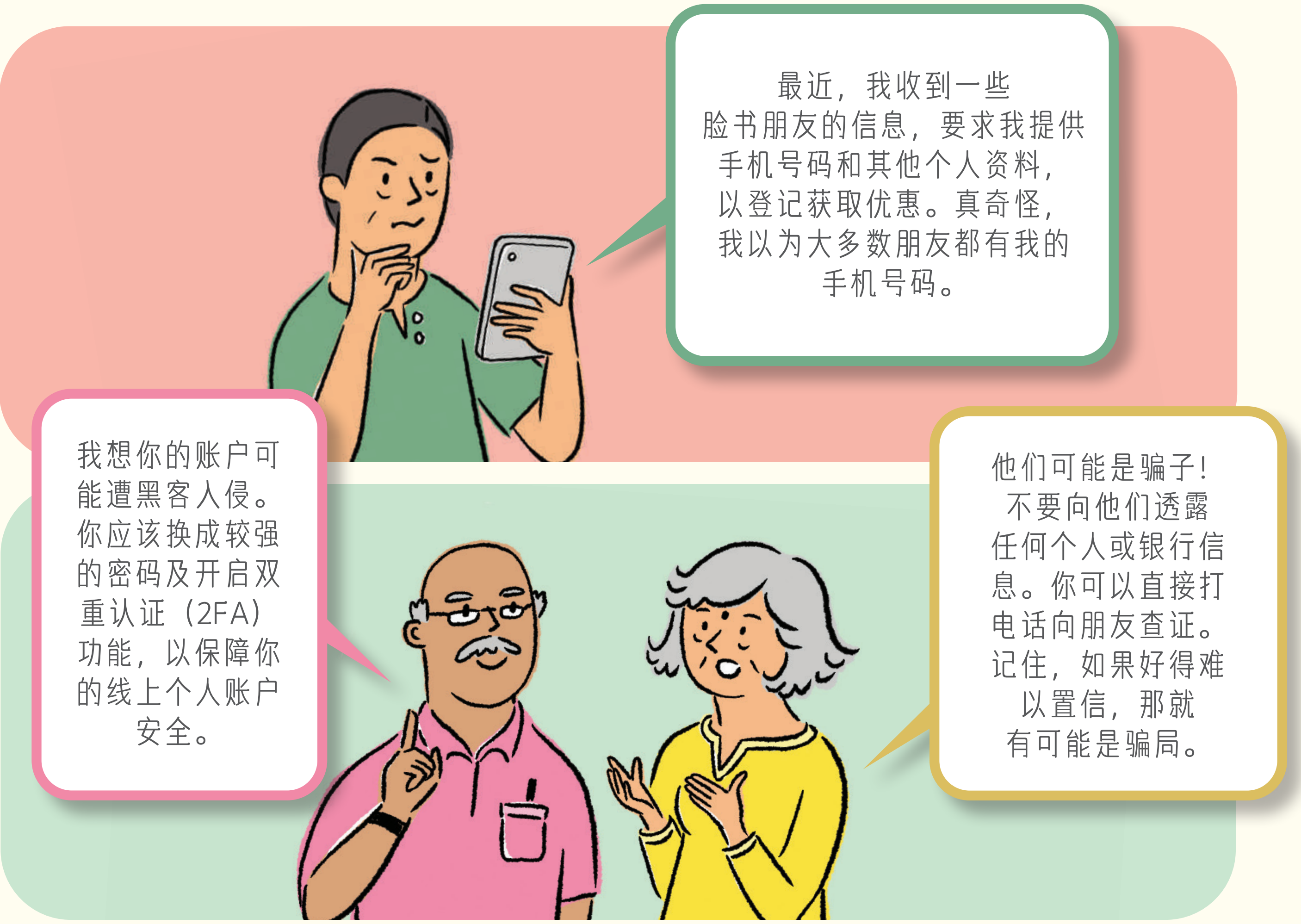
- **注意，**政府官员绝不会要求您立即在网上付款，或指示您把钱转到任何本地或外国银行账户，或不允许您挂断电话。

- 如果链接或电子邮件地址中没有“**.gov.sg**”，**请参考www.gov.sg/ trusted-sites**的可靠政府相关网站列表。


RECENTLY I RECEIVED A FEW REQUESTS FROM MY FRIENDS ON FACEBOOK ASKING FOR MY MOBILE NUMBER AND OTHER PERSONAL DETAILS TO SIGN UP FOR A GOOD DEAL. I THOUGHT MOST OF MY FRIENDS WOULD AT LEAST HAVE MY MOBILE NUMBER, RIGHT? STRANGE.
I THINK YOUR ACCOUNT HAS BEEN HACKED. CHANGE YOUR PASSWORD TO A STRONG ONE AND ENABLE TWO-FACTOR AUTHENTICATION (2FA) ON YOUR ONLINE ACCOUNTS TO SECURE THEM.
THESE COULD BE SCAMMERS! DO NOT SHARE ANY PERSONAL OR BANKING INFORMATION WITH THEM. CALL YOUR FRIEND DIRECTLY TO CHECK IF HE/SHE HAS MADE THAT REQUEST. REMEMBER, IF IT SOUNDS TOO GOOD TO BE TRUE, IT PROBABLY IS.

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.


最近，我收到一些脸书朋友的信息，要求我提供手机号码和其他个人资料，以登记获取优惠。真奇怪，我以为大多数朋友都有我的手机号码。
我想你的账户可能遭黑客入侵。你应该换成较强的密码及开启双重认证（2FA）功能，以保障你的线上个人账户安全。
他们可能是骗子！不要向他们透露任何个人或银行信息。你可以直接打电话向朋友查证。记住，如果好得难以置信，那就有可能是骗局。

如果您无意间泄露了个人和/或银行信息，应该立即采取以下步骤：

- **立即更改账户密码**（Singpass或银行），包括使用此密码的所有其他账户。
- 如果泄露了信用卡资料，**请通知所属银行**。
- **核查所属账户**是否有未经授权的提款或购买行为。
- 如果有任何金额损失，**请向警方报案**。
- **使用防毒软件**来扫描您的系统是否有任何恶意软件。恶意软件是一种入侵电子设备并造成损害的软件，这包括资料遭窃，破坏或甚至被删除。
- 如果您想提交事件报告，**请到网络安全局紧急反应组(SingCERT)网页www.csa.gov.sg/singcert/reporting**。

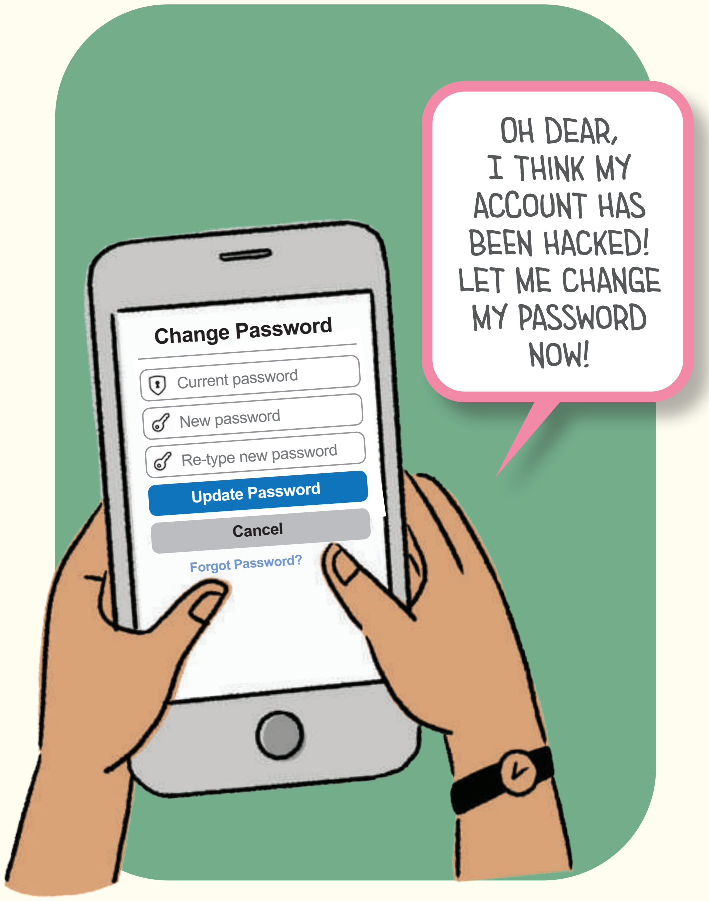
KEEP TABS ON YOUR ONLINE ACCOUNT

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!

维护个人账户的安全

如何保障您的个人和财务信息安全？

- **密码的设定**尽量个人化，最好含有至少12个字母，或使用只有自己知道的短句，例如：IhadKAYAtoastAT8AM!

- **密码应由**大小写字母、号码和符号组成。

- 尽可能**启动双重认证（2FA）**。除了网络银行外，社交媒体、电子邮件、购物和政府账户也可以使用2FA。

如果遭黑客入侵该怎么办？

如果您还能登入受影响的账户，

- 请将所有与这个账户有链接的个人通讯设备**登出这个账户**。

- **立刻更换密码**，并启动双重认证（若有）以保护自己。

如果无法登入自己的账户：

- **请联系有关平台**，例如银行或社交媒体平台，请立即通报，并寻求协助取回您的账户。

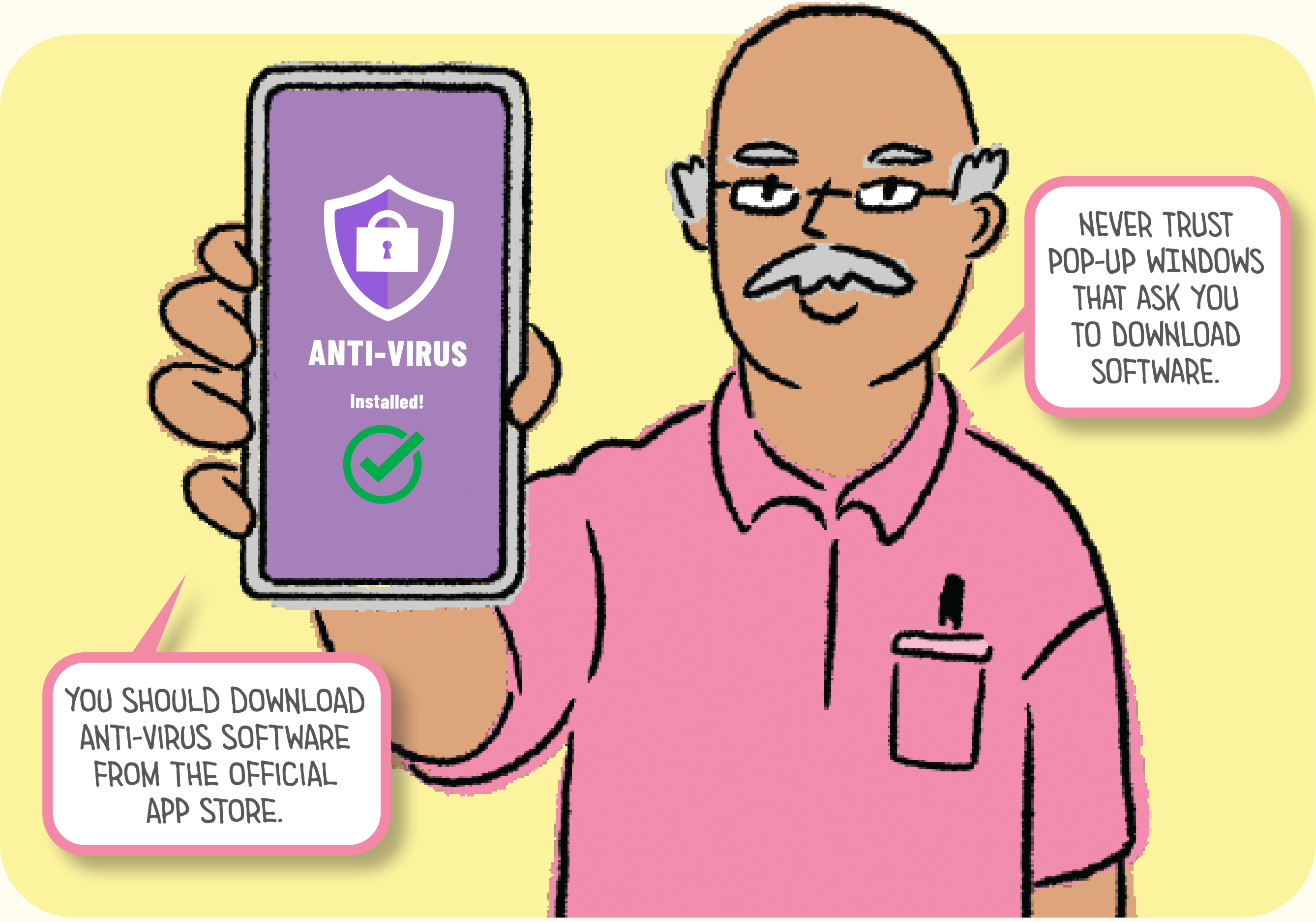
- 如果信用卡/借记卡有不实的消费记录，请**通知**您的银行，并立即注销受影响的卡。

- 如果涉及金钱损失，请到邻近的警局、邻里警岗或上网**https://eservices.police.gov.sg** **报案**。

- 如果账户被盗，冒充者可能会联系您认识的人或机构。**请通知家人朋友**不要泄露任何个人资料。

活动

想知道密码是否牢固？快来使用密码检测器就知道！


ANTI-VIRUS
Installed!
NEVER TRUST POP-UP WINDOWS THAT ASK YOU TO DOWNLOAD SOFTWARE.
YOU SHOULD DOWNLOAD ANTI-VIRUS SOFTWARE FROM THE OFFICIAL APP STORE.

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.

防毒软件
成功安装!
不要相信那些指示你下载软件的弹出式信息。
你应该从官方应用程序商店下载防毒软件。

什么是恶意软件?

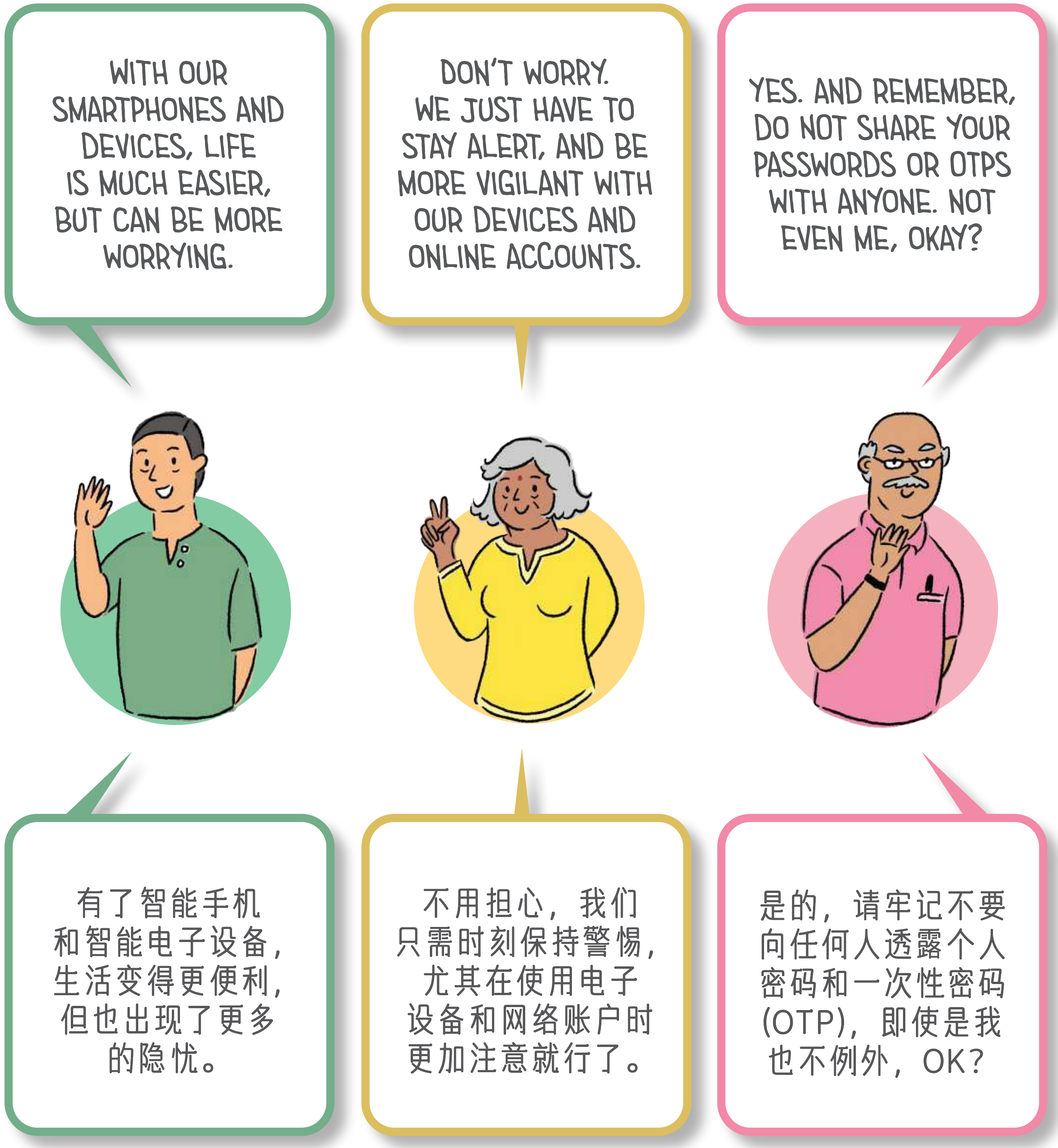
恶意软件是一种入侵您的电子设备并造成损害的软件,这包括窃取个人资料,破坏甚至删除个人数据.

如何保护您的电子设备免受恶意软件入侵?

- 请从官方应用程序商店**下载防病毒软件**以保障网络安全。

- 请定期并及时**更新软件**,以确保电子设备安全。更新软件可以有效防堵电子设备的漏洞。

- 通过无线网络Wi-Fi**自动更新**,或在睡前为您的手机或平板电脑充电时,设置时段以更新软件。


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?
有了智能手机和智能电子设备，生活变得更便利，但也出现了更多的隐忧。
不用担心，我们只需时刻保持警惕，尤其在使用电子设备和网络账户时更加注意就行了。
是的，请牢记不要向任何人透露个人密码和一次性密码(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 the Scam Alert webpage of the National Crime Prevention Council.

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，或全国罪案防范理事会反诈骗网页查询。

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