BETTER CYBER SAFE THAN SORRY

A GUIDE TO STAYING SAFE ONLINE

安全使用网络　避免憾事发生

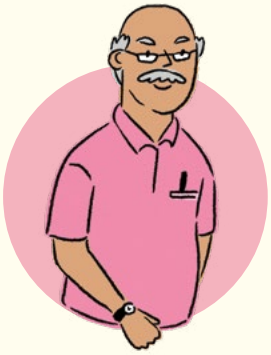
网络安全须知

CSA SINGAPORE

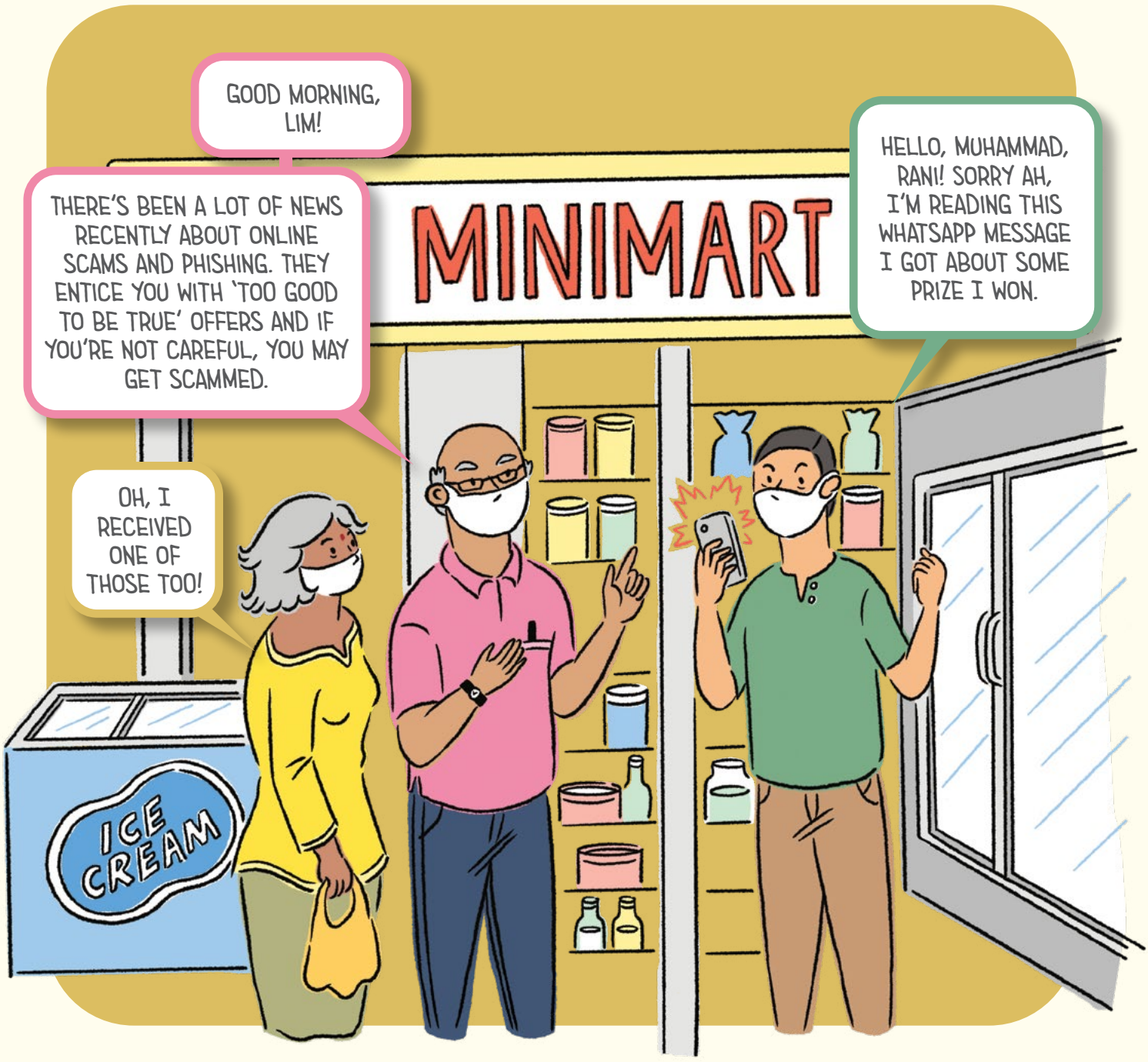
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

LIM
Taxi Driver

RANI
Administrative Assistant



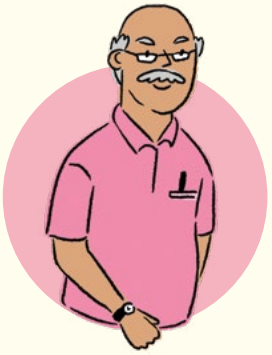
MUHAMMAD
Retired Teacher



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.

林
德士司机

拉妮
行政助理



穆罕默德
退休教师

这听起来是不是很熟悉？智能手机和其他智能设备的普及使生活更便利，但我们也更应该小心防范网络罪案。我们如何识别骗局保护自己呢？这本手册将为您提供所需信息，助你安全上网。

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 2
Subject: [URGENT] CLAIM YOUR GIFT CARD OR ACCOUNT WILL BE DEACTIVATED 3

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

Dear John,

5

Congratulations! We are pleased to inform you that you have won a $100 gift card 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 3 hours will result in the permanent deactivation 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

什么是网络威胁?

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。

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) 4

亲爱的约翰,

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。 5

www.252749.co/d43lFk 1

您只要上网 www.sgshopping.com 或填写附件,并注明身份证号码、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。 6 3

1

不协调和具误导性的信息

2

没有预料、突如其来的邮件

3

使用语调紧急或带威胁性的字眼

4

可疑的附件

5

承诺诱人奖品

6

索取机密资料

HOW TO SPOT PHISHING/ONLINE SCAMS

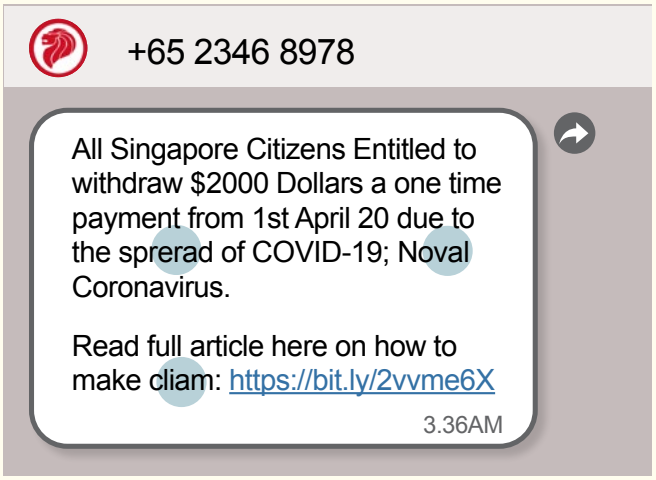
IMPERSONATION SCAMS

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

如何防范网络钓鱼和网络诈骗

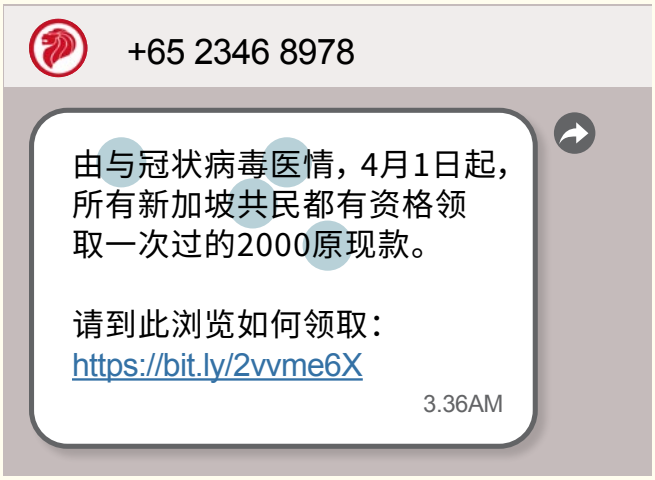
冒充骗局

这些罪犯可能冒充可信赖的机构例如政府官员或银行人员，打电话,发简讯或发WhatsApp信息给您，要求您遵循紧急指示，解决银行户账或一些虚假的技术问题，或要求提供个人资料以换取其实是骗局的优惠。

- **请注意，**政府官员绝不会通过电话要您立刻进行网络转账，或把钱转账至本地或外国银行户口，也不会阻止您挂电话

- 如果电邮或短信中错字或其他错误连连，**务必提高警惕**

- 若链接或电邮地址无“**gov.sg**”，**请到 www.gov.sg/trusted-sites** 参阅可信赖的政府相关网址名单



谎称技术支援骗局

诈骗者可能自称是网络安全局或电信公司人员，正在调查您网络上可疑的活动。

- **不要下载**他们所“建议”的任何软件应用程序

- **不要透露**任何个人资料或财务信息

银行相关的网络钓鱼骗局

- **别向任何人透露您的密码**、一次性密码 (OTP) 或个人与财务信息

- **不要**汇款给刚在网上认识的人

- 如果您不是等着接任何来自海外的电话，请对显示“+”符号的来电**保持警惕**。本地电话不会显示“+”符号

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:

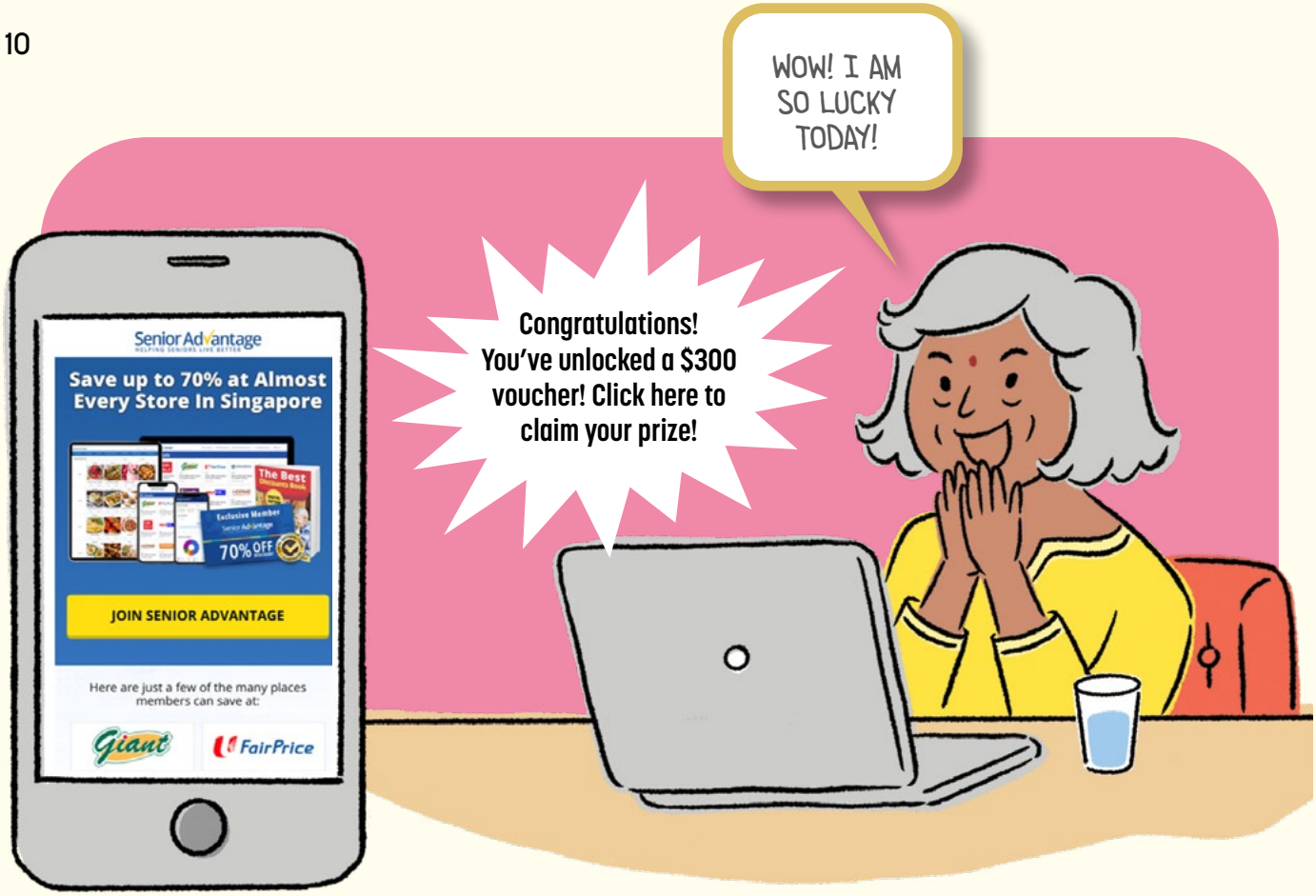
- CHANGE THE PASSWORD FOR YOUR BANKING ACCOUNT IMMEDIATELY, including all other accounts using this password
- ALERT YOUR BANK if you revealed credit card details
- MONITOR YOUR ACCOUNT for unauthorised withdrawals or purchases
- MAKE A POLICE REPORT if any funds are missing
- USE AN ANTI-VIRUS SOFTWARE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

如果您或您所认识的人收到了网络钓鱼简讯、电话或电邮……

- **请不要理会**并将其删除
- **不要点击**短信、邮件中的任何附件或链接

如果您收到了广告或信息，急迫要您遵循一些指示，请勿惊慌。您可以打电话给亲朋好友征询他们的意见。如果要查询有关防范诈骗的信息，请上网www.scamalert.sg或拨打反诈骗热线1800-722-6688查询。如果您无意中点击了附件或链接，请尽快即刻采取以下行动：

- **立即更改密码**，包括所有使用这个密码的其他账户
- 如果您透露了信用卡信息，**请通知信用卡所属银行**
- **注意账户**是否有未经授权的提款或结账
- 如果有任何金钱损失，**请马上报警**
- **使用防病毒软件**扫描系统，以策安全
- 如果您想呈交事件报告，**请上新加坡网络安全局电脑紧急反应组(SingCERT)网站 www.csa.gov.sg/singcert/reporting**



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

网络诈骗

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，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

社交媒体冒充诈骗

骗子也可能冒充您的朋友、家人或同事的身份，在社交媒体上与您联系，询问个人资料或谎称“误发”一次性密码 (OTP) 给您。

如何保护自己？

- **别向任何人，包括家人朋友，透露**您的个人资料、银行信息或一次性密码
- **提防**来自任何人，包括亲朋好友的不寻常要求或提议

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!

维护个人账户的安全

如何保障您的个人和财务信息安全?

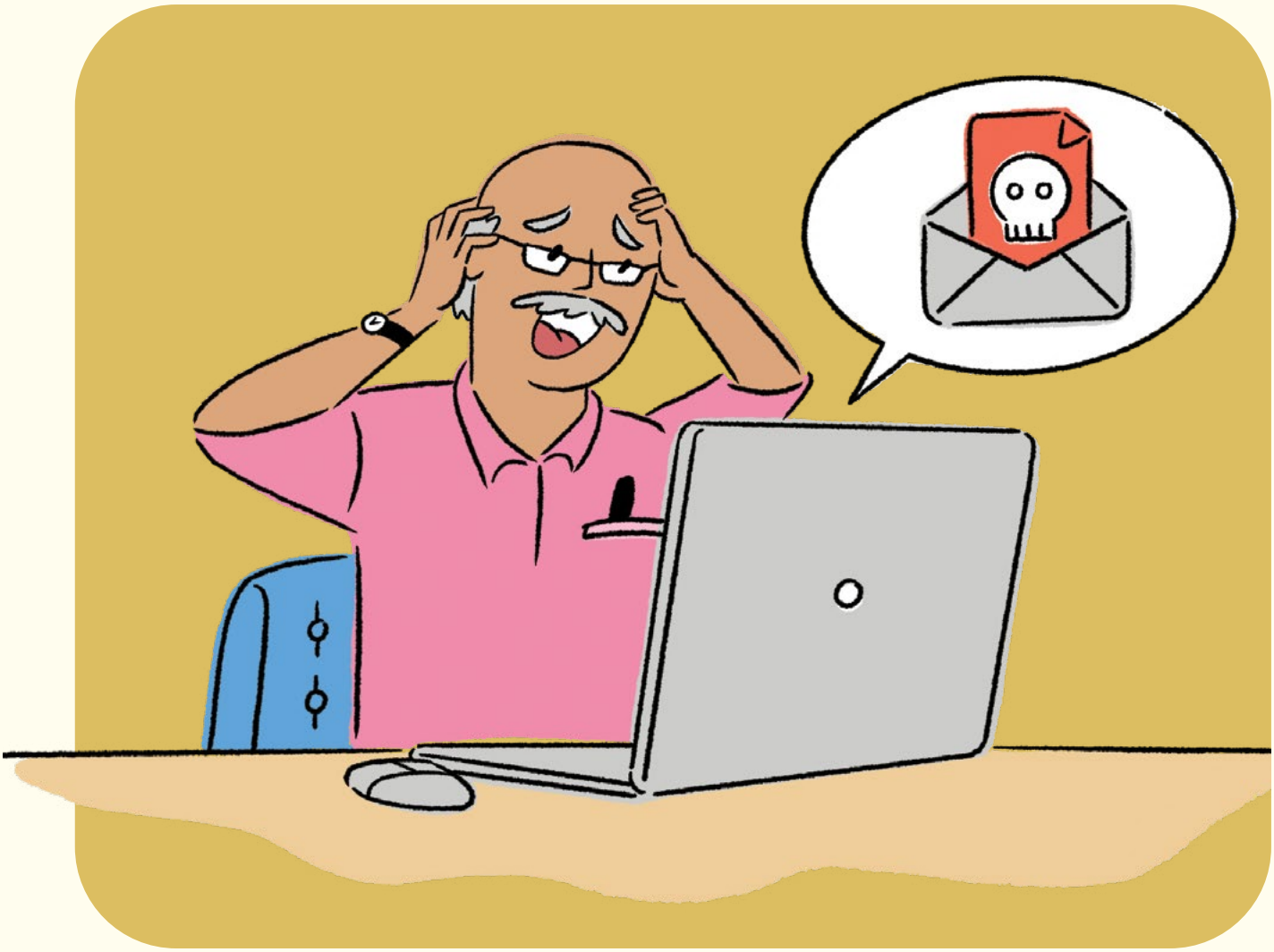
- **密码的设定**尽量个人化,最好含有至少12个字母,或使用只有自己知道的短句,例如:IhadKAYAtoastAT8AM!
- **密码应由**大小写字母、号码和符号组成
- **尽可能启动双重认证(2FA)**。除了网络银行外,社交媒体、电子邮件、购物和政府账户也可以使用2FA

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
- 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,请到邻近的警局或邻里警岗或上网**https://eservices.police.gov.sg报案**
- 如果账户被盗,冒充者可能会联系受害者的亲朋好友。**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!

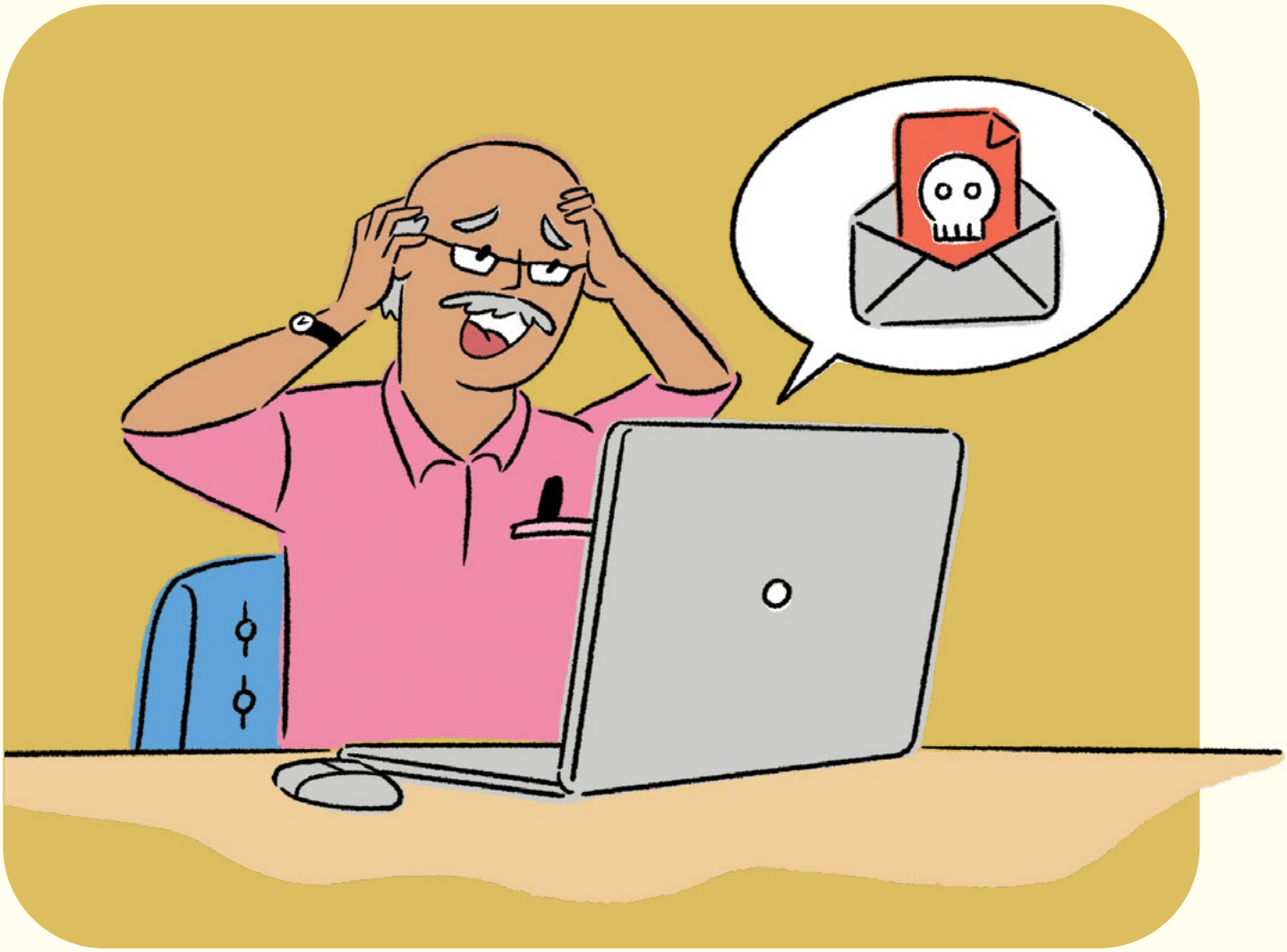


MALWARE. WHAT EXACTLY IS IT?

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



什么是恶意软件？

恶意软件是一种导致电脑、智能手机、平板电脑遭病毒入侵的软件。它能造成很大的损害，包括资料遭窃、破坏或甚至被删除。

如何让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**，或在睡前给您的手机或平板电脑充电时，设置时段更新软件

WITH OUR SMARTPHONES AND DEVICES, LIFE IS MUCH EASIER, BUT ALSO SCARIER.

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。

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

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。

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

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, 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

欲知更多详情，请报名参加“询问网络专家”系列，或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: