

BE CYBER SAFE

A GUIDE TO STAYING SAFE ONLINE



安全上网 网络安全须知



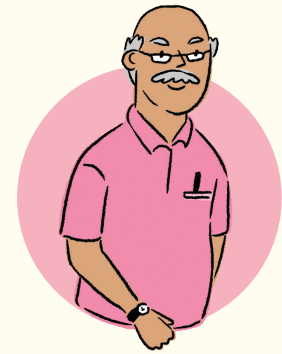
SINGAPORE
POLICE FORCE
SAFEGUARDING EVERY DAY



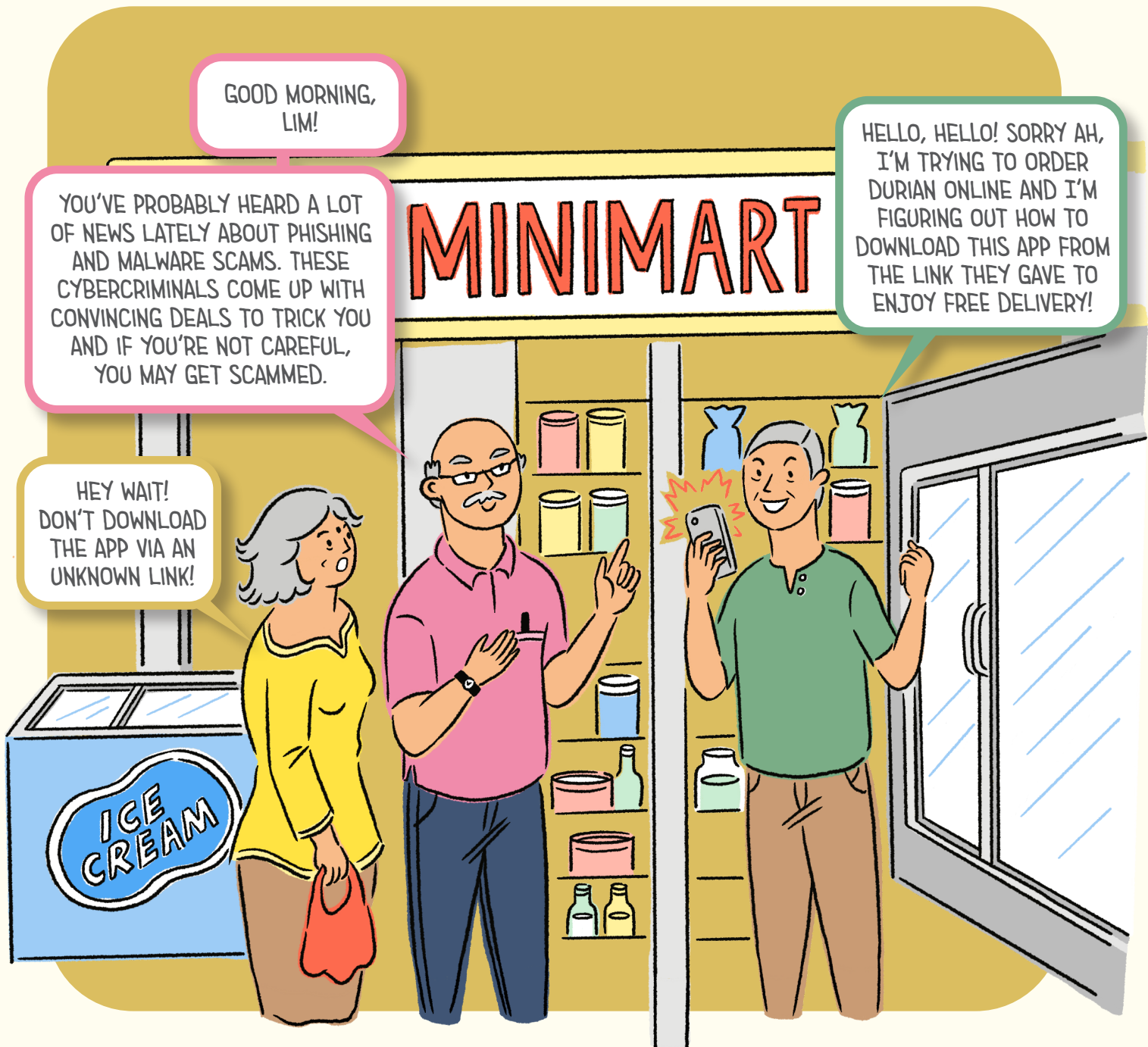
LIM
Taxi Driver



RANI
Administrative Assistant



MUHAMMAD
Retired Teacher



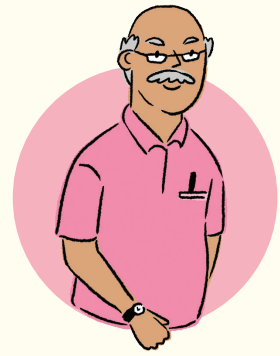
The increased use of smartphones and other smart devices has made life more convenient but at the same time, there are also cybercrimes which we need to be aware of. This handbook will arm you with the information you need to protect yourselves from cyber threats.



林
德士司机



拉妮
行政助理



穆罕默德
退休教师

早上好，林！

最近有很多网络钓鱼诈骗的新闻。这些网络罪犯用诱人的条件吸引你，一不小心就会受骗上当。

等等！不要通过来历不明的链接下载应用程序！

MINIMART

你们好！我要上网订购榴莲，我想知道如何通过他们提供的链接下载这个应用程序，以享有免费送货服务！



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?

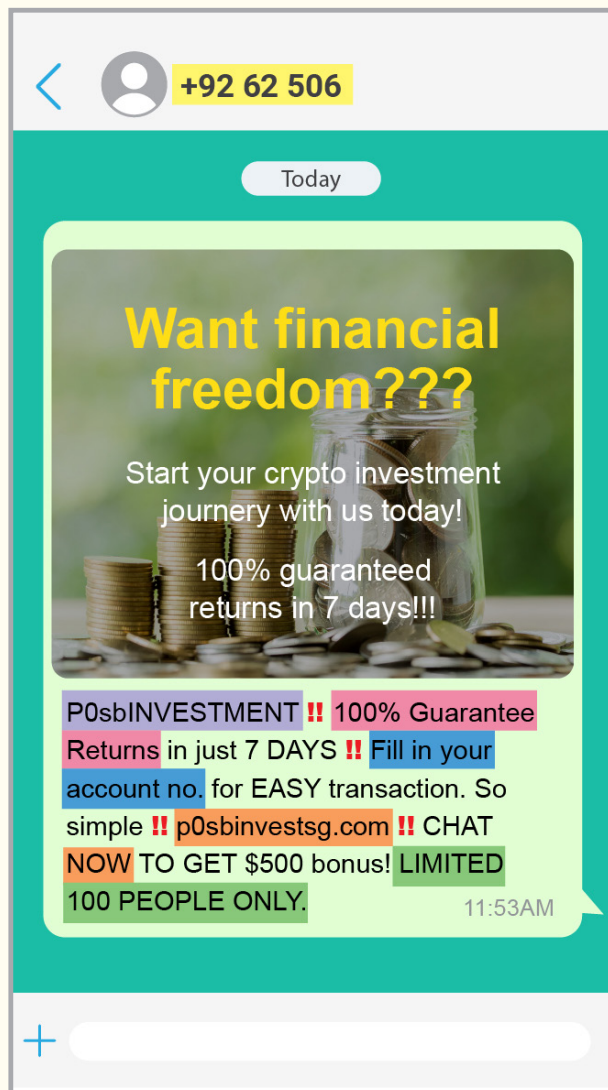
As we go online more often to do banking or shopping at our own convenience, we are at risk from cyber threats in the form of online scams and data theft.

WHAT IS PHISHING?

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

Cybercriminals 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 messages



1. Unexpected emails or messages



2. Promise of attractive rewards



3. Use of urgent or threatening language



4. Mismatched & misleading information



5. Suspicious links or attachments.



6. Request for personal information

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。

如何识别网络钓鱼信息



1. 没有预料, 突如其来的电邮或手机简讯



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. 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

TYPES OF PHISHING SCAMS

E-COMMERCE SCAMS

Using huge discounts and offers as a draw, cybercriminals will insist on immediate payment or bank transfers before delivery. Once they have received the money, they will be uncontactable. They may ask you to download a malicious app to make payment.

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.
- **DO NOT DOWNLOAD** apps or software from unknown or unofficial sources.
- **DO NOT CLICK** on any attachment or link in the message. Delete it.

BE CAREFUL OF DEALS THAT ARE TOO GOOD TO BE TRUE. ALWAYS GO TO THE STORE'S OFFICIAL WEBSITE TO SEE IF THE DEALS ARE VALID.

ONLY DOWNLOAD APPS FROM OFFICIAL APP STORES (GOOGLE PLAY STORE OR APPLE APP STORE).

INVESTMENT SCAMS

Cybercriminals may approach you through social media or communications platforms to offer you "investment opportunities" and trick you into conducting transactions under the pretext of the 'investments'.

- **STAY VIGILANT AND BE CAUTIOUS** when making investment decision, especially when the returns are too good to be true.
- **VERIFY SUSPICIOUS MESSAGES** by calling the company's official hotline or visit their official website directly. Do not contact the organisation via the contact details provided in the message.
- **DO NOT SHARE** your password, OTP or personal and banking information.


网络钓鱼诈骗类型

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。他们可能会要求您下载恶意应用程序来付款。

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。
- 不要下载来历不明或非官方来源的应用程序或软件。
- 不要点击任何附件或链接，而应删除信息。



小心那些好得难以置信的优惠。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。

只从官方应用商店（谷歌或苹果应用商店）下载应用程序。

投资诈骗

网络罪犯可能会通过社交媒体或通信平台，向您提供“投资机会”，并以“投资”为由诱骗您进行交易。

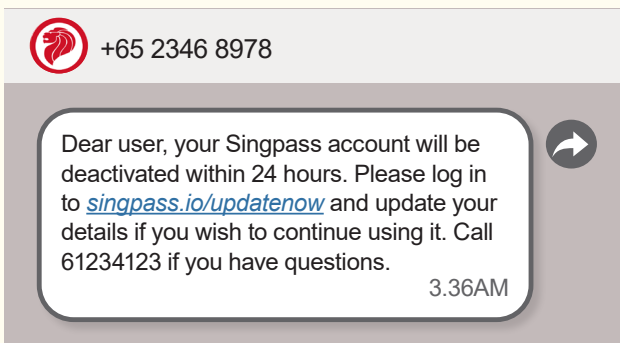
- 保持警惕和谨慎做出投资决策，尤其当回报好得难以置信。
- 直接拨打企业的官方热线或浏览其官网，以查证可疑信息。不要通过信息中提供的联系方式联络该机构。
- 不要透露您的密码、OTP或个人和银行信息。

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.

GOVERNMENT OFFICIAL IMPERSONATION SCAMS

Cybercriminals pretend to be from government organisations asking you for personal information or to download malicious apps to steal your money.



Singpass and banks no longer send clickable links in emails or SMSes.

FAKE FRIEND SCAMS

Cybercriminals may impersonate a family member or friend and capitalise on the friendship element to trick you into transferring money to them online.

QR CODE PHISHING

Cybercriminals may also trick you into scanning 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.

WHATSAPP ACCOUNT TAKEOVER SCAMS

Scammers may pretend to be your contact and request for a six-digit verification code to be sent to them.

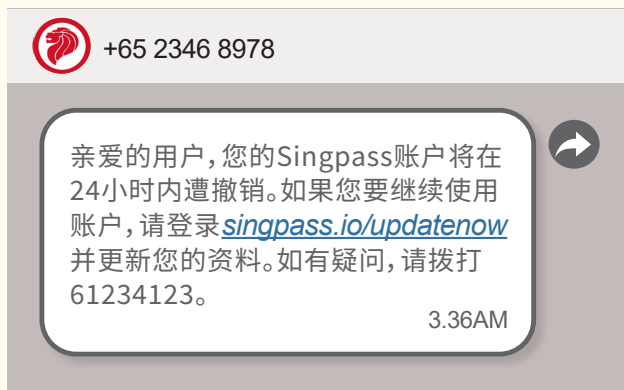
- **DO NOT CLICK ON SUSPICIOUS LINKS.** Banks do not send clickable links in emails or SMSes or ask for your banking credentials via text.
- **DO NOT SHARE PERSONAL OR FINANCIAL INFORMATION** unless you are sure it is a legitimate request.
- **DO NOT SCAN** QR codes in the form of stickers or flyers placed randomly in public places.
- **DO NOT PANIC.** Government officials will never demand immediate payment online or instruct you to transfer money to any local or foreign bank account.
- **VERIFY SUSPICIOUS CALLS OR MESSAGES** by calling the official hotline or visit official app/website directly. You can also verify calls or messages from your friend by calling the number saved in your contact.
- **SET UP BANK TRANSACTION ALERTS.** by setting up email or SMS notifications to help you keep track of transactions.
- **ADD SCAMSHIELD APP** which can protect you by detecting scam messages and blocking scam calls.
- **CHECK THE LIST** of trusted government-related websites at www.gov.sg/trusted-sites if the link or email addresses does not have “.gov.sg” in them.

银行钓鱼

诈骗者谎称是银行员工,要求遵循紧急指示,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。

冒充政府官员诈骗

网络罪犯冒充政府机构,要求您提供个人资料或下载恶意应用程序,以盗取您的钱财。



Singpass和银行不会在电邮或手机短信发送可点击的链接。

假朋友诈骗

网络罪犯可能会冒充您的家人或朋友,利用你们的情谊,诱骗您在网上转账给他们。

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。

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。

- **不要点击可疑链接。**银行不会在电邮或手机短信发送可点击的链接,或要求您通过短信提供银行资料。
- 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**随意放在公共场所的贴纸或传单上的QR码。
- **不要惊慌。**政府官员不会要求您立即上网付款,或指示您向任何海内外银行账户转账。
- 直接拨打官方热线或浏览官方应用程序/官网,以**查证可疑来电或信息**。您也可以拨打存在您联络簿的号码,以查证朋友的来电或信息。
- **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。
- **添加ScamShield应用**,以检测诈骗信息和屏蔽诈骗电话,保护自己。
- 如果链接或电邮地址中不含“.gov.sg”,可上网www.gov.sg/trusted-sites **查看**可靠的政府相关网站列表。

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. Cybercriminals may even gain remote access to your devices, retrieve your banking credentials and make withdrawals from your bank accounts.

- **DOWNLOAD ANTI-VIRUS APPS** to detect malware and malicious phishing links.
- **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 devices is plugged in.



Find the list of recommended anti-virus apps to download. There is no 100% protection and it is important to remain vigilant and adopt good cyber hygiene habits to protect your devices

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 quickly.

NEVER TRUST POP-UP WINDOWS THAT ASK YOU TO DOWNLOAD SOFTWARE.



YOU SHOULD DOWNLOAD APPS FROM OFFICIAL APP STORES!

What should you do if your phone has been infected with malware

- Turn your phone to 'flight mode'. Check that Wi-Fi is switched off and do not switch it on
- Review the apps installed, remove unknown or suspicious apps
- Deep-scan your phone with an updated anti-virus app
- Use a different and trusted device to check for any unauthorised banking or CPF transactions
- As further precautions, consider doing a "factory reset" of your phone.

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。网络罪犯甚至可能会远程入侵您的电子设备，索取您的银行资料，并从您的银行账户中提款。

- **设置反病毒 (Anti-virus) 应用程序**，以检测恶意软件和网络钓鱼链接。
- **请定期并及时更新软件**，以确保电子设备安全。更新软件可以有效封堵电子设备的漏洞。
- **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。

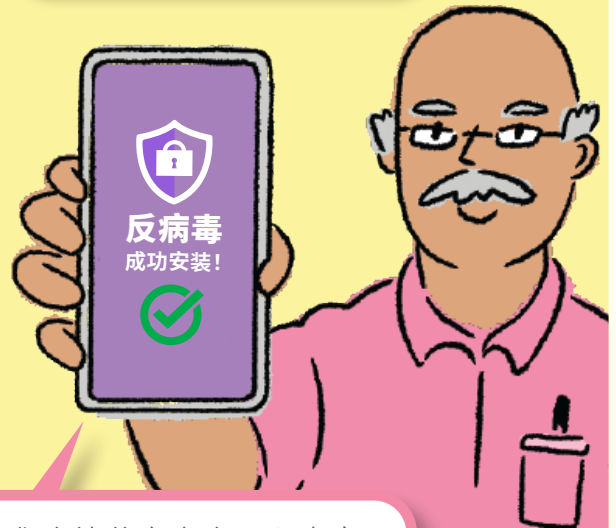


查找推荐下载的反病毒应用程序列表。这些软件不能提供100%的保护，因此您必须保持警惕和培养良好的上网习惯，以保护您的电子设备。

如何识别您的手机是否遭恶意软件入侵？

- 过多和无法解释的数据用量。
- 随意弹出窗口或出现不是您安装的新应用程序。
- 反应或性能明显变慢。
- 电池消耗异常快速。

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。

如果您的手机遭恶意软件入侵，该怎么办？

- 将手机转到“飞行模式”。查看Wi-Fi是否已关闭，不要打开Wi-Fi。
- 检查已安装的应用程序，并删除来历不明的可疑应用程序。
- 使用最新版本的反病毒应用程序，在手机上进行深度扫描。
- 使用不同的可靠设备检查任何未经授权或未经授权的银行或公积金交易。
- 作为进一步的防范措施，考虑对手机进行“出厂重置”。

PROTECT YOURSELF FROM CYBER THREATS

How to protect yourself online

- **BEWARE OF PHISHING SCAMS** by spotting the six signs of phishing.
- **UPDATE YOUR SOFTWARE PROMPTLY** by enabling automatic updates.
- **ADD SCAMSHIELD** to detect scam messages and block scam calls.
- **DOWNLOAD ANTI-VIRUS APP** to detect malware and malicious phishing links.
- **ENABLE TWO-FACTOR AUTHENTICATION (2FA)** where available. Besides internet banking, 2FA is available for social media, email, shopping and government accounts.
- **USE STRONG PASSPHRASES** to keep your online accounts and personal information safe.

How to create a strong passphrase

Step 1: **STRING TOGETHER FIVE DIFFERENT WORDS** that relate to a memory that is unique to you.

Step 2: **USE** uppercase and lowercase letters, numbers and symbols to make at least 12 characters.

E.g. IhadKAYAtoastAT8AM!

DO NOT USE PERSONAL INFORMATION such as your name, NRIC or birthdate, or other easily obtainable information.

DO NOT SHARE YOUR PASSWORDS with anyone or write them down.



ACTIVITY

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



保护自己免受网络威胁

如何在网上保护自己

- 识别网络钓鱼的六大迹象,小心网络钓鱼骗局。
- 开启自动更新功能,及时更新您的软件。
- 添加ScamShield应用,以检测诈骗信息和屏蔽诈骗电话。
- 请从官方应用程序商店下载防病毒软件以保障网络安全。
- 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。
- 使用安全性高的密码短语,以保障您的线上个人账户和资料安全。

如何创建安全性高的密码短语

步骤一:将与您独特记忆有关的五个不同单词串联起来。

步骤二:使用大小写字母、数字和符号组成至少12个字符。

E.g. lhadKAYAtoastAT8AM!

不要使用个人资料,例如您的姓名、身份证号码或出生日期,或其他容易取得的信息。

不要把密码告诉任何人或写下来。



活动

想知道密码是否牢固? 快来使用密码检测器就知道!



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



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 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 still have access to your account,

- **LOG OUT OF THIS ACCOUNT FROM ALL DEVICES** connect 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.
- **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.

如果您落入网络钓鱼诈骗陷阱，该怎么办？



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启用2FA，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。

如果您还能进入自己的账户，

- 在所有连接到账户的电子设备上登出账户。
- 立即更换密码及启用2FA (如有)。

如果您不能进入自己的账户，

- 联系银行或社交媒体等相关平台，告知您遇到的问题，并寻求协助恢复您的账户。
- 如果信用卡/借记卡有任何不实的消费记录，应立即通知银行，并注销您的卡。

- 如果涉及金钱损失，应到最靠近的邻里警局或邻里警岗，或上网 <http://eservices.police.gov.sg> 报案。
- 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。
- 如果账户被盗，冒充者可能会联系您认识的人。您应通知家人和朋友不要理会任何要求，也不要泄露他们的个人资料。

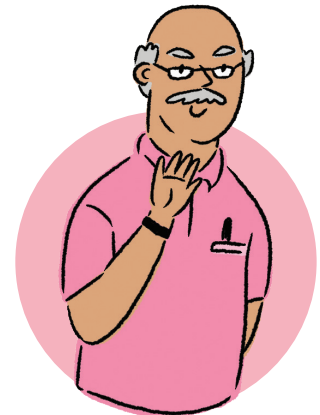
I'M WORRIED I
WILL GET SCAMMED.
MAYBE I SHOULD
NOT RESPOND TO ANY
MESSAGES OR CALLS.



DON'T WORRY.
WE JUST HAVE TO
STAY VIGILANT.
PAUSE TO 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?



我担心自己会被
骗。也许我不应该
回复任何短信或接
听来电。

不要担心。我们只须
保持警惕。停一停，
检查一下，并向家人
或朋友求助。

是的，请牢记不要
向任何人透露个人
密码和OTP，即使是
我也不例外，OK？



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:

