BETTER CYBER SAFE THAN SORRY

A GUIDE TO STAYING SAFE ONLINE

SESAL DAHULU PENDAPATAN, SESAL KEMUDIAN TIDAK BERGUNA

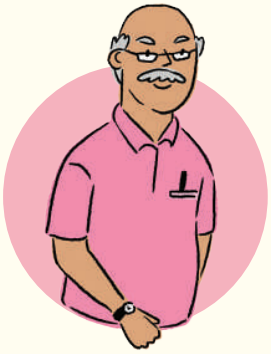
PANDUAN UNTUK KEKAL SELAMAT SECARA DALAM TALIAN

CSA SINGAPORE

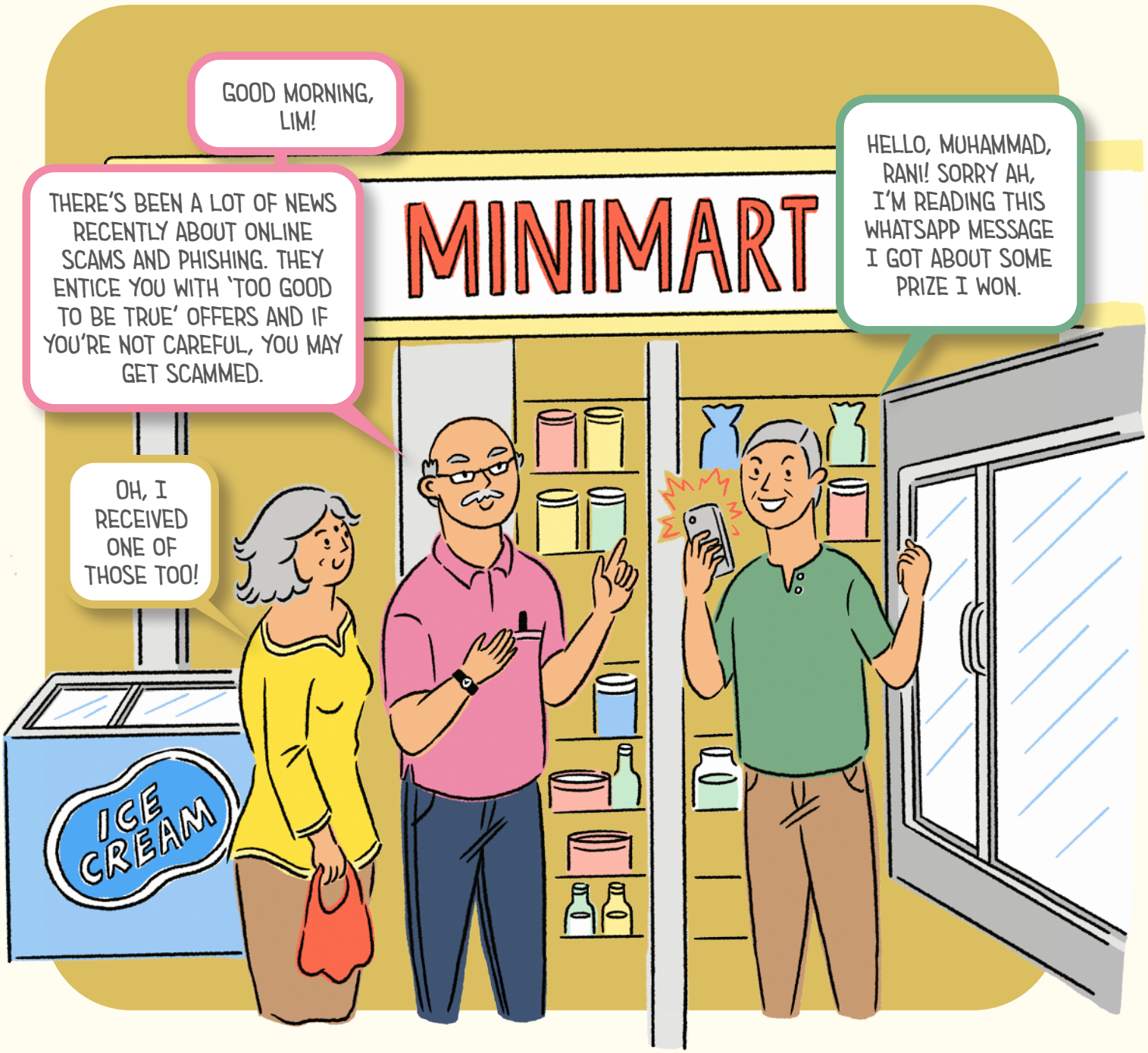
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

LIM
Taxi Driver

RANI
Administrative Assistant



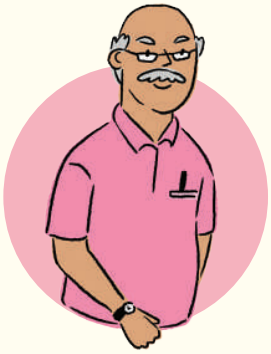
MUHAMMAD
Retired Teacher



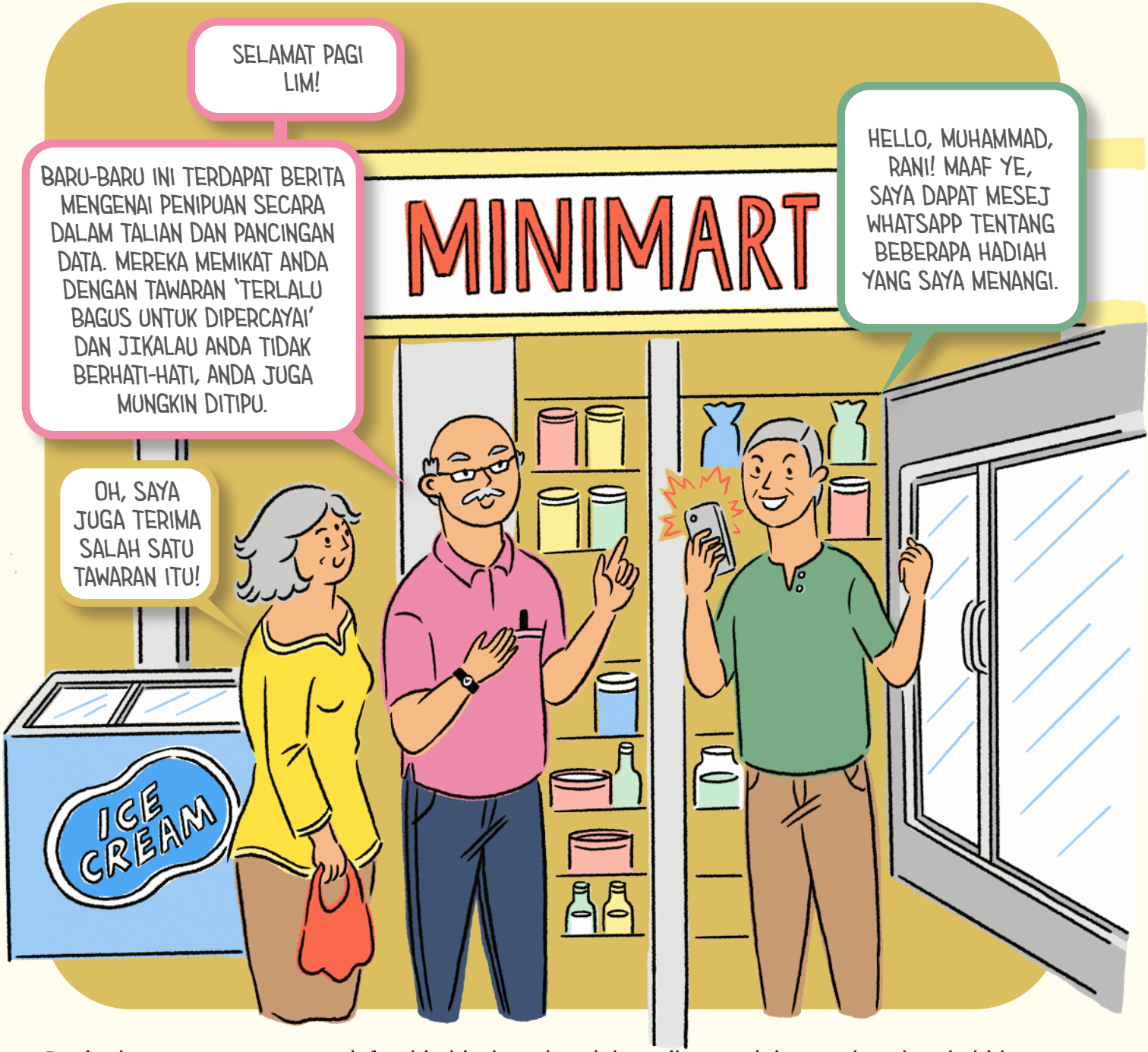
The increased use of smartphones and other smart devices has made life more convenient but at the same time, there are also cybercrimes which we need to be aware of. This handbook will arm you with the information you need to protect yourselves from cyber threats.

LIM
Pemandu Teksi

RANI
Pembantu Pentadbiran



MUHAMMAD
Guru Pencen



Peningkatan penggunaan telefon bimbit dan alat elektronik yang lain membuatkan kehidupan lebih mudah tetapi pada masa yang sama, wujud jenayah siber yang anda perlu berwaspada. Buku panduan ini memberi anda maklumat yang anda perlu untuk melindungi diri anda daripada ancaman siber.

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 2
Subject: [URGENT] CLAIM YOUR GIFT CARD 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 for our monthly lucky draw! 2

www.252749.../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

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)

APAKAH BAHAYA YANG TERDEDAH?

Sedang kita semakin kerap lakukan urusan perbankan atau membeli belah secara dalam talian, kita hadapi risiko ancaman siber dari segi penipuan dalam talian dan pencurian data.

APAKAH PANCINGAN DATA?

Pancingan data adalah satu cara yang digunakan penjenayah siber untuk menipu mangsa agar memberi maklumat peribadi dan maklumat kewangan anda seperti kata laluan, Kata Laluan Sekali (OTP) atau nombor akaun bank.

Penjenayah siber akan menghubungi anda dan menyamar sebagai pertubuhan seperti pemerintah atau bank berkaitan tentang isu yang memerlukan perhatian anda dengan segera. Mereka boleh berbuat demikian melalui panggilan, SMS, aplikasi pemesejan, e-mel atau iklan pop-up.

Cara kesan percubaan pancingan data

[SEGERA] TUNTUT KAD HADIAH ANDA ATAU AKAUN ANDA AKAN DIMATIKAN

Dari: SGSHOPPING <SGSHOPPING@S1231.NET> 1
Tarikh: 11 April 2018, 12.42 pagi
Kepada: John Tan
Subjek: TUNTUT KAD HADIAH ANDA ATAU AKAUN ANDA AKAN DIMATIKAN 2 3

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

Encik John,

Tahniah! Kami berbesar hati memaklumkan bahawa anda memenangi kad hadiah $100 bagi cabutan bulanan bertuah! 2

www.252749.../d43IFk 4

Sila layari www.sgshopping.com atau isi dokumen yang dilampir dengan NRIC, alamat dan perincian akaun bank untuk tuntut kad hadiah anda. Gagal membuat demikian dalam tempoh 24 jam akan menyebabkan akaun anda dimatikan. 6 3

1

E-mel dan mesej yang tidak dijangka melalui WhatsApp, SMS

2

Tawaran ganjaran yang terlalu baik untuk dipercayai

3

Penggunaan bahasa yang mendesak atau mengancam

4

Maklumat yang tidak tepat dan mengelirukan

5

Pautan atau lampiran yang mencurigakan

6

Permintaan bagi maklumat sulit seperti maklumat peribadi atau perbankan, kata laluan atau Kata Laluan Sekali (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:

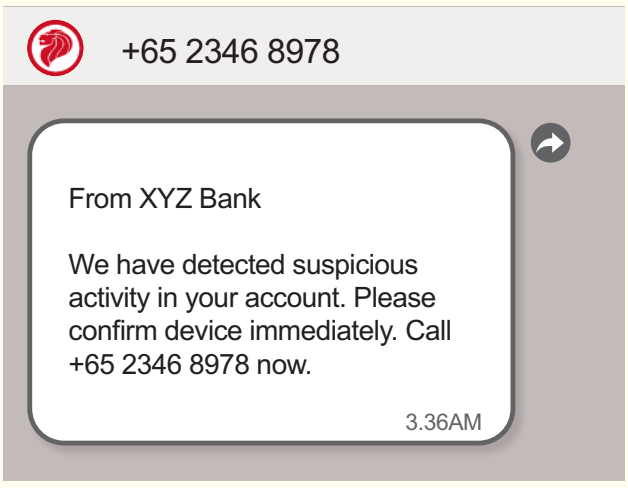
- USE ONLY OFFICIAL E-payment apps (e.g. DBS Paylah!, GrabPay).
- SET UP BANK TRANSACTION ALERTS by setting up email or SMS notifications to help you keep track of transactions.
- CHECK that the QR code for payment is not tampered with.

** 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.



PANCINGAN DATA KOD QR

Penjenayah siber juga boleh menipu anda untuk mengimbas kod QR yang membawa kepada laman web yang meminta maklumat anda. Mereka juga boleh menyembunyikan kod QR dengan perisian hasad* untuk mencuri maklumat daripada alat peranti anda.

- JANGAN KONGSI apa-apa maklumat peribadi atau kewangan, melainkan anda yakin bahawa ia adalah permintaan yang sah.
- JANGAN IMBAS kod QR yang berupa pelekat atau risalah yang diletakkan secara rawak di tempat awam (terutama jika mereka menawarkan baucar atau diskaun), atau kelihatan seperti telah diganggu.

Semasa membuat e-pembayaran dengan kod QR:

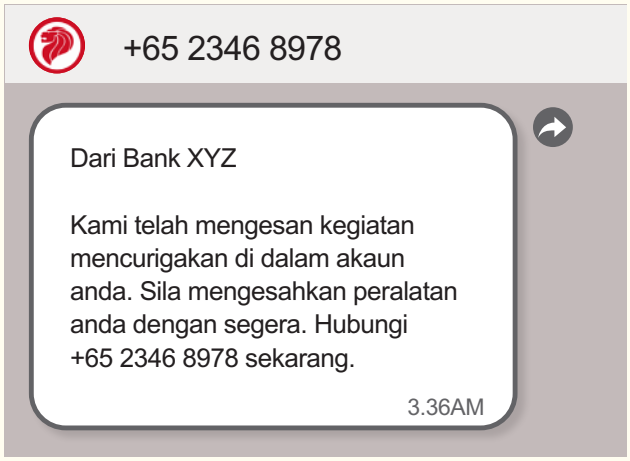
- GUNA HANYA APLIKASI E-pembayaran rasmi (seperti DBS Paylah!, GrabPay).
- SEDIAKAN MAKLUMAN URUS NIAGA BANK dengan menyediakan pemberitahuan e-mel atau SMS untuk membantu anda menjejaki urus niaga.
- PASTIKAN kod QR untuk pembayaran tidak diganggu.

** Perisian hasad ialah sejenis perisian yang menjangkiti alat peranti anda dan menyebabkan kerosakan, termasuk mencuri maklumat anda, merosakkan dan juga memadam data anda.*

CARA MENGESAN PENIPUAN PANCINGAN DATA/DALAM TALIAN

PENIPUAN PENYAMARAN

- Dalam PENIPUAN SOKONGAN TEKNIKAL, penipu boleh menyamar sebagai pegawai daripada CSA, Polis atau syarikat telekomunikasi yang menyiasat kegiatan yang mencurigakan dalam rangkaian anda.
- Dalam PENIPUAN PANCINGAN DATA BANK, penipu menyamar sebagai pekerja bank yang meminta anda mengikuti arahan secepat mungkin untuk menangani beberapa akaun bank atau isu teknikal atau memberikan butiran peribadi untuk tawaran yang tidak wujud.
- Dalam PENIPUAN PENYAMARAN MEDIA SOSIAL, penipu mungkin menyamar sebagai rakan, keluarga atau rakan sekerja anda dan menghubungi anda di media sosial, meminta maklumat peribadi anda atau OTP yang anda menerima 'secara tidak sengaja'.
- Dalam PENIPUAN PENGAMBILALIHAN AKAUN WHATSAPP, penipu mungkin menyamar sebagai kenalan anda dan meminta kod pengesahan enam digit dihantar kepada mereka.

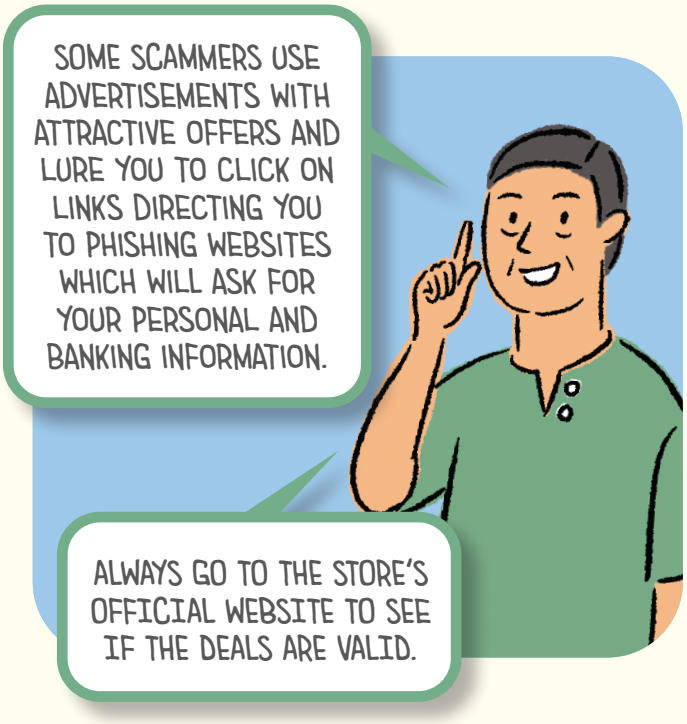


E-COMMERCE SCAM

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.

PENIPUAN E-DAGANG

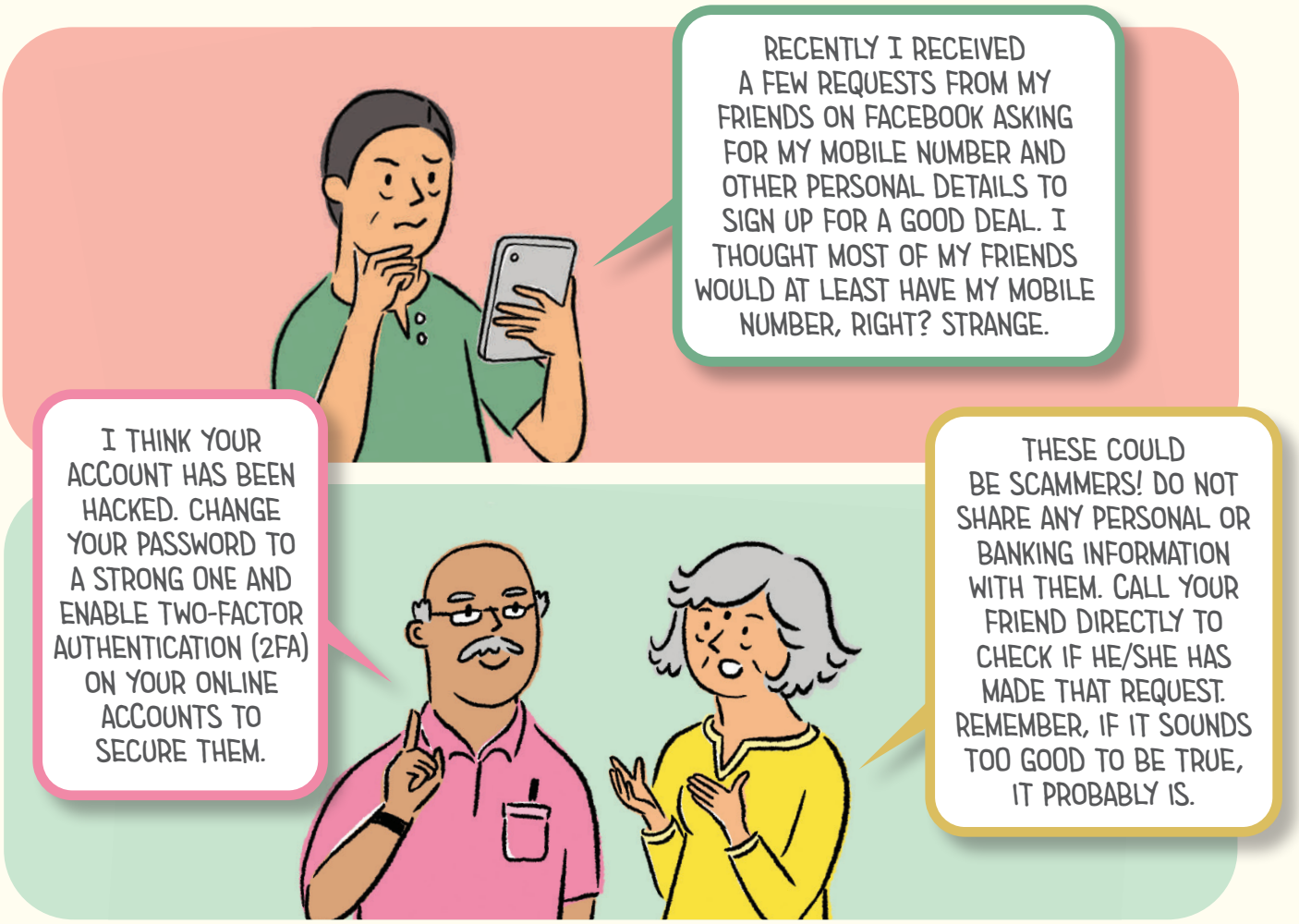
Gunakan potongan dan tawaran yang besar, penipu ini akan menuntut pembayaran segera atau pindahan bank sebelum penghantaran. Setelah mereka terima wang, mereka tidak boleh dihubungi.

Apa yang anda boleh lakukan?

- BELI HANYA DARI LAMAN WEB BEREPUTASI BAIK.
- BAYAR MELALUI PLATFORM BELI BELAH. Dengan cara ini, penjual hanya terima pembayaran setelah anda terima barangan anda.
- Sentiasa BERWASPADA, dan fikirkan semula pembelian anda jika tawaran terlalu bagus untuk dipercayai.

Jika anda atau seseorang yang anda kenali telah menerima mesej pancingan data...

- JANGAN PANIK. Hubungi ahli keluarga atau rakan anda, atau hubungi talian bantuan AntiScam di 1800-722-6688 untuk mendapatkan nasihat.
- JANGAN JAWAB panggilan yang menunjukkan tanda '+' jika anda tidak menjangkakan panggilan luar negara.
- JANGAN PASANG sebarang perisian jika anda 'dinasihatkan' untuk berbuat demikian.
- JANGAN KONGSI KATA LALUAN, OTP atau maklumat peribadi dan perbankan.
- JANGAN HANTAR WANG kepada sesiapa pun.
- JANGAN KLIK pada mana-mana lampiran atau pautan dalam mesej. Padamkannya.
- LAKSANAKAN PENGESAHAN DUA LANGKAH DALAM WHATSAPP sebagai lapisan keselamatan tambahan.
- MENGESAHKAN PANGGILAN ATAU MESEJ YANG MENCURIGAKAN dengan menghubungi talian rasmi pemerintah/perniagaan atau aplikasi/laman web rasmi secara terus. Jangan hubungi pertubuhan melalui butiran hubungan yang disediakan dalam panggilan atau mesej.
- AMBIL PERHATIAN bahawa pegawai pemerintah tidak akan menuntut pembayaran segera dalam talian atau menyuruh anda pindah wang ke mana-mana akaun bank tempatan atau asing, atau tidak membenarkan anda menggantung panggilan.
- RUJUK senarai laman web berkaitan pemerintah yang dipercayai di laman **www.gov.sg/trusted-sites** sekiranya alamat e-mel tidak mempunyai "**.gov.sg**" di dalamnya.



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.

Sekiranya anda memberikan butiran peribadi dan/atau perbankan anda secara tidak sengaja, lakukan langkah-langkah ini dengan segera:

- **TUKAR KATA LALUAN** untuk akaun anda (Singpass atau bank) dengan segera, termasuk semua akaun lain yang menggunakan kata laluan yang sama.
- **BERITAHU BANK ANDA** jika anda telah mendedahkan butiran kad kredit.
- **PANTAU AKAUN ANDA** untuk pengeluaran atau pembelian yang tidak dibenarkan.
- **BUAT LAPORAN POLIS** jika ada duit hilang.
- **GUNAKAN PERISIAN ANTI-VIRUS** untuk mengimbas sistem anda bagi sebarang perisian hasad. Perisian hasad menjangkiti peranti anda dan menyebabkan kerosakan, termasuk mencuri, merosakkan dan juga memadamkan data anda.
- **PERGI KE LAMAN WEB SingCERT CSA** **www.csa.gov.sg/singcert/reporting** jika anda ingin membuat laporan.

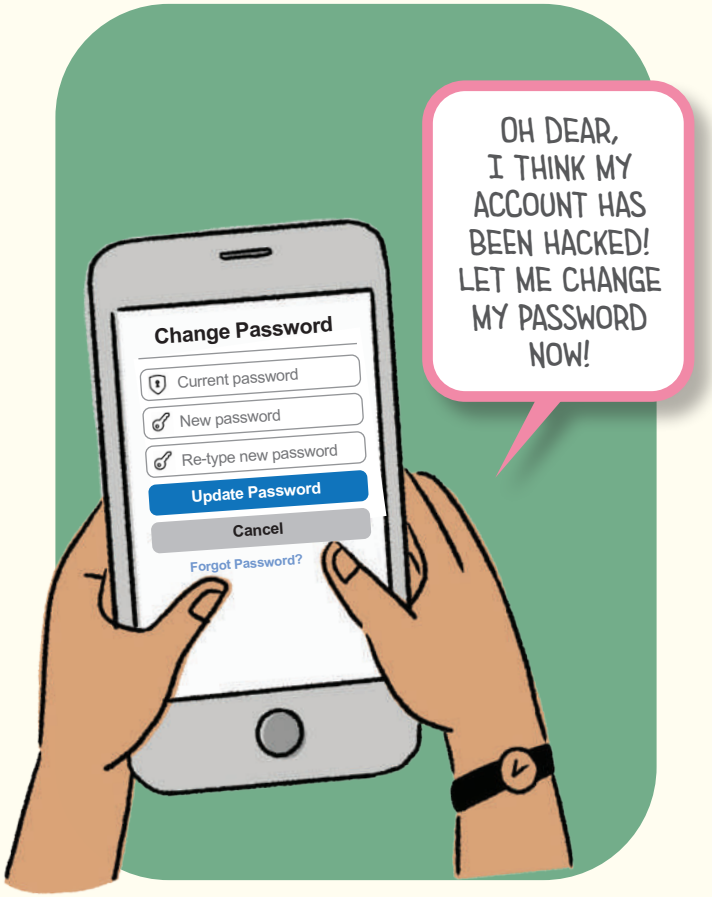
KEEP TABS ON YOUR ONLINE ACCOUNT

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!

BERWASPADA DENGAN AKAUN DALAM TALIAN ANDA

Bagaimana anda boleh lindungi akaun dalam talian?

- BUAT KATA LALUAN yang unik untuk anda. Panjangnya sekurang-kurangnya 12 aksara. Gunakan perkataan yang berkaitan dengan kenangan yang unik untuk anda, misalnya IhadKAYAtoastAT8AM!

- GUNA huruf besar dan huruf kecil, angka dan simbol.

- GUNA PENGESAHAN DUA FAKTOR (2FA) jika boleh. Selain perbankan internet, 2FA boleh diguna bagi media sosial, e-mel, beli belah, dan akaun pemerintah.

Apakah yang perlu anda lakukan sekiranya anda fikir anda digodam?

Sekiranya anda mempunyai akses akaun,

- LOG KELUAR DARIPADA SEMUA PERANTI yang dihubungkan ke akaun ini.

- TUKAR KATA LALUAN ANDA DENGAN SEGERA dan aktifkan 2FA jika ada.

Sekiranya anda tidak mempunyai akses akaun,

- HUBUNGI PLATFORM misalnya bank atau platform media sosial, untuk melaporkan masalah tersebut dan meminta bantuan untuk mendapat balik akaun anda.

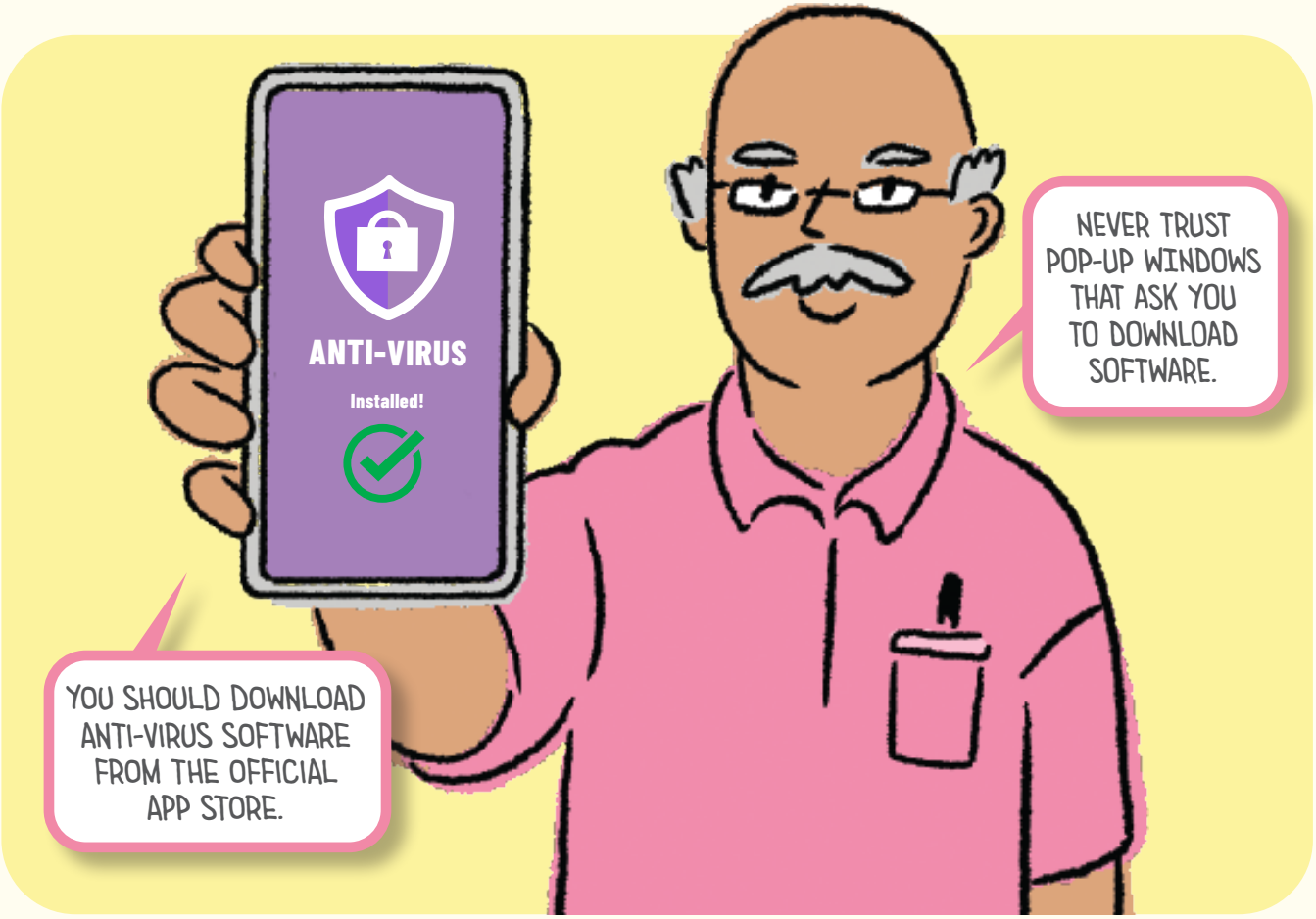
- BUAT LAPORAN mengenai sebarang caj kad kredit/debit palsu ke bank anda dan batalkan kad anda dengan segera.

- BUAT LAPORAN POLIS di Pusat Polis Kejiranan atau Pos Polis Kejiranan terdekat atau dalam talian di **https://eservices.police.gov.sg** sekiranya berlaku kerugian.

- Sekiranya akaun anda terjejas, penyamar boleh menghubungi kenalan anda. BERI AMARAN KEPADA KELUARGA DAN RAKAN ANDA untuk mengabaikan sebarang permintaan dan tidak berkongsi maklumat peribadi mereka.

KEGIATAN

Ingin tahu sekiranya kata laluan anda kuat? Sila guna Password Checker untuk mengetahui lebih lanjut!



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.

PERISIAN HASAD (MALWARE): APA IA SEBENARNYA?

Perisian hasad ialah sejenis perisian yang menjangkiti peranti anda dan menyebabkan kerosakan, termasuk mencuri maklumat anda, merosakkan dan juga memadam data anda.

Bagaimana boleh anda lindungi peranti anda dari perisian hasad?

- SILA MUAT TURUN APLIKASI ANTI-VIRUS daripada kedai aplikasi rasmi untuk lindungi peranti anda.
- SILA KEMAS PERISIAN ANDA secara berkala dan pastikan keselamatan peranti anda selamat. Kemas kini ini akan perbaiki kelemahan pada peranti anda.
- SILA AKTIFKAN KEMAS KINI AUTOMATIK melalui Wi-Fi, atau susun jadual kemas kini untuk dipasang semalaman semasa peranti anda mengecas.

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?

DENGAN TELEFON PINTAR DAN PERANTI, HIDUP MENJADI LEBIH MUDAH, TETAPI JUGA LEBIH MEMBIMBANGKAN.

JANGAN BIMBANG. KITA HANYA PERLU BERJAGA-JAGA, DAN LEBIH BERWASPADA DENGAN PERANTI DAN AKAUN DALAM TALIAN KITA.

YA, DAN INGAT, JANGAN KONGSI KATA LALUAN ATAU OTP ANDA DENGAN SESIAPAPUN. JANGAN KONGSI DENGAN SAYA, OKAY?

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.

Untuk maklumat lanjut, layari lelaman SG Cyber Safe Seniors CSA atau lelaman Scam Alert Majlis Pencegahan Jenayah Kebangsaan.

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

Get more cyber tips at:

Dapatkan lebih banyak nasihat siber di:

For the latest scam info, visit:

Bagi maklumat penipuan terbaru, lawati: