BETTER CYBER SAFE THAN SORRY

A GUIDE TO STAYING SAFE ONLINE

LEBIH SELAMAT SIBER DARIPADA MENYESAL

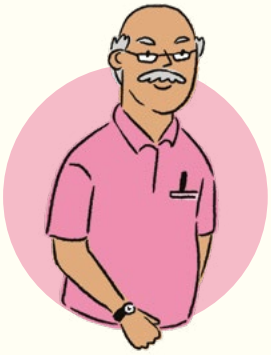
PANDUAN UNTUK KEKAL SELAMAT SECARA DALAM TALIAN

CSA SINGAPORE

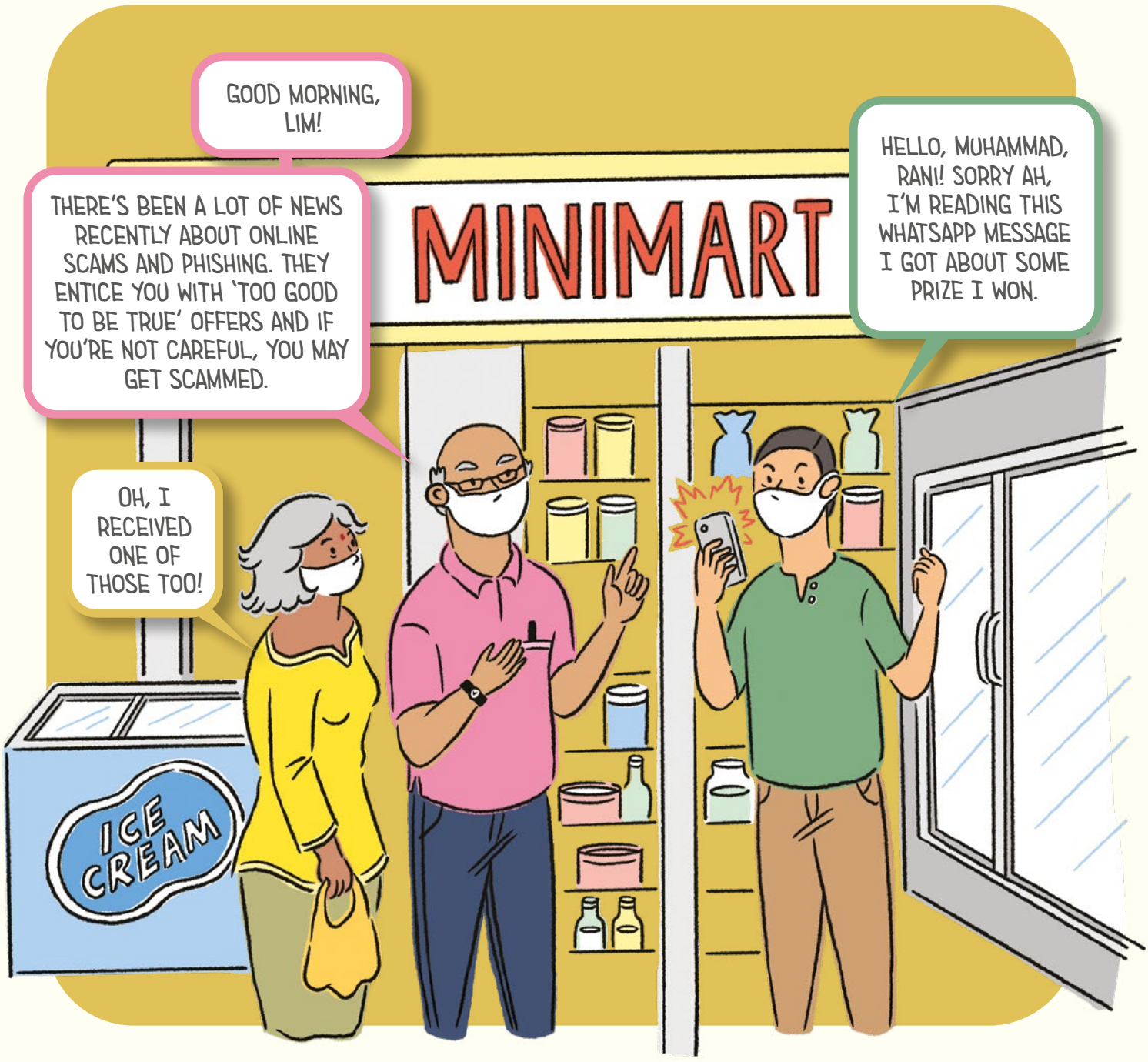
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

LIM
Taxi Driver

RANI
Administrative Assistant



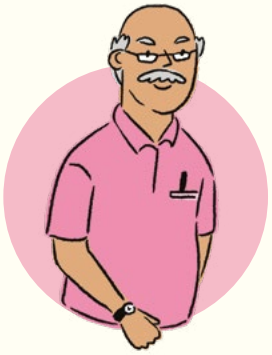
MUHAMMAD
Retired Teacher



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.

LIM
Drebar Teksi

RANI
Pembantu Pentadbiran



MUHAMMAD
Guru Pesara

Adakah ini biasa anda dengar? Peningkatan penggunaan telefon pintar dan alat elektronik menyebabkan peningkatan yang sama bagi jenayah siber. Jadi apakah tanda-tanda dan bagaimana dapat kita lindungi diri kita sendiri? Buku panduan ini akan memberi anda maklumat yang anda perlukan untuk mengharungi dunia baru ini.

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,

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 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

APAKAH ANCAMAN SIBER?

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

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 2
Subjek: TUNTUT KAD HADIAH ANDA ATAU AKAUN ANDA AKAN DIMATIKAN 3

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

Encik John,

Tahniah! Kami berbesar hati memaklumkan bahawa anda memenangi kad hadiah $100 5 bagi cabutan bulanan bertuah!

www.252749.co/d43lFk 1

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

1

Maklumat Tidak Tepat & Mengelirukan

2

E-mel yang tidak dijangka

3

Bahasa yang mendesak atau mengancam

4

Lampiran mencurigakan

5

Janji Hadiah Menarik

6

Permintaan bagi Maklumat Rahsia

HOW TO SPOT PHISHING/ONLINE SCAMS

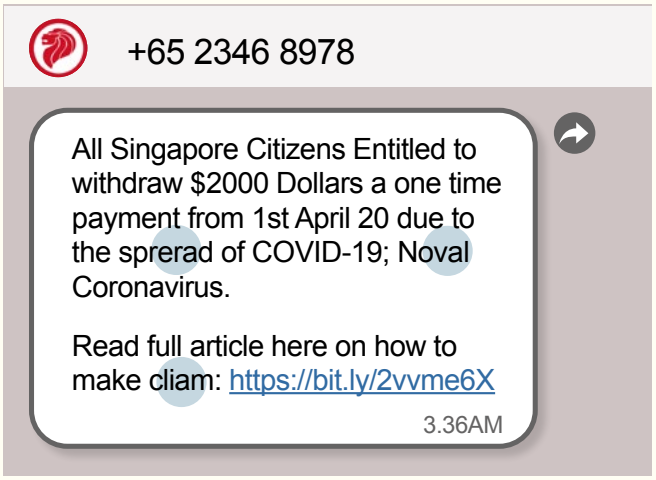
IMPERSONATION SCAMS

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

CARA MENGESAN PENIPUAN PANCINGAN DATA/DALAM TALIAN

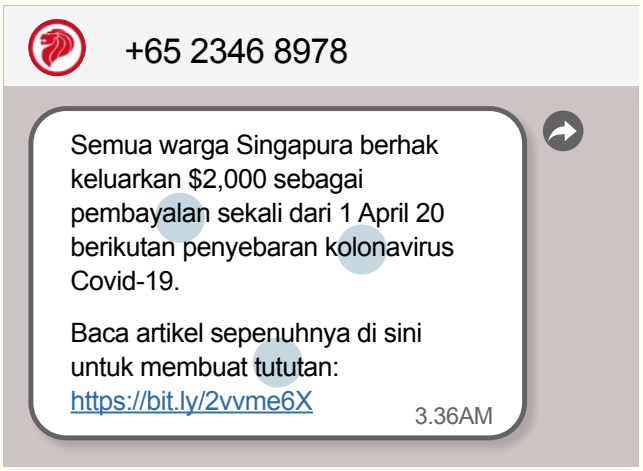
PENIPUAN PENYAMARAN

Penjenayah ini boleh memanggil, SMS atau WhatsApp anda, berpura-pura daripada pertubuhan dikenali seperti agensi pemerintah atau bank. Mereka mungkin meminta anda mematuhi arahan mendesak untuk menangani beberapa akaun bank atau masalah teknikal palsu atau menyediakan butir-butir peribadi bagi tawaran yang tidak wujud.

- PERHATIAN bahawa pegawai pemerintah tidak akan meminta anda memindahkan wang secara dalam talian melalui telefon

- HARUS BERWASPADA jika mesej itu penuh dengan kesalahan ejaan dan kesalahan lain

- SILA RUJUK kepada senarai lelaman pemerintah yang dipercayai di **www.gov.sg/trusted-sites** sekiranya pautan atau alamat e-mel tidak mempunyai "**gov.sg**" di dalamnya



PENIPUAN SOKONGAN TEKNOLOGI

Penipu ini mengaku sebagai pegawai CSA atau syarikat telko menyiasat kegiatan mencurigakan di rangkaian anda.

- JANGAN MUAT NAIK sebarang aplikasi perisian yang 'dinasihatkan' kepada anda

- JANGAN DEDAHKAN sebarang maklumat peribadi atau kewangan

PANCING DATA BERKAITAN PERBANKAN

- JANGAN KONGSI KATA LALUAN atau kata laluan guna sekali (OTP) atau maklumat kewangan anda dengan sesiapa

- JANGAN HANTAR WANG kepada seseorang yang baru anda temui dalam talian

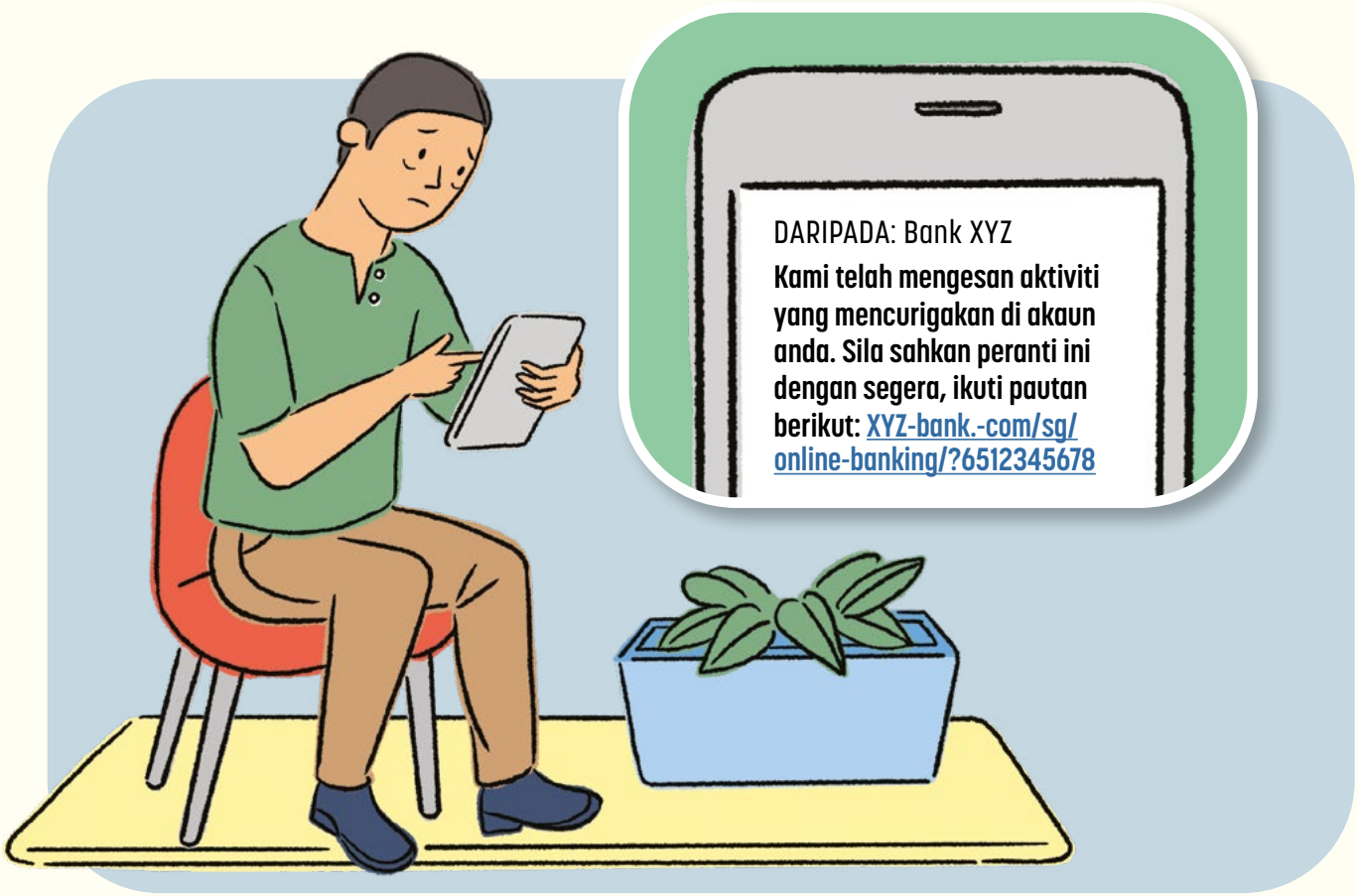
- BERWASPADA menerima panggilan yang menunjukkan tanda '+' jika anda tidak menjangkakan sebarang panggilan. Panggilan tempatan tidak akan memaparkan tanda '+'

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

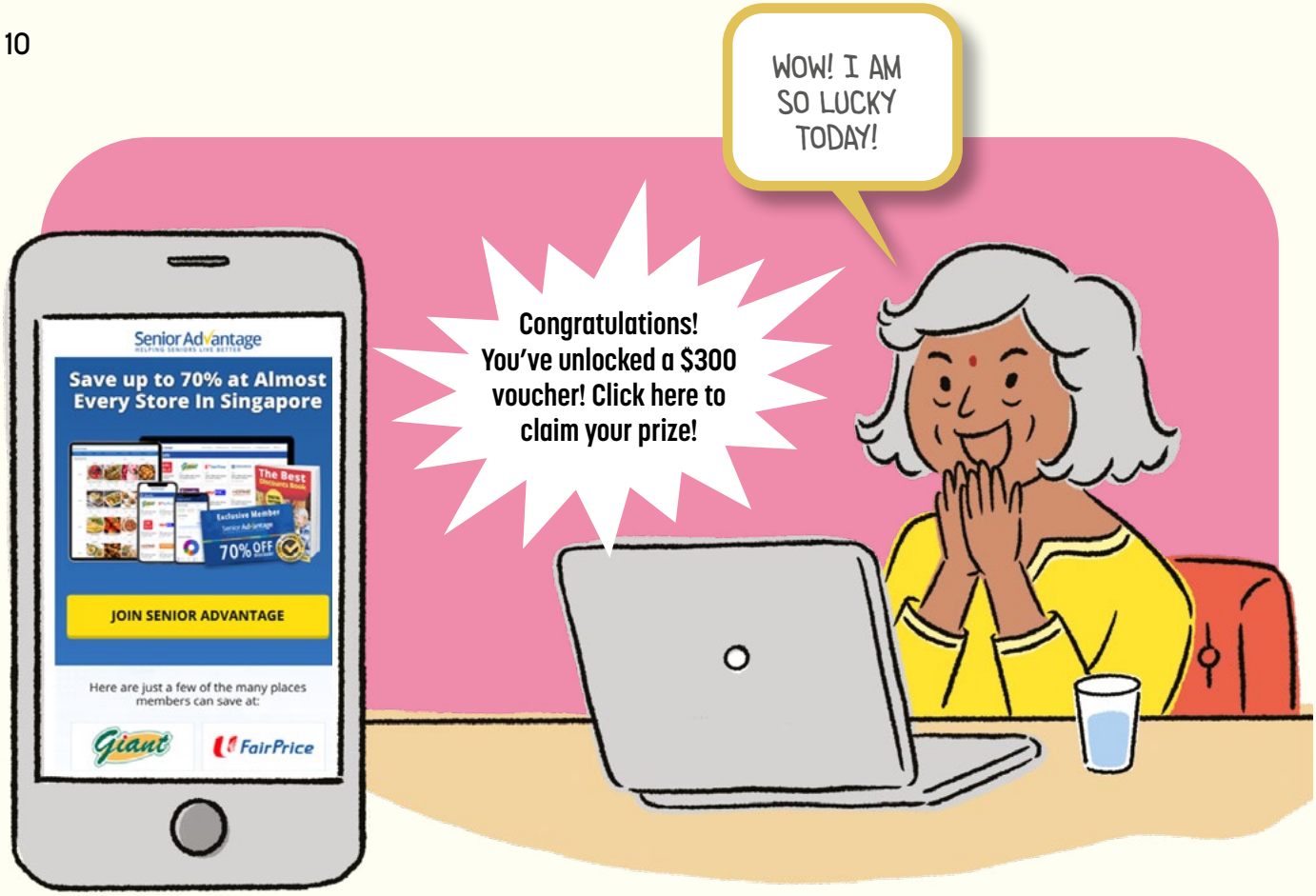


Jika anda atau seseorang yang anda kenali telah menerima mesej, panggilan atau e-mel pancingan data,

- SILA ABAIKAN dan buangnya
- JANGAN KLIK lampiran atau pautan dalam mesej

Sekiranya anda terima iklan atau mesej yang tidak diminta mengarahkan anda ikut beberapa arahan dengan segera, jangan panik. Hubungi anggota keluarga atau rakan untuk nasihat. Untuk dapatkan nasihat berkaitan penipuan, layari **www.scamalert.sg** atau hubungi talian hotline anti-penipuan di **1800-722-6688**. Sekiranya anda tidak sengaja mengkliknya, inilah yang harus anda lakukan dengan segera:

- UBAH KATA LALUAN dengan segera, termasuk semua akaun lain yang menggunakan kata laluan ini
- SEGERA HUBUNGI BANK anda jika anda dedahkan butiran kad kredit
- PANTAU AKAUN ANDA bagi pengeluaran atau pembelian tanpa izin
- BUAT LAPORAN POLIS jika ada dana yang hilang
- GUNAKAN PERISIAN ANTI-VIRUS untuk mengimbas sistem anda
- PERGI KE LELAMAN SingCERT CSA **www.csa.gov.sg/singcert/reporting** jika anda ingin buat laporan



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

PENIPUAN SECARA DALAM TALIAN

PENIPUAN E-DAGANG

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

Apa yang boleh anda lakukan?

- BUAT PEMBELIAN hanya dari laman web bereputasi baik
- SILA BAYAR melalui platform beli-belah. Dengan cara ini, penjual hanya terima pembayaran hanya setelah anda terima barangan anda
- SENTIASA BERWASPADA, dan fikirkan semula pembelian anda jika tawaran terlalu bagus untuk dipercayai

PENIPUAN PENYAMARAN MEDIA SOSIAL

Penipu juga boleh berpura-pura menjadi rakan, keluarga atau rakan sekerja anda dan menghubungi anda di media sosial, meminta maklumat peribadi atau kod OTP yang dihantar kepada anda 'secara tidak sengaja'.

Apa yang boleh kita lakukan?

- JANGAN KONGSI maklumat peribadi atau perbankan atau OTP anda dengan sesiapa, termasuk keluarga atau rakan rapat
- SENTIASA BERWASPADA dengan permintaan atau tawaran dari sesiapa sahaja, termasuk keluarga atau rakan rapat

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!

WASPADA DENGAN AKAUN DALAM TALIAN ANDA

Bagaimana anda boleh lindungi akaun dalam talian?

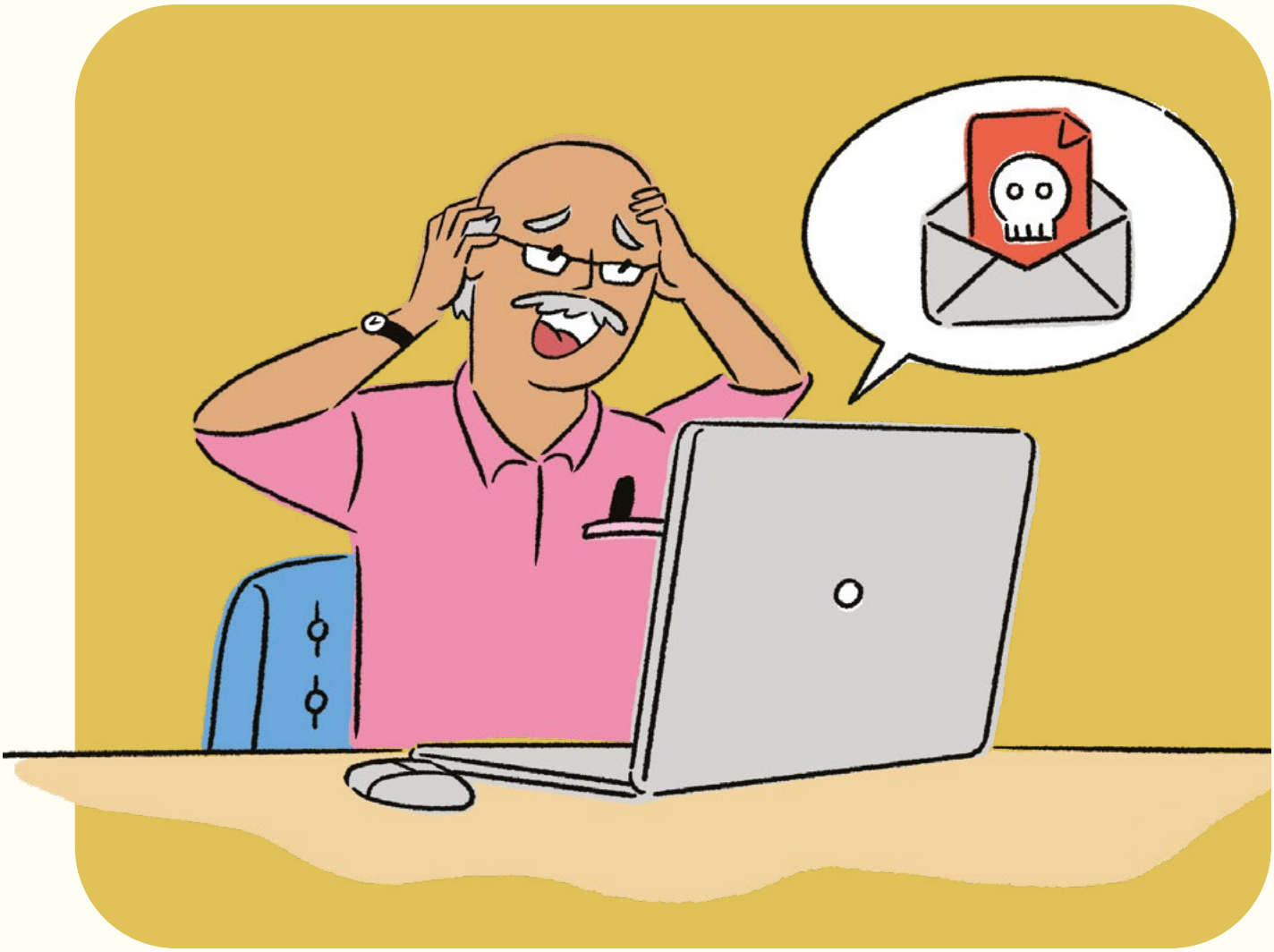
- SILA BUAT KATA LALUAN yang unik untuk anda. Panjangnya sekurang-kurangnya 12 aksara, atau gunakan lima perkataan berbeza yang berkaitan secara peribadi dengan anda, misalnya IhadKAYAtoastAT8AM!
- SILA GUNAKAN huruf besar, huruf kecil dan angka dan simbol
- GUNA PENGESAHAN DUA FAKTOR (2FA) jika boleh. 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, SILA LOG KELUAR DARIPADA SEMUA PERANTI yang dihubungkan ke akaun ini
- TUKAR KATA LALUAN ANDA DENGAN SEGERA dan aktifkan 2FA jika ada
- Tiada akses ke akaun anda? SILA HUBUNGI WADAH misalnya bank atau wadah media sosial, untuk melaporkan masalah tersebut dan meminta bantuan untuk mendapatkan semula akaun anda
- BUAT LAPORAN mengenai sebarang caj kad kredit / debit palsu ke bank anda dan batalkan kad anda dengan segera. Sekiranya berlaku kerugian, buat laporan polis di Pusat Polis Kejiranan atau Pos Polis Kejiranan terdekat atau dalam talian di **https://eservices.police.gov.sg**
- Sekiranya akaun anda dicerobohi, penyamar akan dapat menghubungi kontak anda. BERI AMARAN KEPADA KELUARGA DAN RAKAN-RAKAN untuk mengabaikan sebarang permintaan dan tidak kongsi maklumat peribadi mereka

KEGIATAN

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

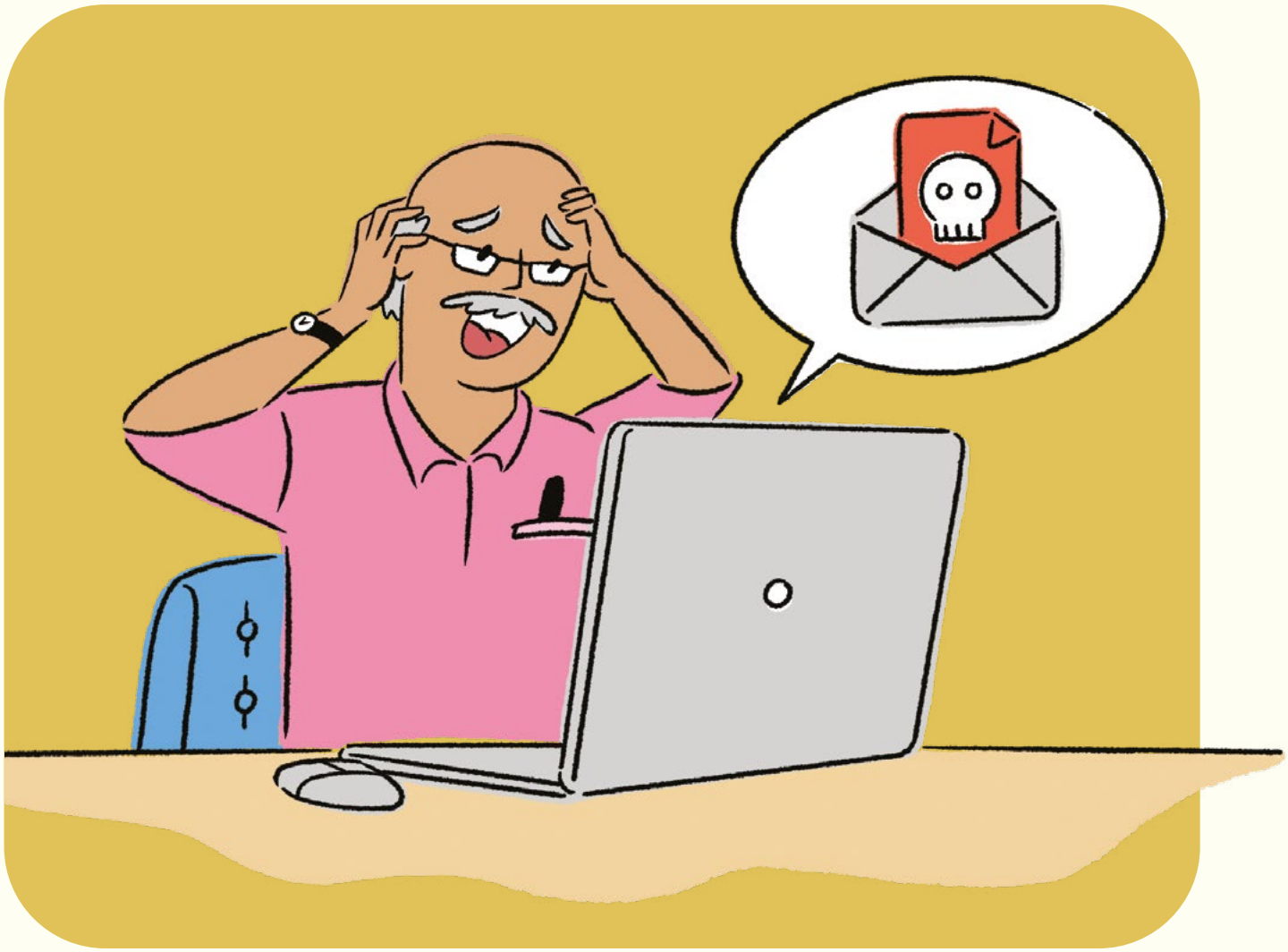


MALWARE. WHAT EXACTLY IS IT?

Malware is a type of software that infects your 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



PERISIAN HASAD (MALWARE): APA IA SEBENARNYA?

Perisian hasad atau malware adalah virus yang menjangkiti komputer dan peranti mudah alih. Mereka boleh lakukan banyak kerosakan, merosakkan data sehingga ia dapat dicuri atau bahkan dihapuskan.

Bagaimana dapat anda lindungi peranti anda dari perisian hasad?

- SILA MUAT TURUN APLIKASI ANTI-VIRUS daripada kedai aplikasi rasmi untuk lindungi peranti anda
- SILA KEMAS KINI 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 dipasang

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?

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

JANGAN TAKUT. KITA HANYA PERLU BERJAGA-JAGA, DAN LEBIH WASPADA 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, 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

Untuk maklumat lanjut, daftar ke Webinar Ask the Cyber Experts Series (Siri Tanya Pakar Siber) atau layari lelaman Siber CSA Warga Emas Lebih Selamat 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: