BE CYBER SAFE

A GUIDE TO STAYING SAFE ONLINE

KEKAL SELAMAT SIBER

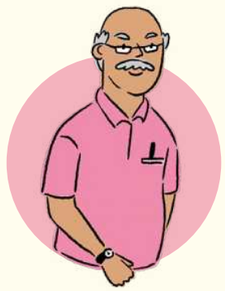
PANDUAN UNTUK KEKAL SELAMAT SECARA DALAM TALIAN

CSA SINGAPORE
Cyber Security Agency of Singapore

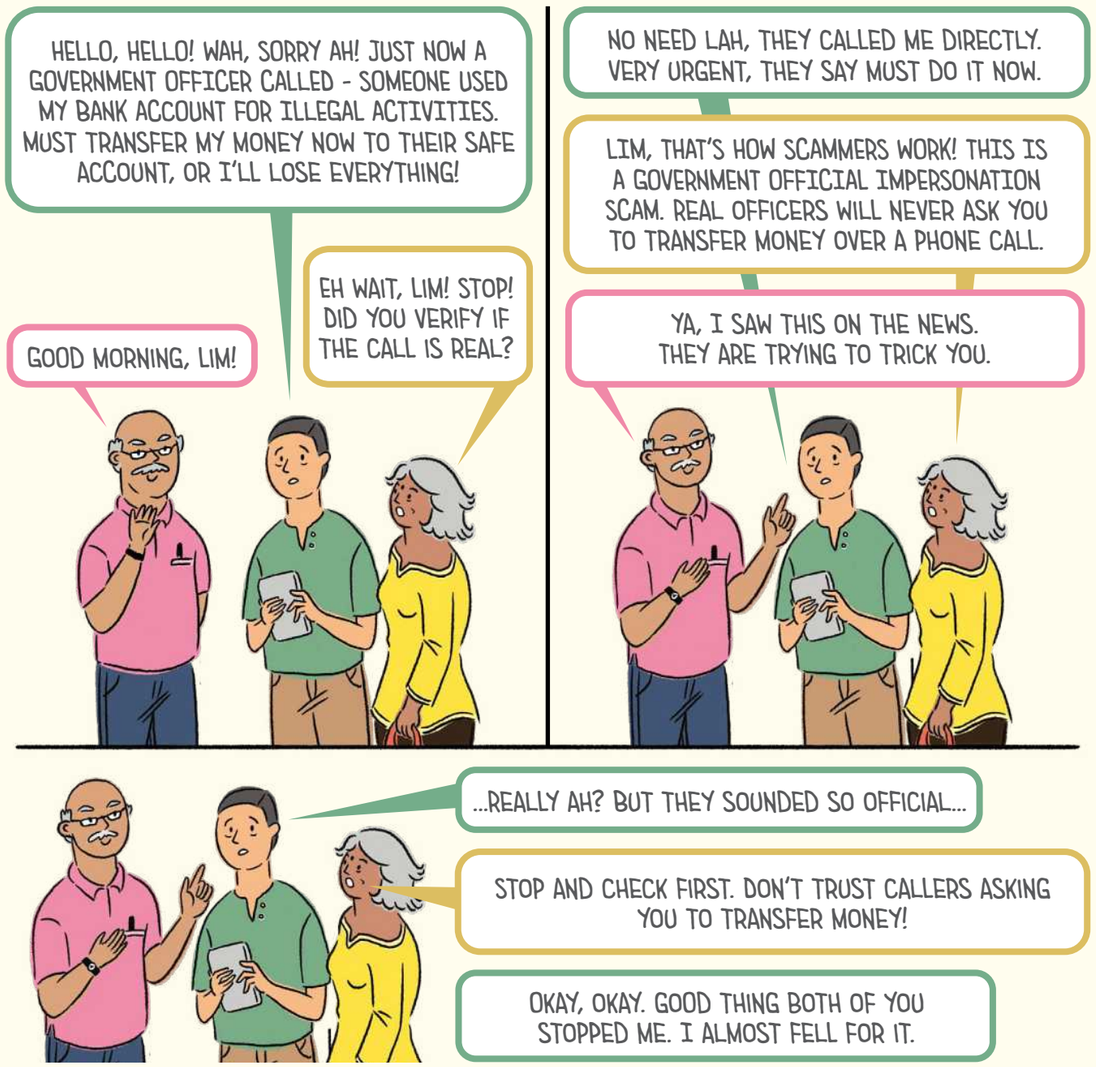
SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY

LIM
Taxi Driver

RANI
Administrative Assistant



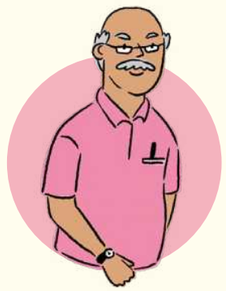
MUHAMMAD
Retired Teacher



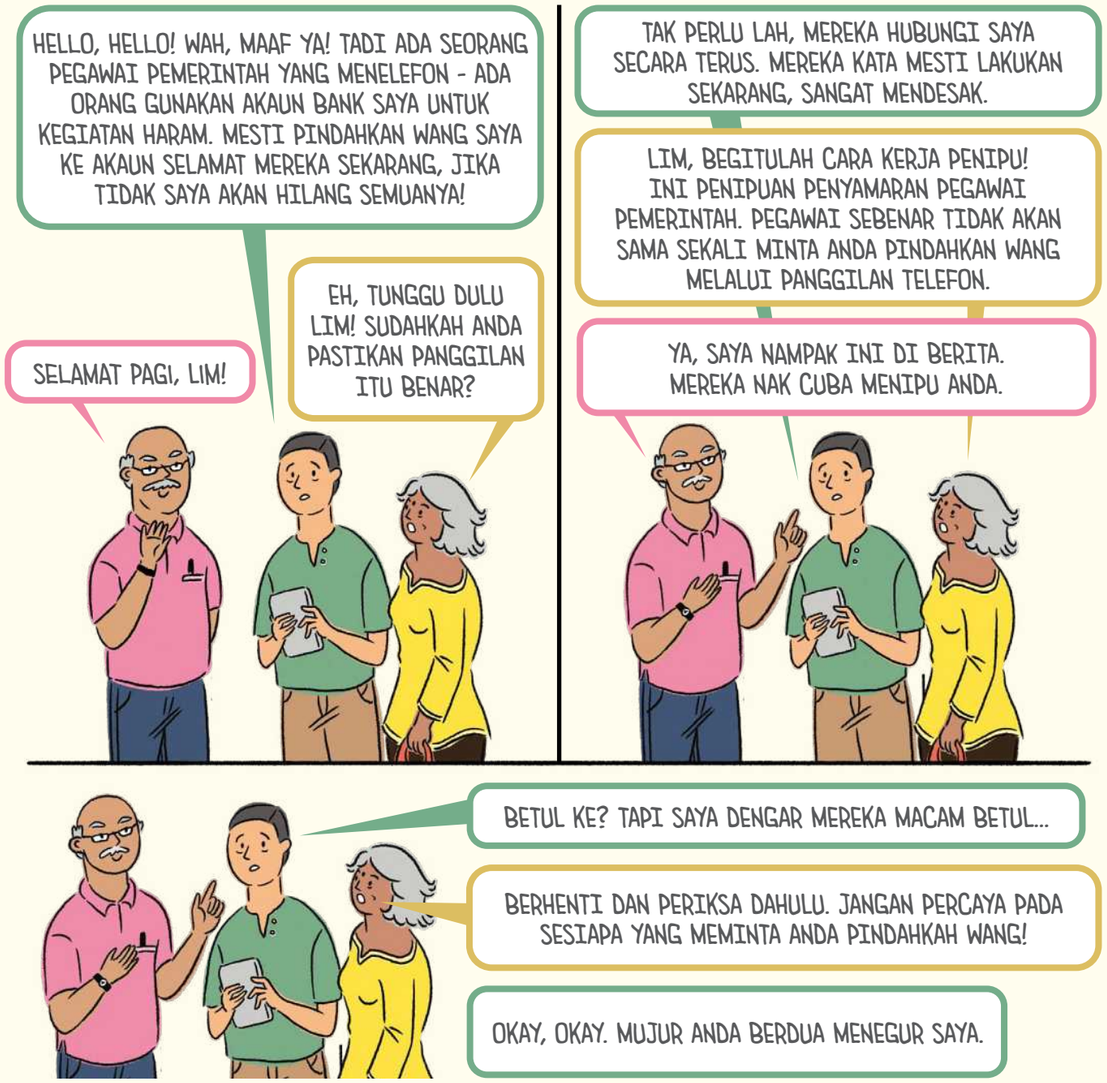
Smartphones and smart devices have made life more convenient. However, this has also created more opportunities for cybercriminals to carry out cybercrimes. This handbook will arm you with the information you need to protect yourself and your loved ones online.

LIM
Pemandu Teksi

RANI
Pembantu Pentadbiran



MUHAMMAD
Guru Bersara



Telefon bimbit dan alat elektronik lain memudahkan kehidupan. Namun, pada masa yang sama, ia membuka lebih banyak peluang kepada penjenayah siber untuk melakukan jenayah siber. Buku panduan ini memberikan maklumat yang anda perlukan untuk melindungi diri sendiri dan orang yang disayangi 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 cybercriminals to trick you into giving out personal and financial information such as passwords, One-Time Passwords (OTPs) or bank account numbers.

Cybercriminals may pretend to be from the government, banks or businesses, claiming that there are urgent issues requiring your immediate attention. They may contact you through social media, messaging platforms, and phone calls to trick you into revealing personal and banking information that can be used to make unauthorised transactions.

STOP AND CHECK!

Cybercriminals often use fear and urgency to pressure you into making hasty decisions.

By taking a moment to stop and check with official sources, family and friends, you can better protect yourself from falling prey to cybercriminals out to steal your hard-earned money and data.

APAKAH BAHAYA YANG KITA HADAPI?

Sedang kita semakin kerap melakukan urusan perbankan atau membeli-belah secara dalam talian dengan mudah, kita berdepan dengan risiko ancaman siber berupa penipuan dalam talian dan pencurian data.

APAKAH PANCINGAN DATA?

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

Penjenayah siber mungkin menyamar sebagai pegawai pemerintah, bank atau perniagaan dengan mendakwa ada isu penting yang memerlukan perhatian anda. Mereka mungkin menghubungi anda melalui media sosial, aplikasi pemesejan, dan panggilan telefon untuk menipu anda supaya mendedahkan maklumat peribadi dan perbankan yang boleh digunakan untuk membuat transaksi tanpa kebenaran.

BERHENTI DAN PERIKSA!

Penjenayah siber sering menggunakan rasa takut dan keadaan mendesak untuk memaksa anda membuat keputusan secara terburu-buru.

Bila anda berhenti seketika untuk memeriksa dengan sumber rasmi, anda boleh melindungi diri anda daripada menjadi mangsa penjenayah siber yang ingin mencuri data dan wang titik peluh anda.

COMMON TYPES OF ONLINE SCAMS

GOVERNMENT OFFICIALS IMPERSONATION SCAMS

Cybercriminals typically pose as government officers and trick you into revealing personal information, banking details and/or transferring money to bank accounts they provide.

What to look out for:

Government officials will **never** ask you to do the following over a phone call:

- Transfer money
- Disclose banking details
- Install mobile apps from unofficial app stores
- Transfer your call directly to the police

IMPERSONATION OF BANK REPRESENTATIVES

CYBERCRIMINALS MAY ALSO PRETEND TO BE BANK EMPLOYEES, CLAIMING THERE ARE ISSUES WITH YOUR ACCOUNT.
DO NOT PANIC. CALL YOUR BANK'S OFFICIAL HOTLINE TO VERIFY THE ISSUE. REMEMBER, BANKS WILL NEVER SEND CLICKABLE LINKS VIA SMS OR TRANSFER YOUR CALL TO THE POLICE.

JENIS PENIPUAN DALAM TALIAN YANG BIASA BERLAKU

PENIPUAN PENYAMARAN PEGAWAI PEMERINTAH

Penjenayah siber biasanya menyamar sebagai pegawai pemerintah dan memperdaya anda supaya mendedahkan maklumat peribadi, butiran perbankan dan/atau memindahkan wang ke akaun bank yang mereka sediakan.

Apa yang perlu diperhatikan:

Pegawai pemerintah **tidak akan sama sekali** minta anda melakukan perkara berikut melalui panggilan telefon:

- Pindahkan wang
- Dedahkan butiran perbankan
- Muat turun aplikasi mudah alih daripada gedung aplikasi tidak rasmi
- Pindahkan panggilan anda terus kepada pihak polis

PENYAMARAN WAKIL BANK

PENJENAYAH SIBER JUGA MUNGKIN MENYAMAR SEBAGAI PEKERJA BANK, MENDAKWA ADA MASALAH DENGAN AKAUN ANDA. JANGAN PANIK. HUBUNGI TALIAN HOTLINE RASMI BANK ANDA UNTUK MENGESAHKAN MASALAH TERSEBUT. INGAT, BANK TIDAK AKAN SAMA SEKALI MENGHANTAR PAUTAN YANG BOLEH DIKLIK MELALUI SMS ATAU MEMINDAHKAN PANGGILAN ANDA KEPADA POLIS.

INVESTMENT SCAMS

Cybercriminals use social media and messaging platforms to carry out investment scams. They advertise fake investments promising high returns, or adding you to chat groups where accomplices share fake success stories or payment screenshots to make the scam appear genuine. Some may befriend you first to build trust before tricking you into transferring money.

JOB SCAMS

Cybercriminals may promise you commission for carrying out simple tasks such as reviewing hotels or completing surveys via WhatsApp or Telegram chat groups. Small payouts will be given to you to build your trust. Following this, you will be encouraged to take on other tasks with higher payout that require you to create accounts and transfer large sums of money to unknown bank accounts.

E-COMMERCE SCAMS

Cybercriminals use attractive deals to pressure you into immediate payment before delivery. Once paid, they become uncontactable. In some cases, they ask you to download a malicious app to make payment or process a refund. Installing the app gives them access to your device, banking, and social media accounts.

What to look out for:

These are the signs of phishing to look out for. Cybercriminals may do the following to trick you:

- Send unexpected or unsolicited emails, messages or calls
- Promise attractive rewards or promote exclusive deals
- Use urgent or threatening language to pressure action
- Request for personal and/or banking information
- Include suspicious links or attachments

PENIPUAN PELABURAN

Penjenayah siber menggunakan media sosial dan platform pesanan untuk menjalankan penipuan pelaburan. Mereka mengiklankan pelaburan palsu yang menjanjikan pulangan yang tinggi, atau masukkan anda ke dalam kumpulan sembang di mana rakan subahat akan berkongsi kisah kejayaan palsu atau tangkapan skrin pembayaran untuk menjadikan penipuan itu kelihatan tulen. Ada yang mungkin berkawan dengan anda terlebih dahulu bagi membina kepercayaan sebelum memperdaya anda supaya memindahkan wang.

PENIPUAN PEKERJAAN

Penjenayah siber mungkin menjanjikan komisen kepada anda bagi menjalankan tugas mudah seperti mengulas hotel atau melengkapkan tinjauan melalui kumpulan sembang WhatsApp atau Telegram. Anda akan diberikan sedikit pembayaran untuk membina kepercayaan. Berikutan itu, anda akan digalakkan supaya mengambil tugas lain dengan bayaran yang lebih tinggi namun memerlukan anda membuat akaun dan memindahkan sejumlah besar wang ke akaun bank yang tidak diketahui.

PENIPUAN E-DAGANG

Penjenayah siber menggunakan tawaran menarik untuk mendesak anda supaya mengirim bayaran dengan segera sebelum mereka membuat hantaran. Setelah dibayar, mereka akan hilangkan diri. Dalam beberapa kes, mereka meminta anda memuat turun perisian hasad, dengan alasan mahu membuat bayaran atau mengembalikan wang. Memasang aplikasi itu akan memberi mereka akses kepada peranti, akaun perbankan dan media sosial anda.

Apa yang perlu diperhatikan:

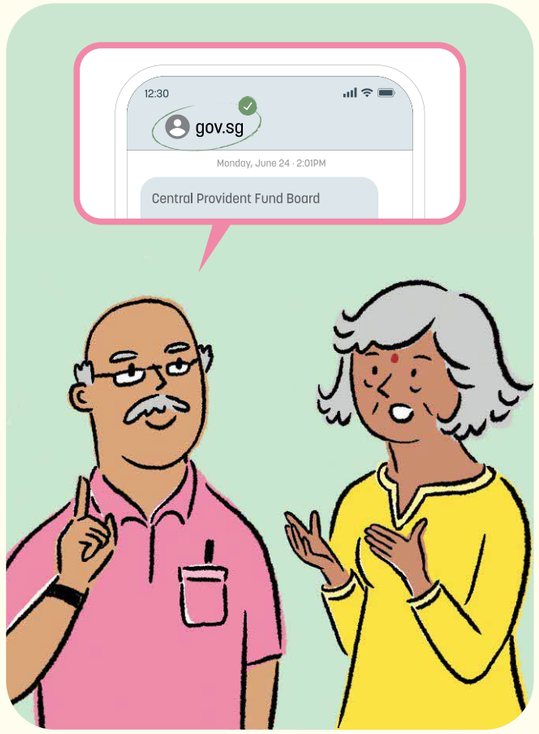
Berikut antara tanda-tanda pancingan data yang perlu diperhatikan. Penjenayah siber mungkin melakukan perkara berikut untuk menipu anda:

- Hantar e-mel, mesej atau panggilan yang tidak diundang atau tidak diminta
- Janjikan ganjaran menarik atau promosikan tawaran eksklusif
- Gunakan bahasa yang mendesak atau mengancam untuk mencetus tindakan
- Minta maklumat peribadi dan/atau perbankan
- Sertakan pautan atau lampiran yang mencurigakan

What you can do:

Take a moment to **STOP** and **CHECK** using the steps below:

- **Verify unexpected calls or messages** by contacting the official hotline or visiting the official app or website directly. To confirm messages or calls from a friend, call the number saved in your contacts.
- **Rethink** if the purchase or investment returns sound too good to be true
- **Call for advice.** Check with your family members or friends, or call the ScamShield Helpline at 1799.
- **Do not share** your personal and banking information unless you are sure it is a legitimate request
- **Do not click** on any attachment or link in the message. Delete it.
- **Do not download** unknown apps or software from a third-party website



WHAT IS MALWARE?

Malware is short for "malicious software". It refers to a type of software that infects your devices, steals your information, corrupts and even deletes your data.

MALWARE-ENABLED SCAMS

Cybercriminals may trick you into installing malware by asking you to download their app to enjoy free deliveries or discounts.

Once installed, the malware gives them access to your device and allows them to steal your banking details, passwords and OTPs to make unauthorised transactions.

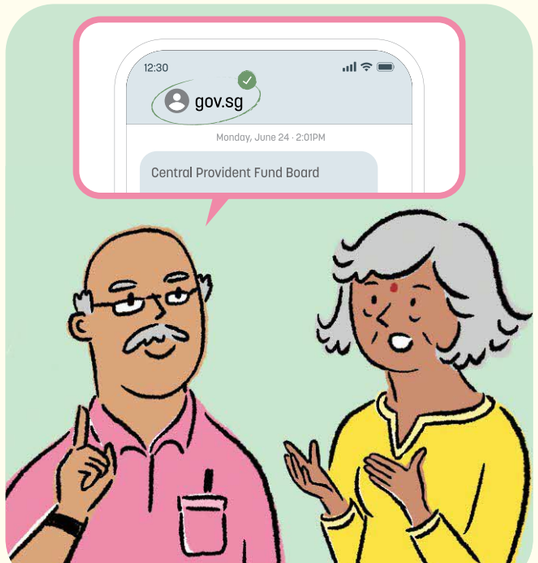
What to look out for:

Be cautious if someone asks you to download an app from unofficial sources for discounts or free services. Cybercriminals may also pressure you and give step-by-step instructions on how to download the app.

Apa yang boleh anda lakukan:

Luangkan masa untuk **BERHENTI** dan **SEMAK** menggunakan langkah-langkah di bawah:

- **Semak panggilan atau mesej yang tidak dijangka** dengan menghubungi talian hotline rasmi atau melayari aplikasi atau laman web rasmi secara langsung. Untuk mengesahkan mesej atau panggilan daripada rakan, hubungi nombor yang disimpan dalam senarai kenalan anda.
- **Fikirkan semula** jika pembelian atau pulangan pelaburan yang kelihatan terlalu baik
- **Hubungi untuk nasihat.** Semak dengan ahli keluarga atau rakan anda, atau hubungi Talian Bantuan ScamShield di 1799.
- **Jangan kongsi** maklumat peribadi dan perbankan anda melainkan anda pasti ia adalah permintaan yang sah
- **Jangan klik** pada sebarang lampiran atau pautan dalam mesej. Padamkannya.
- **Jangan muat turun** aplikasi atau perisian yang tidak diketahui daripada laman web pihak ketiga



APAKAH ITU PERISIAN HASAD (MALWARE)?

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

PENIPUAN MENGGUNAKAN PERISIAN HASAD

Penjenayah siber mungkin memperdaya anda supaya memasang perisian hasad dengan meminta anda memuat turun aplikasi mereka untuk menikmati penghantaran percuma atau diskaun.

Setelah dipasang, perisian hasad tersebut memberi mereka akses kepada peranti anda dan membolehkan mereka mencuri butiran perbankan, kata laluan dan OTP anda untuk membuat transaksi tanpa kebenaran.

Apa yang perlu diperhatikan:

Berwaspada jika seseorang meminta anda memuat turun aplikasi daripada sumber tidak rasmi untuk mendapatkan diskaun atau perkhidmatan percuma. Penjenayah siber juga mungkin mendesak anda dan menunjukkan langkah-langkah terperinci tentang cara memuat turun aplikasi tersebut.

What you can do:

- **Do not grant accessibility permissions** to unknown apps
- **Only download apps from official app stores** such as Google Play Store (Android) or Apple App Store (iOS) as these platforms have measures in place to detect and remove malicious apps

How can you tell if your phone has been infected with malware?

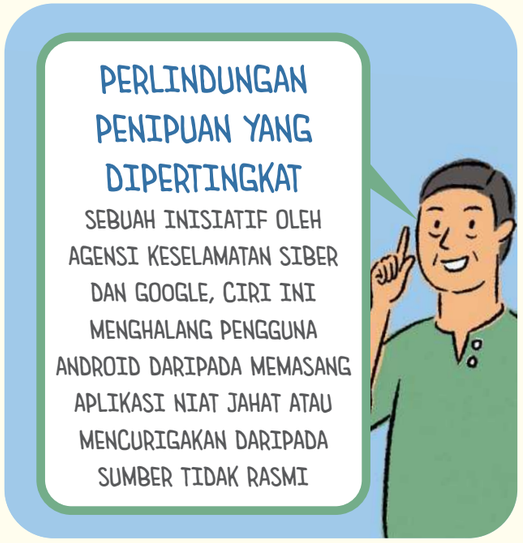
- Excessive and unexplained data use
- Random pop-ups or new apps not installed by you
- Noticeably slower responses or performance
- Battery drains unusually
- Unexpected or suspicious behaviours from the device such as auto-activation of camera or microphone

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

- Turn on the "airplane mode" and keep Wi-Fi off
- Run an anti-virus scan on your phone with an updated anti-virus app
- Use a different and trusted device to check for any unauthorised banking, Singpass or CPF transactions
- If there are unauthorised transactions, report them to the bank and Police immediately
- After completing these steps, if you believe your phone is not infected, you may resume use. As a precaution, consider a "factory reset" and changing important passwords. Back up your data first.

Apa yang anda boleh lakukan:

- **Jangan berikan akses** kepada aplikasi yang tidak diketahui
- **Hanya muat turun aplikasi daripada gedung aplikasi rasmi** seperti Google Play atau App Store kerana platform ini mempunyai langkah-langkah untuk mengesan dan mengalih keluar aplikasi berniat jahat



Bagaimana anda boleh ketahui sama ada telefon anda telah dijangkiti perisian hasad?

- Penggunaan data yang berlebihan dan tidak dapat dijelaskan
- Tetingkap timbul secara rambang atau kemunculan aplikasi baru yang anda tidak pasang
- Respons atau prestasi lebih perlahan yang ketara
- Bateri cepat habis secara luar biasa
- Tingkah laku yang tidak dijangka atau mencurigakan daripada peranti seperti kamera atau mikrofon menjadi aktif secara automatik

Apa yang perlu anda lakukan jika telefon anda dijangkiti perisian hasad?

- Tukarkan telefon anda kepada "mod pesawat" dan matikan Wi-Fi
- Laksanakan imbasan antivirus di telefon anda dengan aplikasi antivirus yang terkini
- Gunakan peranti lain dan yang dipercayai untuk semak sebarang transaksi perbankan, SingPass atau CPF yang tidak dibenarkan
- Jika terdapat transaksi yang tidak dibenarkan, laporkannya kepada bank dan Polis dengan segera
- Selepas melengkapkan langkah-langkah ini, jika anda percaya telefon anda tidak dijangkiti, anda boleh sambung semula penggunaannya. Sebagai langkah berjaga-jaga, pertimbangkan langkah "tetapan asal" dan tukar kata laluan penting. Buat salinan data anda terlebih dahulu.

DEEPFAKES

Deepfakes are photos, videos, or audio recordings digitally created or altered using Generative Artificial Intelligence (AI). As technology advances, deepfakes are becoming increasingly convincing. They are used in online scams to impersonate authority figures and celebrities, tricking you into revealing personal details or authorising fraudulent payments. This can lead to irreversible financial losses.

What to look out for:

- Check if content comes from an official or trusted source
- Be extra careful if the content:
  - Includes the use of urgent language ("transfer now", "last chance")
  - Asks for sensitive information (NRIC, bank account, OTP)
  - Requests for money transfers
- Look for unnatural signs in videos/audio:
  - Blurring around face edges
  - Unnatural blinking or facial movements
  - Lips not matching speech

What you can do:

- **Pause and think.** Do not rush, especially if the message is urgent, unsafe, or unusual.
- **Verify the source.** Contact the person or organisation using a phone number or channel you already know (e.g. official hotline, saved contact), not the one given in the message.
- **Do not share sensitive information.** Never reveal your passwords, OTPs, or full bank details over calls, messages, or videos.
- **Do not transfer money.** Discuss with family members and friends first.

LEARN MORE

Scan the QR code for more information on Generative AI & Deepfakes!

DEEPFAKE

Deepfake ialah foto, video atau rakaman audio yang dicipta atau diubah suai secara digital menggunakan Kecerdasan Buatan Generatif (AI). Seiring dengan kemajuan teknologi, deepfake menjadi semakin meyakinkan. Ia digunakan dalam penipuan dalam talian untuk menyamar sebagai tokoh berkuasa atau selebriti bagi memperdaya anda supaya mendedahkan butiran peribadi atau membenarkan pembayaran palsu. Ini boleh menyebabkan kerugian kewangan yang tidak dapat dipulihkan.

Apa yang perlu diperhatikan:

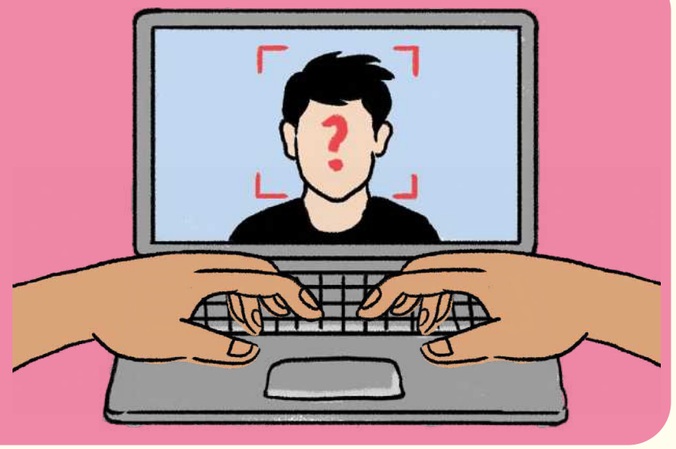
- Semak sama ada kandungan berasal dari sumber rasmi atau dipercayai
- Berhati-hati jika kandungan tersebut:
  - Menggunakan bahasa mendesak ("pindahkan sekarang", "peluang terakhir")
  - Meminta maklumat sensitif (NRIC, akaun bank, OTP)
  - Meminta pemindahan wang
- Cari tanda-tanda luar biasa dalam video/audio:
  - Kabur di sekitar tepi muka
  - Kelipan mata atau pergerakan muka yang tidak wajar
  - Bibir tidak sepadan dengan pertuturan

Apa yang boleh anda lakukan:

- **Berhenti seketika dan fikir.** Jangan tergesa-gesa, terutamanya jika mesej tersebut mendesak, tidak selamat atau luar biasa.
- **Sahkan sumbernya.** Hubungi individu atau pertubuhan berkenaan menggunakan nombor telefon atau aluran yang anda sudah ketahui (cth. talian hotline rasmi, nombor kenalan yang disimpan), bukan yang diberikan dalam mesej.
- **Jangan kongsi maklumat sensitif.** Jangan sama sekali dedahkan kata laluan, OTP atau butiran bank penuh anda melalui panggilan, mesej atau video.
- **Jangan pindahkan wang.** Bincang dengan ahli keluarga dan rakan-rakan terlebih dahulu.

KETAHUI LEBIH LANJUT

Imbas kod QR untuk mendapatkan lebih banyak maklumat tentang AI Generatif dan Deepfake!



HOW TO BE CYBER SAFE

Practising good cyber hygiene helps protect you from falling prey to online scams. Protect yourself through the adoption of three cyber tips:

Enable 2FA and Use Strong Passphrases

Using Two-Factor Authentication (2FA) together with a strong passphrase provides an additional layer of protection for your online accounts.

2FA uses more than one type of information to verify your identity and access your online accounts.

How to create a strong passphrase:

Step 1: **String together 5 different words** from a personal memory

Bread → ihadbread**at8am**

Step 2: **Use uppercase, lowercase, numbers and symbols** (at least 12 characters)

ihadBREADat8am!

Do not use easily obtainable information such as your name, NRIC number, or birthdate.

Do not share your passwords with anyone or write them down.

CARA KEKAL SELAMAT SIBER

Mengamalkan langkah siber yang baik boleh bantu lindungi anda daripada menjadi mangsa penipuan dalam talian. Lindungi diri anda dengan mengamalkan tiga tip siber:

Aktifkan Pengesahan Dua Faktor (2FA) dan Frasa Laluan yang Kuat

Menggunakan Pengesahan Dua Faktor (2FA) dengan frasa laluan yang kukuh menyediakan lapisan perlindungan tambahan untuk akaun dalam talian anda.

2FA menggunakan lebih dari satu jenis maklumat untuk mengesahkan identiti dan mengakses akaun dalam talian anda.

Cara mencipta frasa laluan yang kukuh:

Langkah 1: **Gabungkan 5 perkataan berbeza dari ingatan peribadi**

Roti → sayamakanroti**pada8pg**

Langkah 2: **Campurkan huruf besar, huruf kecil, nombor dan simbol** (sekurang-kurangnya 12 karakter)

sayamakanROTIpada8pg!

Jangan gunakan maklumat yang mudah diperoleh seperti nama, nombor kad pengenalan dan tarikh lahir.

Jangan kongsi kata laluan anda dengan sesiapa atau tuliskannya.

Update Software Promptly

Software and app updates contain important security fixes that can help keep your devices safe.

LEARN MORE

Scan here to find out how to enable automatic updates!

Add ScamShield and Anti-Virus Apps

ScamShield is a suite of products and tools that help defend against scams. Download the app to block and filter scam calls and messages.

Anti-Virus Apps help detect malware and malicious phishing links. They are key to safeguarding your devices and accounts.

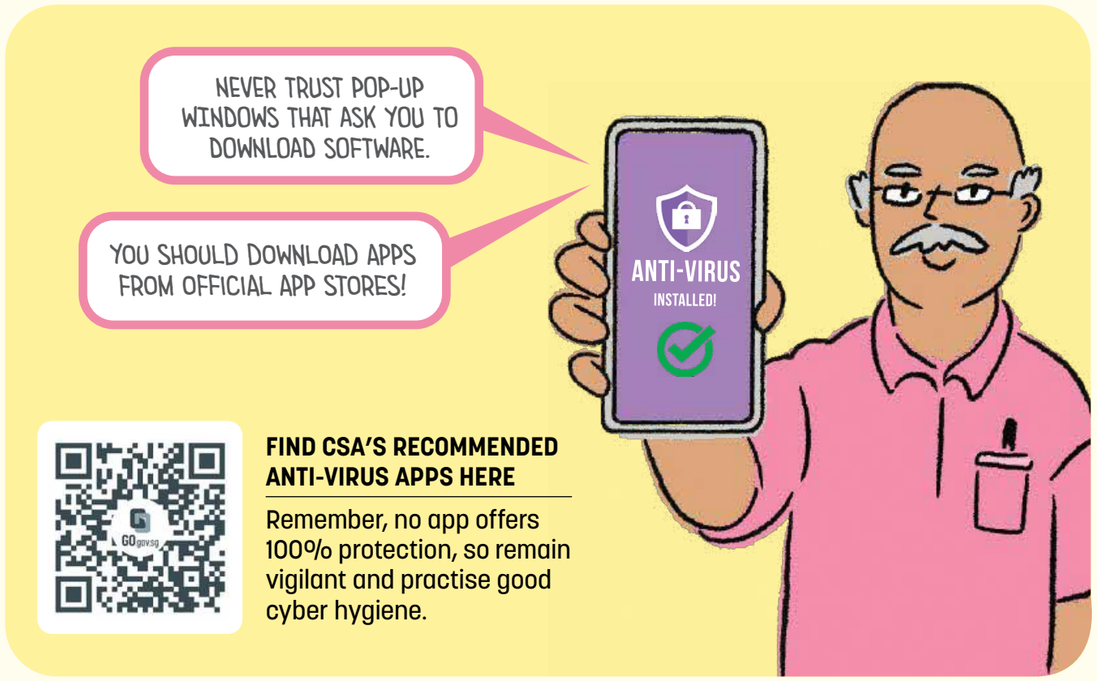
How to choose an Anti-Virus App

Anti-virus apps from different brands have varying functions and capabilities. Here are some tips when choosing an anti-virus app:

- **Download from official app stores** such as Google Play Store (Android) or Apple App Store (iOS)
- **Check out app reviews before downloading.** Look at the developer's reputation, app ratings and the number of downloads too.
- **Choose apps with detection and removal capabilities.** Look for those that provide real time malware detection (for Android devices only) and removal capabilities.

LEARN MORE

Scan here for more information on ScamShield



FIND CSA'S RECOMMENDED ANTI-VIRUS APPS HERE

Remember, no app offers 100% protection, so remain vigilant and practise good cyber hygiene.

Kemas Kini Perisian Dengan Segera

Perisian dan aplikasi terkini mengandungi pembetulan keselamatan penting yang boleh bantu memastikan peranti anda selamat.

KETAHUI LEBIH LANJUT

Imbas di sini untuk ketahui cara mendayakan kemas kini automatik!

Muat Turun Aplikasi-aplikasi ScamShield dan Antivirus

ScamShield ialah set produk dan alatan yang membantu melindungi anda daripada penipuan. Muat turun aplikasi ini untuk menyekat dan menapis panggilan serta mesej penipuan.

Aplikasi Antivirus membantu mengesan perisian hasad dan pautan pancingan data yang berniat jahat. Ia adalah kunci untuk melindungi peranti dan akaun anda.

Cara memilih Aplikasi Antivirus

Aplikasi antivirus daripada jenama yang berbeza mempunyai fungsi dan keupayaan yang berbeza. Berikut beberapa petua ketika memilih aplikasi antivirus:

- **Muat turun daripada gedung aplikasi rasmi** seperti Google Play Store (Android) atau Apple App Store (iOS)
- **Semak ulasan aplikasi sebelum memuat turun.** Lihat Juga reputasi pembangun, penilaian aplikasi dan bilangan muat turun.
- **Pilih aplikasi dengan keupayaan pengesanan dan penyingkiran.** Cari aplikasi yang menyediakan pengesanan malware (untuk peranti Android sahaja) dan keupayaan penyingkiran masa nyata.

KETAHUI LEBIH LANJUT

Imbas kod QR untuk mendapatkan lebih banyak maklumat tentang ScamShield

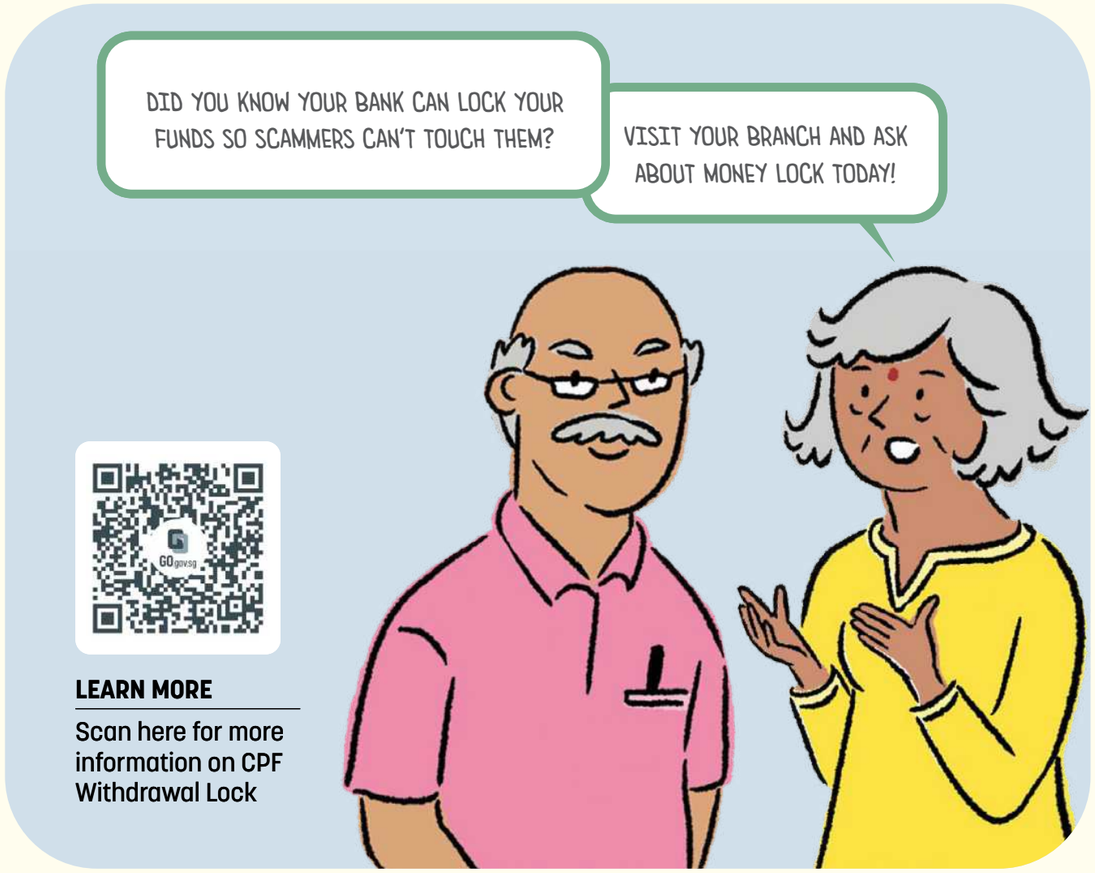
CARI APLIKASI ANTIVIRUS YANG DISYORKAN OLEH CSA DI SINI.

Ingat: tiada aplikasi yang menawarkan perlindungan 100%, jadi kekal berwaspada dan amalkan langkah siber yang baik.

What else can you do to protect yourself?

Besides practising good cyber hygiene, there are additional security features you can enable in your apps to protect your savings and reduce potential losses in the event of a scam.

- **Money Lock** was introduced by the local banks to safeguard your bank account and guard against scams by allowing funds to be 'locked' so they cannot be transferred digitally. Check with your bank on how to activate this feature.
- The **CPF Withdrawal Lock** feature allows members aged 55 and above to instantly disable online CPF withdrawals. You can activate this feature at any time through your CPF account settings and set your Daily Withdrawal Limit to safeguard your savings.



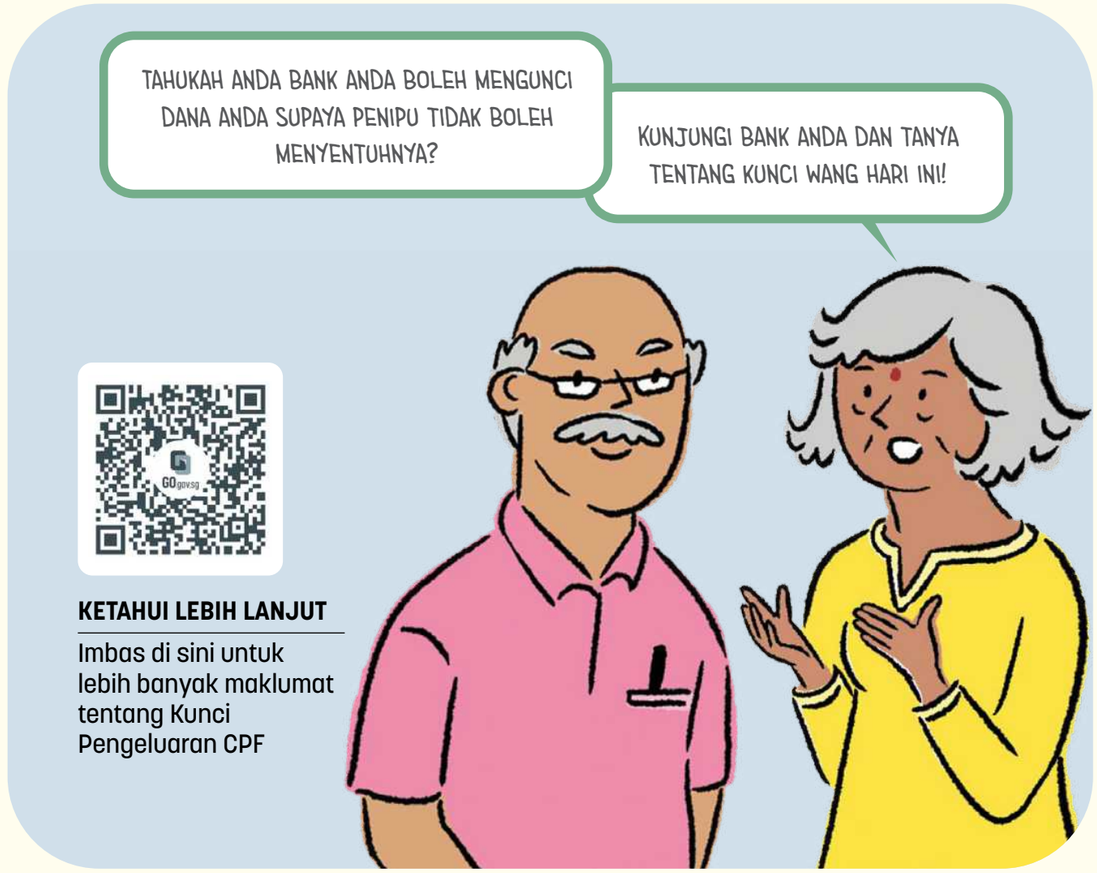
LEARN MORE

Scan here for more information on CPF Withdrawal Lock

Apa lagi yang boleh anda lakukan untuk melindungi diri anda?

Selain mengamalkan langkah-langkah keselamatan siber yang baik, terdapat ciri keselamatan tambahan yang boleh anda dayakan dalam aplikasi-aplikasi anda untuk melindungi simpanan dan mengurangkan potensi kerugian sekiranya berlaku penipuan.

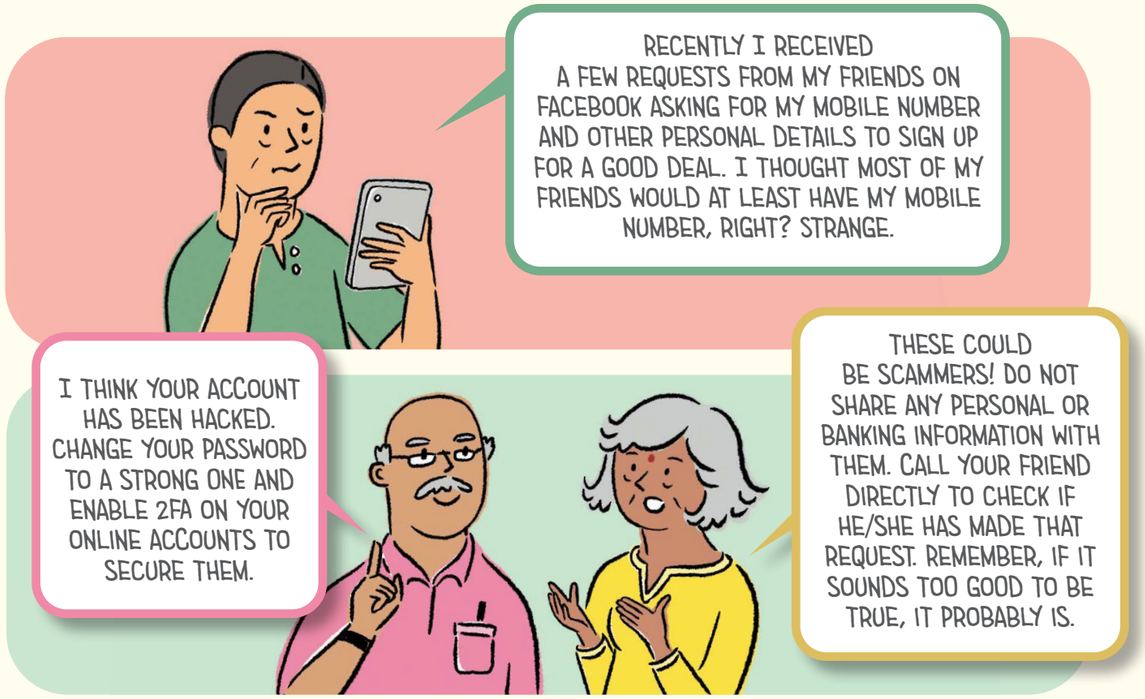
- **Money Lock** diperkenalkan oleh bank tempatan untuk melindungi akaun bank anda dan mencegah penipuan dengan 'mengunci' dana supaya ia tidak boleh dipindahkan secara digital. Rujuk bank anda untuk mengetahui cara mengaktifkan ciri ini.
- Ciri **Kunci Pengeluaran CPF** membolehkan ahli berumur 55 tahun ke atas melumpuhkan pengeluaran CPF dalam talian secara serta-merta. Anda boleh mengaktifkan ciri ini pada bila-bila masa melalui tetapan akaun CPF dan menetapkan Had Pengeluaran Harian untuk melindungi simpanan anda.



KETAHUI LEBIH LANJUT

Imbas di sini untuk lebih banyak maklumat tentang Kunci Pengeluaran CPF

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



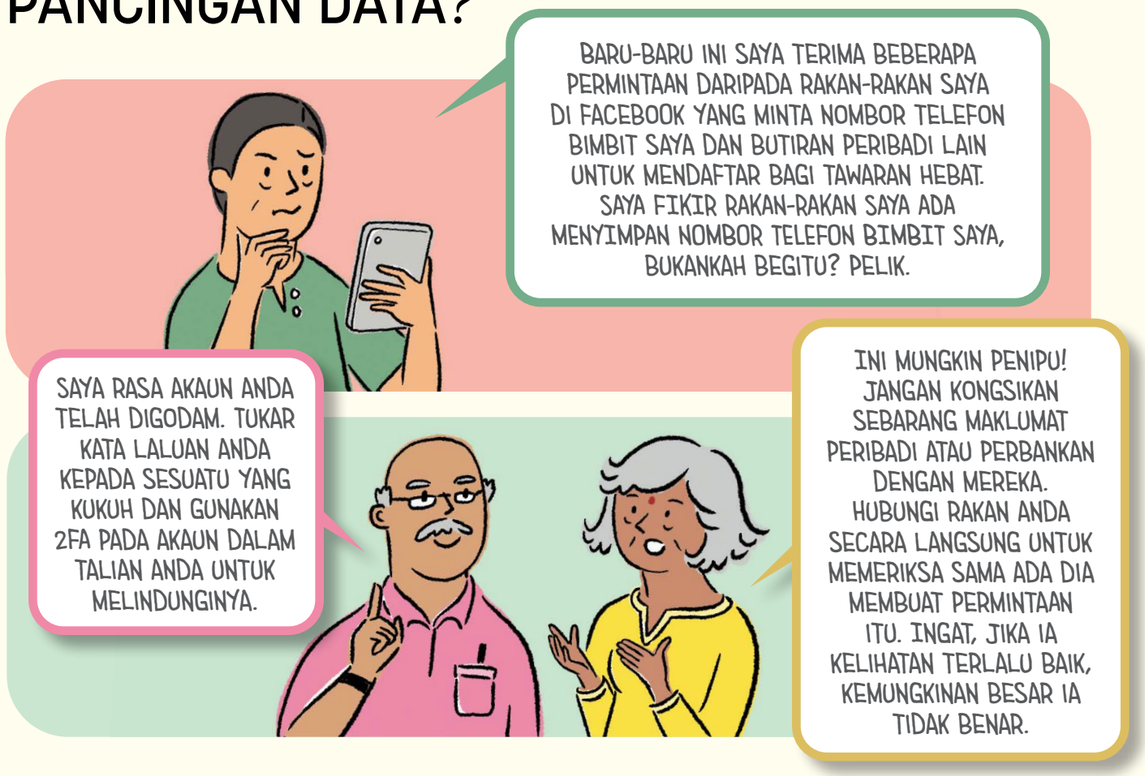
If you still have access to your account,

- **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 www.police.gov.sg/e-services 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.

APAKAH YANG PERLU ANDA LAKUKAN JIKA ANDA MENJADI MANGSA PENIPU PANCINGAN DATA?



Jika anda masih ada akses kepada akaun anda,

- **Log keluar daripada akaun ini daripada semua peranti** yang disambungkan ke akaun tersebut
- **Tukar kata laluan anda dengan segera** dan gunakan 2FA jika tersedia

Jika anda tidak ada akses kepada akaun anda,

- **Hubungi platform** contohnya bank atau platform media sosial, untuk melaporkan isu tersebut dan minta bantuan untuk dapatkan semula akaun anda
- **Laporkan sebarang caj kad kredit/debit palsu** kepada bank anda dan batalkan kad anda dengan segera
- **Buat laporan polis** di pusat polis kejiranan atau pos polis kejiranan terdekat, atau secara dalam talian di www.police.gov.sg/e-services sekiranya berlaku kerugian kewangan
- **Layari Laman Web SingCERT CSA** di www.csa.gov.sg/singcert/reporting jika anda ingin mengemukakan laporan insiden
- Sekiranya akaun anda digodam, penyamar boleh menghubungi kenalan anda. **Beri amaran kepada keluarga dan rakan** anda supaya mengabaikan sebarang permintaan dan jangan berkongsi butiran peribadi mereka.

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. STOP AND 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?

SAYA BIMBANG SAYA AKAN DITIPU. MUNGKIN SAYA TIDAK HARUS MEMBALAS SEBARANG MESEJ ATAU PANGGILAN.

JANGAN RISAU. KITA HANYA PERLU BERWASPADA. BERHENTI SEKETIKA UNTUK MEMERIKSA DAN HUBUNGI AHLI KELUARGA ATAU RAKAN UNTUK MENDAPATKAN NASIHAT.

YA. DAN INGAT, JANGAN KONGSI KATA LALUAN ATAU OTP ANDA DENGAN SESIAPA PUN. DENGAN SAYA PUN TAK BOLEH, OKAY?

Better cyber safe than sorry

For more information, visit CSA's SG Cyber Safe Seniors webpage or ScamShield website.

Untuk maklumat lanjut, lawati laman web Warga Emas Siber Selamat SG CSA atau laman web ScamShield.

www.csa.gov.sg **www.scamshield.gov.sg**

Get more cyber tips at:

Dapatkan lebih banyak tip siber di:

For the latest scam info, visit:

Untuk maklumat penipuan terkini, lawati: