LAPORKAN KEJADIAN DAN SERANGAN-SIBER UNTUK MEMASTIKAN AUSTRALIA KEKAL SELAMAT.

LAYANI

Perkhidmatan amaran percuma kami
cyber.gov.au

LAPORKAN

Jenayah siber kepada REPORTCYBER:
cyber.gov.au/report

HUBUNGI

Sila panggil 1300 CYBER1 atau layari cyber.gov.au

Nombor ini tersedia untuk digunakan di dalam Australia sahaja.

IKUTI KAMI

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5. BERWASPADA TERHADAP PENIPUAN DALAM TALIAN (SCAM)

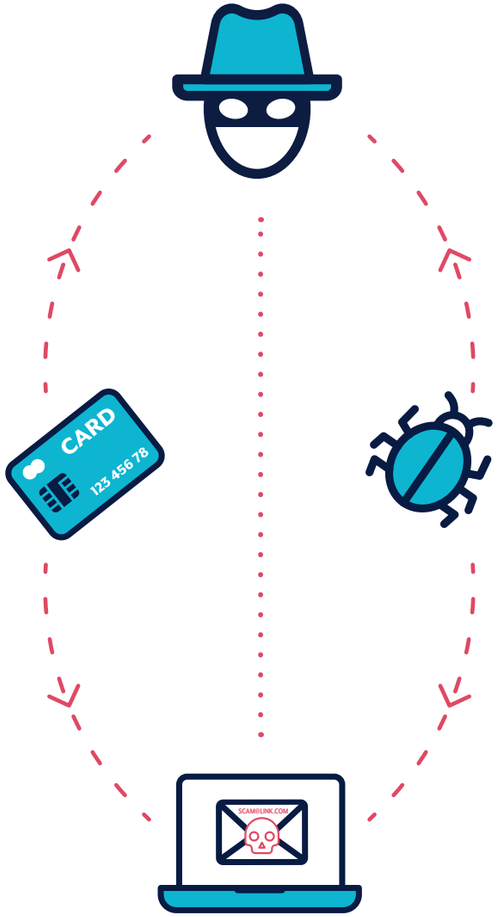
Penjenayah siber menggunakan emel, SMS, panggilan telefon dan media sosial bagi menipu anda untuk membuka lampiran, melayari laman web, mendedahkan butir-butir daftar masuk ke dalam akaun, mendedahkan maklumat sensitif atau menghantar wang atau kad hadiah. Mesej-mesej ini dibentuk sedemikian rupa supaya ia kelihatan seakan-akan dikirim daripada para individu atau organisasi yang anda fikir anda kenali, atau yang anda fikir anda patut percayai.

Untuk mengenalpasti mesej scam, berhenti dan fikirkan dahulu:

- **Pihak Berkuasa:** Adakah mesej itu mendakwa ia datang daripada seorang pegawai rasmi?
- **Tindakan Mustahak:** Adakah anda diberitahu anda hanya mempunyai tempoh masa terhad untuk bertindak?
- **Emosi:** Adakah mesej itu menjadikan anda cemas, takut, menaruh harapan atau tergerak untuk ingin tahu dengan lebih lanjut?
- **Jarang ada:** Adakah mesej itu menawarkan sesuatu yang sukar diperolehi?
- **Peristiwa semasa:** Adakah mesej itu berkaitan kisah berita semasa, kejadian hebat atau masa-masa tertentu dalam setahun (misalnya pelaporan cukai).

Untuk menyemak sama ada mesej tersebut sahih atau tidak:

- Sila rujuk kembali kepada sesuatu yang anda boleh percaya. Sila layari laman web rasmi, daftar masuk ke dalam akaun anda, atau panggil nombor telefon mereka yang diiklankan. Jangan guna pautan atau butir-butir kontak di dalam mesej yang telah dikirimkan kepada anda or diberi menerusi telefon.
- Sila semak dahulu untuk menentukan jika sumber rasmi berkenaan sudah pun memberitahu anda apa yang mereka tidak akan sama sekali minta daripada anda. Contohnya, bank anda mungkin telah memberitahu anda bahawa mereka sama sekali tidak akan meminta kata laluan anda.



Untuk maklumat lanjut tentang cara untuk mengenalpasti mesej scam, sila rujuk 'Detecting Socially Engineered Messages' (Mengesan Mesej-Mesej yang Dijana Secara Sosial) terbitan Pusat Keselamatan Siber Australia (Australian Cyber Security Centre) (ACSC), dan pastikan anda senantiasa menerima maklumat terkini dengan melayani Perkhidmataan Amaran ACSC (ACSC's Alert Service) di **cyber.gov.au**

LANGKAH-LANGKAH MUDAH

UNTUK MENEGUHKAN KESELAMATAN ALAT-ALAT PERANTI DAN AKAUN-AKAUN ANDA

KURANGKAN RISIKO MENJADI SASARAN PENJENAYAH SIBER DENGAN MEMATUHI LANGKAH-LANGKAH BERIKUT

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1. KEMASKINIKAN ALAT-ALAT PERANTI ANDA

Penjenayah siber menggodam alat-alat peranti dengan menggunakan kelemahan yang diketahui dalam sistem-sistem atau apps. Pengemaskinian mempunyai penaiktarafan keselamatan untuk membaiki kelemahan-kelemahan ini. Pasangkan pengemaskinian automatik supaya ia boleh dilakukan tanpa input anda.

Pasangkan pengemaskinian automatik bagi semua alat-alat peranti anda:

- Telefon bimbit
- Komputer riba
- Komputer

Kerap periksakan pengemaskinian anda bagi:

- Apps
- Program
- Alat-Alat Pintar

2. PASANGKAN PENGESAHAN PELBAGAI-FAKTOR (MULTI-FACTOR AUTHENTICATION) (MFA)

MFA memperbaiki keselamatan anda dengan meningkatkan tahap kesukaran bagi penjenayah siber untuk mengakses fail-fail atau akaun anda.

Aktifkan MFA, bermula dengan akaun-akaun penting anda:

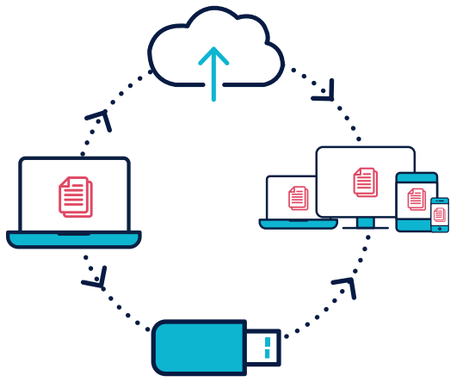
- Akaun-akaun e-mel
- Perbankan dan akaun-akaun dalam talian yang menyimpan butir-butir pembayaran.
- Media sosial

3. SANDARKAN ALAT-ALAT PERANTI ANDA

Sebuah salinan sandaran ialah salinan digital maklumat yang tersimpan dalam alat peranti anda, contohnya foto, dokumen, video, dan data daripada aplikasi. Ia boleh disimpan ke dalam sebuah alat peranti simpanan luaran atau ke awan. Membikinkan salinan sandaran bererti anda boleh mengembalikan fail-fail anda sekiranya alat peranti anda hilang, dicuri atau mengalami kerosakan.

Kerap buatkan salinan sandaran bagi alat peranti anda:

- Telefon bimbit
- Komputer riba
- Komputer
- Tablet



4. SETKAN FRASA LALUAN YANG KUKUH

Dalam kes di mana MFA tidak disediakan, sebuah frasa laluan yang kukuh seringkali merupakan satu-satunya perkara yang boleh melindungi maklumat dan akaun anda daripada penjenayah.

Sebuah frasa laluan menggunakan empat perkataan rawak atau lebih sebagai kata laluan anda. Tukarkan kata laluan anda kepada frasa laluan, dengan memastikan ianya:

- Panjang: Lagi panjang frasa laluan anda, lagi baik. Pastikan ia sekurang-kurangnya sepanjang 14 huruf.
- Tidak boleh diramal: Gunakan campuran rawak perkataan yang tiada kaitan antara satu sama lain
- Unik: Jangan gunakan kembali frasa laluan bagi pelbagai akaun