LAPORKAN SERANGAN DAN INSIDEN DUNIA MAYA UNTUK MENJAGA AUSTRALIA TETAP AMAN.

DAFTAR

Ke layanan peringatan gratis kami
cyber.gov.au

LAPORKAN

Kejahatan dunia maya kepada REPORTCYBER:
cyber.gov.au/report

HUBUNGI

Telepon 1300 CYBER1 atau
kunjungi **cyber.gov.au**
Nomor ini hanya dapat digunakan di Australia.

IKUTI KAMI

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5. HATI-HATI DENGAN PENIPUAN

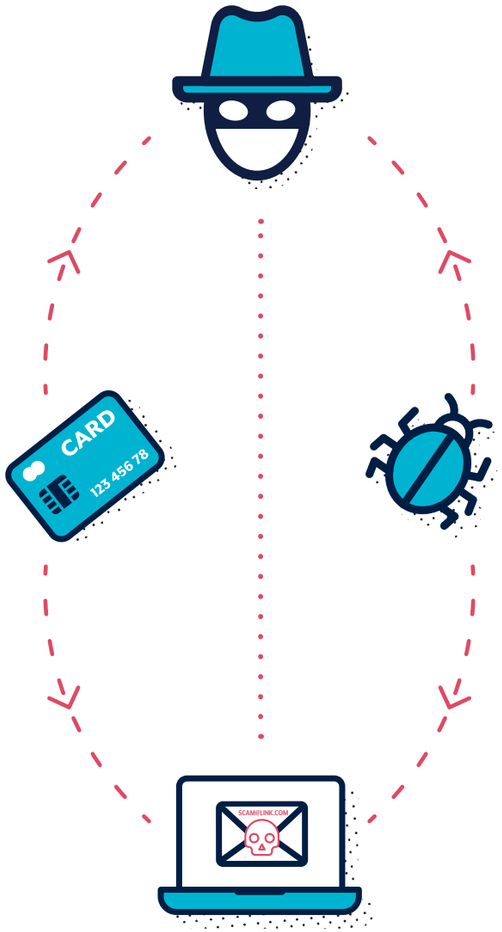
Penjahat dunia maya menggunakan email, SMS, panggilan telepon, dan media sosial untuk menipu Anda agar membuka lampiran, mengunjungi situs web, mengungkapkan detail login akun, mengungkapkan informasi sensitif, atau mentransfer uang atau kartu hadiah. Pesan-pesan tersebut dibuat agar tampak seolah-olah dikirim dari individu atau organisasi yang sepertinya Anda tahu, atau menurut Anda seharusnya dipercaya.

Untuk mengenali pesan penipuan, luangkan waktu dan pikirkan:

- **Otoritas:** Apakah pesan itu mengaku dari pihak resmi?
- **Urgensi:** Apakah Anda diberi tahu bahwa waktu Anda untuk merespons terbatas?
- **Emosi:** Apakah pesan tersebut membuat Anda panik, takut, berharap, atau penasaran?
- **Kelangkaan:** Apakah pesan itu menawarkan sesuatu yang terbatas?
- **Peristiwa terkini:** Apakah pesan itu terkait dengan berita terkini, peristiwa besar, atau waktu tertentu dalam setahun (seperti pelaporan pajak)?

Untuk memeriksa keabsahan sebuah pesan:

- Berpeganglah pada sesuatu yang dapat Anda percayai. Kunjungi situs web resmi, masuk ke akun Anda, atau hubungi nomor telepon yang diiklankan. Jangan gunakan tautan atau detail kontak dalam pesan yang dikirim kepada Anda atau diberikan melalui telepon.
- Periksa untuk mengetahui apakah sumber resmi telah memberi tahu Anda apa yang tidak akan pernah mereka tanyakan kepada Anda. Misalnya, bank Anda mungkin telah memberi tahu Anda bahwa pihaknya tidak akan pernah meminta kata sandi Anda.



Untuk informasi selengkapnya tentang mengenali pesan penipuan, lihat publikasi Mendeteksi Pesan Rekayasan Sosial (Socially Engineered Messages) dari Australian Cyber Security Center (ACSC), dan ikuti informasi terbaru dengan mendaftar ke Layanan Peringatan ACSC di **cyber.gov.au.**

LANGKAH MUDAH
UNTUK MENGAMANKAN PERANGKAT DAN AKUN ANDA

KURANGI RISIKO MENJADI
TARGET PENJAHAT DUNIA MAYA DENGAN
MENGIKUTI LANGKAH-LANGKAH INI

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1. PERBARUI PERANGKAT ANDA

Penjahat dunia maya meretas perangkat menggunakan kelemahan yang diketahui dalam sistem atau aplikasi. Pembaruan akan memberikan peningkatan keamanan untuk memperbaiki kelemahan itu. Aktifkan pembaruan otomatis, sehingga pembaruan dilakukan tanpa menunggu perintah Anda.

Aktifkan pembaruan otomatis di semua perangkat Anda:

- Ponsel
- Laptop
- Desktop

Periksa pembaruan secara teratur pada:

- Aplikasi
- Program
- Perangkat pintar

2. AKTIFKAN MULTI-FACTOR AUTHENTICATION (MFA)

MFA meningkatkan keamanan Anda dengan meningkatkan kerumitan saat penjahat dunia maya mencoba mengakses file atau akun Anda.

Aktifkan MFA, mulai dari akun paling penting Anda:

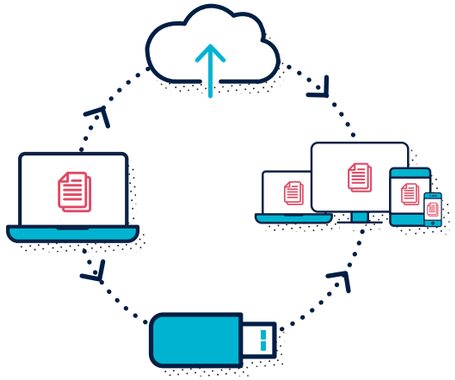
- Akun email
- Perbankan dan rekening online yang menyimpan detail pembayaran
- Media sosial

3. CADANGKAN PERANGKAT ANDA

Cadangan adalah salinan digital dari informasi yang disimpan di perangkat Anda, seperti foto, dokumen, video, dan data dari aplikasi. Cadangan dapat disimpan ke perangkat penyimpanan eksternal atau ke cloud. Dengan mencadangkan, Anda dapat memulihkan file jika perangkat Anda hilang, dicuri, atau rusak.

Cadangkan perangkat Anda secara berkala:

- Ponsel
- Laptop
- Desktop
- Tablet



4. TETAPKAN FRASA SANDI YANG AMAN

Apabila MFA tidak tersedia, frasa sandi yang aman seringkali dapat menjadi satu-satunya hal yang melindungi informasi dan akun Anda dari penjahat.

Frasa sandi menggunakan empat atau lebih kata acak sebagai kata sandi Anda. Ubah kata sandi Anda menjadi frasa sandi, dengan memastikan bahwa frasa sandi itu.

- Panjang: Makin panjang kata sandi Anda, makin baik. Buatlah panjangnya setidaknya 14 karakter
- Tidak dapat diprediksi: Gunakan campuran acak dari kata-kata yang tidak berhubungan
- Unik: Jangan gunakan kembali frasa sandi di banyak akun