



Australian Government
Australian Signals Directorate

ACSC Australian
Cyber Security
Centre



KEAMANAN DUNIA MAYA PRIBADI LANGKAH PERTAMA

cyber.gov.au

Seri Keamanan Dunia Maya Pribadi

Keamanan Dunia Maya Pribadi: Panduan Langkah Pertama merupakan yang pertama dari seri tiga panduan yang dirancang untuk membantu warga Australia awam memahami dasar-dasar keamanan dunia maya dan cara mengambil tindakan untuk melindungi diri Anda dari ancaman dunia maya yang paling sering terjadi.

Anda dapat mengakses dua panduan lainnya di cyber.gov.au



Langkah Pertama



Langkah Berikutnya



Langkah Tingkat Lanjut

Daftar Isi

PENGANTAR	1
MENINGKATKAN KEAMANAN DUNIA MAYA ANDA	2
Mengaktifkan Pembaruan Otomatis	2
Mengaktifkan Autentikasi Multifaktor (MFA)	4
Mencadangkan Perangkat Anda secara Berkala	5
Menggunakan Frasa Sandi untuk Mengamankan Akun Penting Anda	6
Mengamankan Perangkat Seluler Anda	7
Mengembangkan Pemikiran Keamanan Dunia Maya Anda	8
DAFTAR PERIKSA RINGKASAN	11
DAFTAR ISTILAH	12

Pendahuluan

Apa itu keamanan dunia maya pribadi?

Di dunia yang semakin berbasis teknologi, kita menggunakan perangkat dan akun setiap hari yang rentan terhadap ancaman dunia maya:

- Perangkat Anda mungkin mencakup komputer, ponsel, tablet, dan perangkat lain yang terhubung ke internet.
- Anda juga dapat menggunakan akun online untuk email, perbankan, belanja, media sosial, game, dan lainnya.

Keamanan dunia maya pribadi adalah langkah berkelanjutan yang dapat Anda lakukan untuk melindungi akun dan perangkat Anda dari ancaman dunia maya.

Apa itu ancaman dunia maya?

Ancaman dunia maya utama yang sering kali merugikan warga Australia adalah **penipuan dan malware**.

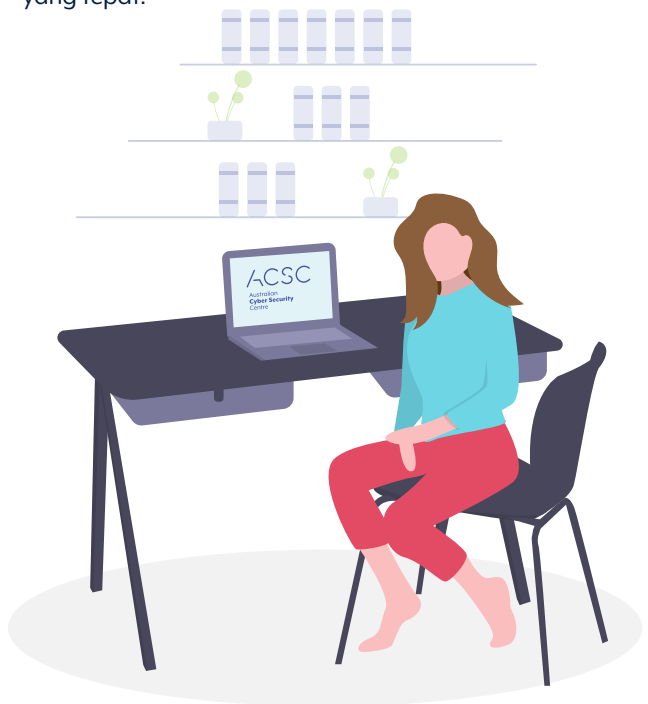
- **Malware adalah istilah umum untuk perangkat lunak berbahaya** yang dirancang untuk menyebabkan kerusakan, termasuk virus, worm, spyware, trojan, dan ransomware. Penjahat dunia maya menggunakan malware untuk mencuri informasi dan uang Anda, serta mengendalikan perangkat dan akun Anda.
- **Penipuan adalah pesan yang dikirim oleh penjahat dunia maya** yang dirancang untuk memanipulasi Anda agar memberikan informasi sensitif atau mengaktifkan malware di perangkat Anda.

Serangan-serangan tersebut dapat memberikan kerugian pribadi dan finansial yang besar terhadap para korban dan semakin canggih dan sering terjadi.

Bagaimana panduan ini dapat membantu melindungi saya dari ancaman dunia maya?

Keamanan Dunia Maya Pribadi: panduan Langkah Pertama merupakan yang pertama dari seri tiga panduan yang dirancang untuk membantu warga Australia awam memahami dasar-dasar keamanan dunia maya dan cara mengambil tindakan untuk melindungi diri Anda dari ancaman dunia maya yang paling sering terjadi.

Jika Anda saat ini belajar tentang keamanan dunia maya untuk pertama kali, atau sedang memperbarui pengetahuan Anda, panduan ini adalah awal yang tepat.



Australian Cyber Security Centre (ACSC), sebagai bagian dari Australian Signals Directorate (ASD), memberikan saran, bantuan, dan tanggapan operasional keamanan dunia maya untuk mencegah, mendeteksi, dan memulihkan ancaman dunia maya terhadap Australia. ACSC hadir untuk membantu menjadikan Australia tempat paling aman untuk terhubung secara online.

Untuk informasi, panduan, dan saran keamanan dunia maya selengkapnya, kunjungi situs web ACSC cyber.gov.au.

Jika Anda merasa menjadi korban kejahatan dunia maya, laporkan melalui ReportCyber ACSC di cyber.gov.au atau hubungi Saluran Siaga Keamanan Dunia Maya kami di 1300 CYBER1 (1300 292 371).

Perbarui pengetahuan tentang ancaman dunia maya terbaru: Daftarkan layanan peringatan online gratis dari ACSC di cyber.gov.au.

Meningkatkan Keamanan Dunia Maya Anda



Mengaktifkan Pembaruan Otomatis

Apa itu pembaruan?

Pembaruan adalah peningkatan versi perangkat lunak (program, aplikasi, dan sistem operasi) yang telah Anda instal pada komputer dan perangkat seluler Anda.

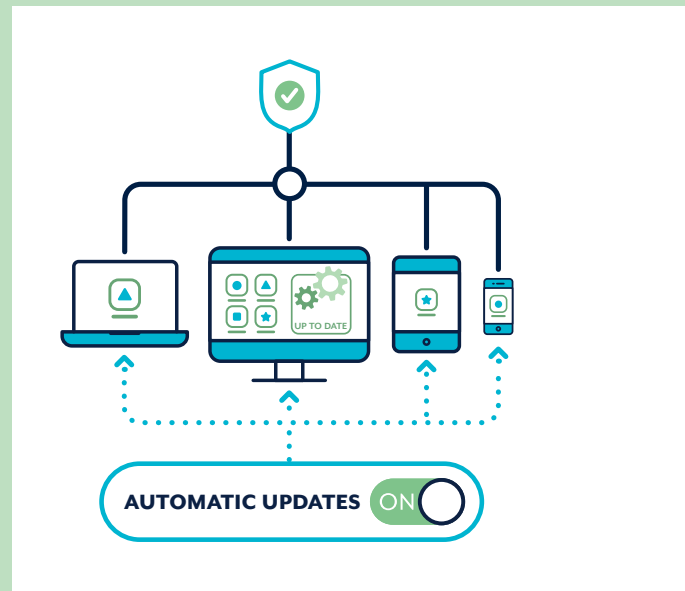
Pembaruan perangkat lunak membantu melindungi perangkat Anda dengan memperbaiki 'bug' perangkat lunak (kesalahan pengodean atau kerentanan) yang dapat digunakan oleh penjahat dunia maya dan malware untuk mengakses perangkat Anda dan mencuri data pribadi, akun, informasi keuangan, dan identitas Anda.

'Bug' perangkat lunak baru terus-menerus ditemukan dan dimanfaatkan oleh penjahat dunia maya, sehingga memperbarui perangkat lunak di perangkat Anda akan membantu melindungi Anda dari serangan dunia maya.

Bagaimana cara menyiapkan pembaruan otomatis?

Pembaruan otomatis adalah pengaturan default atau 'tetapkan dan lupakan' yang menginstal pembaruan baru segera saat tersedia.

- ✓ **Aktifkan dan konfirmasi pembaruan otomatis** pada semua perangkat lunak dan perangkat.
- ✓ **Cara mengaktifkan pembaruan otomatis dapat berbeda** tergantung pada perangkat lunak dan perangkat.



- ✓ **Tetapkan waktu yang tidak menyulitkan untuk pembaruan otomatis** jika memungkinkan, seperti saat Anda tidur atau biasanya tidak menggunakan perangkat.
- ✓ **Perangkat Anda harus aktif**, dicolokkan ke daya, dan memiliki ruang penyimpanan yang tidak terpakai.



Jika Anda menerima permintaan untuk memperbarui perangkat lunak perangkat Anda, Anda harus melakukannya sesegera mungkin.



Keamanan Dunia Maya Pribadi: Langkah Pertama



Bagaimana jika pengaturan pembaruan otomatis tidak tersedia?

Jika pengaturan pembaruan otomatis tidak tersedia, Anda harus secara teratur memeriksa dan menginstal pembaruan baru melalui menu pengaturan perangkat lunak atau perangkat Anda.

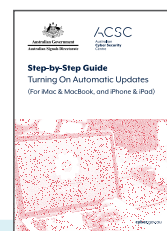
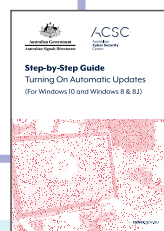
BAGAIMANA JIKA PERANGKAT DAN PERANGKAT LUNAK LAMA SAYA TIDAK MENDAPATKAN PEMBARUAN APA PUN?

Jika perangkat, sistem operasi, atau perangkat lunak Anda terlalu lama, perangkat tersebut mungkin sudah tidak didukung oleh produsen atau pengembang.

Ketika produk mencapai masa 'akhir dukungan' tersebut, produk tidak akan lagi mendapatkan pembaruan, sehingga Anda rentan terhadap serangan dunia karena adanya 'bug' perangkat lunak yang telah diketahui. Contoh produk yang telah masuk akhir dukungan adalah sistem operasi Windows 7 dan iPhone 6.

Jika perangkat, sistem operasi, atau perangkat lunak Anda telah mencapai akhir dukungan, ACSC menyarankan untuk meningkatkannya sesegera mungkin agar tetap aman.

Untuk informasi selengkapnya, baca panduan *Cepat Tanggap dari ACSC tentang Akhir Dukungan* yang tersedia di [cyber.gov.au](https://www.cyber.gov.au).



Untuk informasi selengkapnya tentang cara mengaktifkan pembaruan otomatis, baca panduan *Langkah demi Langkah* dari ACSC yang tersedia di [cyber.gov.au](https://www.cyber.gov.au):

Mengaktifkan Pembaruan Otomatis
(Untuk Microsoft Windows 10 dan Windows 8 & 8.1)

Mengaktifkan Pembaruan Otomatis (Untuk iMac & MacBook, serta iPhone & iPad)



Mengaktifkan Autentikasi Multifaktor (MFA)

Apa itu MFA?

Anda dapat menggunakan autentikasi multifaktor (MFA) untuk meningkatkan keamanan akun terpenting Anda. MFA mengharuskan Anda untuk membuat kombinasi dua jenis autentikasi berikut atau lebih sebelum memberikan akses ke akun:

- **sesuatu yang Anda ketahui** (misalnya PIN, kata sandi, atau frasa sandi);
- **sesuatu yang Anda miliki** (misalnya kartu pintar, token fisik, aplikasi autentikator, SMS atau email); dan
- **sesuatu yang menjadi identitas Anda** (misalnya sidik jari, pengenalan wajah, atau pemindaian iris).

MFA mempersulit penjahat dunia maya untuk mendapatkan akses awal ke akun Anda dengan menambahkan lebih banyak lapisan autentikasi, yang memerlukan waktu, upaya, dan sumber daya ekstra untuk dipecahkan.

Autentikasi dua faktor (2FA) adalah jenis MFA paling umum, yang membutuhkan dua jenis autentikasi yang berbeda.



BAGAIMANA CARA MENGAKTIFKAN 2FA UNTUK MELINDUNGI AKUN SAYA YANG PALING PENTING?

Anda harus mengaktifkan 2FA sekarang, dimulai dengan akun penting Anda:

- ✓ Semua akun perbankan dan keuangan online (misalnya bank Anda, PayPal)
- ✓ Semua akun email (misalnya Gmail, Outlook, Hotmail, Yahoo!)

Jika Anda memiliki banyak akun email, prioritaskan akun yang terhubung dengan perbankan online atau layanan penting lainnya.

Langkah-langkah untuk mengaktifkan 2FA berbeda-beda tergantung pada akun, perangkat, atau aplikasi perangkat lunak.

Untuk informasi selengkapnya tentang cara mengaktifkan 2FA di akun penting Anda, baca panduan *Langkah demi Langkah* dari ACSC yang tersedia di [cyber.gov.au](https://www.cyber.gov.au) atau kunjungi situs web penyedia akun Anda.



Mencadangkan Perangkat Anda secara Berkala

Apa itu cadangan?

Cadangan adalah salinan digital dari informasi terpenting Anda (misalnya foto, informasi keuangan, atau catatan) yang telah Anda simpan ke perangkat penyimpanan eksternal atau ke cloud.

Pencadangan adalah tindakan pencegahan agar informasi Anda dapat dipulihkan jika hilang, dicuri, atau rusak.

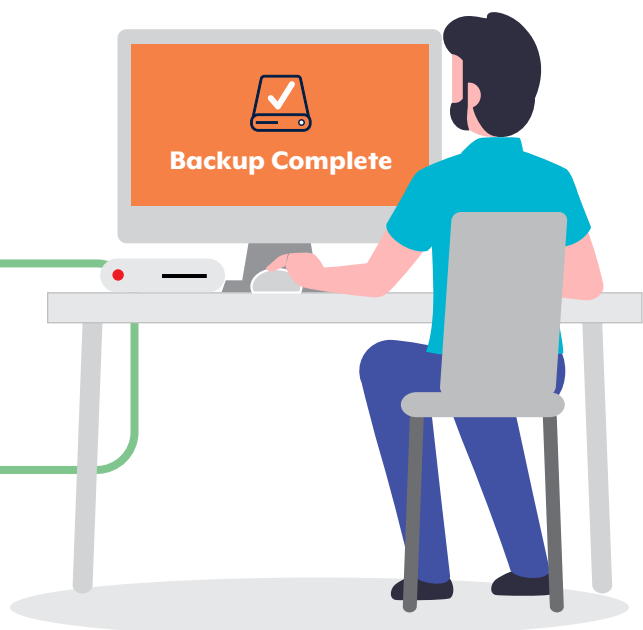
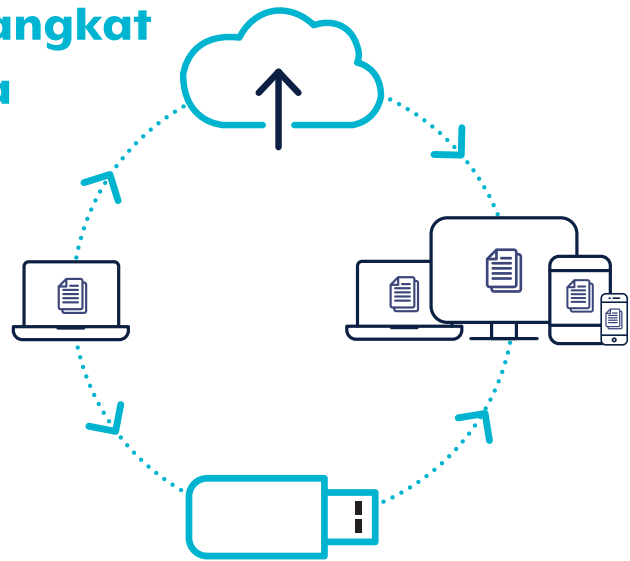
Bagaimana cara mencadangkan perangkat dan file saya?

Anda harus mencadangkan file dan perangkat Anda secara berkala.

Pada akhirnya, cara pencadangan dilakukan, baik secara harian, mingguan, atau bulanan, itu tergantung keputusan Anda. Frekuensi pencadangan dapat bergantung pada jumlah:

- **file baru** yang Anda masukkan ke perangkat Anda,
- **perubahan** yang Anda terapkan pada file, dan
- file yang **ingin Anda singkirkan**.

ACSC menyarankan Anda untuk memeriksa cadangan Anda secara berkala, sehingga Anda terbiasa dengan proses pemulihan dan memastikan cadangan Anda berfungsi dengan baik.



Untuk informasi selengkapnya tentang mencadangkan ke perangkat penyimpanan eksternal dan cloud, baca panduan *Langkah demi Langkah* dari ACSC yang tersedia di [cyber.gov.au](https://www.cyber.gov.au):

UNTUK PC:

- Mencadangkan dan Memulihkan File Anda – Untuk PC (Ke Cloud)
- Mencadangkan dan Memulihkan File Anda – Untuk PC (Menggunakan Perangkat Penyimpanan Eksternal)

UNTUK MAC:

- Mencadangkan dan Memulihkan File Anda – Untuk Mac (Ke Cloud)
- Mencadangkan dan Memulihkan File Anda – Untuk Mac (Menggunakan Perangkat Penyimpanan Eksternal)

UNTUK IOS:

- Mencadangkan dan Memulihkan File Anda – Untuk iPhone (Ke Cloud)



Menggunakan Frasa Sandi untuk Mengamankan Akun Penting Anda

Autentikasi multifaktor (MFA) (lihat halaman 4) adalah salah satu cara paling efektif untuk melindungi akun Anda dari penjahat dunia maya. **Jika MFA tidak tersedia**, frasa sandi yang kuat dan unik dapat lebih melindungi akun Anda dibandingkan dengan sebuah kata sandi sederhana.

Apa itu frasa sandi?

Frasa sandi menggunakan empat kata acak atau lebih sebagai kata sandi Anda.

Misalnya: 'kristal bombai tanah pretzel'.

- **Frasa sandi lebih aman** daripada kata sandi sederhana.
- Frasa sandi **sulit untuk dipecahkan** oleh penjahat dunia maya, tetapi **mudah untuk Anda** ingat.

BAGAIMANA CARA MEMBUAT FRASA SANDI?

Buat frasa sandi yang:

- **Panjang:** minimal 14 karakter, menggunakan empat kata acak atau lebih. Semakin panjang frasa sandi Anda, semakin aman frasa sandi itu.
- **Tidak dapat diprediksi:** gunakan campuran empat kata acak atau lebih yang tidak berkaitan. Jangan pakai frasa, kutipan, atau lirik terkenal.
- **Unik:** tidak digunakan kembali di beberapa akun.

Jika situs web atau layanan mewajibkan kata sandi rumit yang berisi simbol, huruf kapital, atau angka, Anda dapat memasukkannya ke dalam frasa sandi Anda. Frasa sandi Anda harus tetap panjang, tidak dapat diprediksi, dan unik demi keamanan terbaik.



Akun mana yang harus saya amankan dengan frasa sandi?

Jika akun Anda yang paling penting tidak dilindungi dengan MFA (lihat halaman 4), ubah kata sandi Anda menjadi frasa sandi yang unik dan kuat, dimulai dengan:

- ✓ **Akun perbankan dan keuangan online**
- ✓ **Akun email**

Jika Anda memiliki banyak akun email, prioritaskan akun yang terhubung dengan perbankan online atau layanan penting lainnya.

Anda biasanya dapat mengubah sandi menjadi frasa sandi yang unik dan kuat melalui menu pengaturan akun.

“Ingat: Jangan pernah menggunakan kembali frasa sandi di beberapa akun.”

Untuk saran selengkapnya tentang cara membuat frasa sandi yang kuat, lihat panduan *Membuat Frasa Sandi yang Kuat* dari ACSC yang tersedia di cyber.gov.au.

Keamanan Dunia Maya Pribadi: Langkah Pertama



Mengamankan Perangkat Seluler Anda

Saat ini, ponsel pintar dan tablet digunakan untuk terhubung, berbelanja, bekerja, melakukan aktivitas perbankan, meneliti, melacak kemampuan kita, dan menyelesaikan banyak tugas lainnya kapan saja dan dari mana saja.

Apa yang dapat terjadi jika perangkat seluler saya dibobol, hilang, atau dicuri?

- Perangkat itu dapat digunakan oleh penjahat dunia maya untuk mencuri uang atau identitas Anda, menggunakan informasi yang tersimpan di perangkat Anda termasuk akun media sosial dan email.
- Anda dapat kehilangan data yang tidak tergantikan seperti foto, catatan, atau pesan (jika tidak dicadangkan).
- Seorang penjahat dunia maya dapat menggunakan nomor telepon Anda untuk menipu orang lain.



BAGAIMANA CARA MENGAMANKAN PERANGKAT SELULER SAYA?

KEAMANAN PERANGKAT:

- ✓ **Kunci** perangkat Anda dengan frasa sandi, kata sandi, PIN, atau kode sandi. Buatlah sulit ditebak - tanggal lahir dan kunci pola Anda mudah ditebak oleh penjahat dunia maya. Gunakan frasa sandi untuk keamanan optimal (lihat halaman 6). Anda juga dapat mempertimbangkan penggunaan pengenalan wajah atau sidik jari untuk membuka kunci perangkat Anda.
- ✓ **Pastikan** perangkat Anda diatur untuk mengunci secara otomatis setelah beberapa saat tidak aktif.
- ✓ **Jangan** mengisi daya perangkat Anda di tempat pengisian daya umum dan hindari pengisian daya dari pihak ketiga.
- ✓ **Perlakukan** ponsel Anda seperti dompet Anda. Simpan dengan aman dan bawa ke mana Anda pergi setiap saat.

KEAMANAN PERANGKAT LUNAK DAN APLIKASI:

- ✓ **Gunakan** fitur pembaruan otomatis perangkat Anda untuk menginstal pembaruan aplikasi dan sistem operasi baru segera saat tersedia (lihat halaman 5).

- ✓ **Atur** perangkat untuk meminta frasa sandi/kata sandi sebelum aplikasi diinstal. Kontrol orang tua juga dapat digunakan untuk tujuan ini.
- ✓ **Periksa** izin privasi dengan cermat saat menginstal aplikasi baru di perangkat Anda, terutama untuk aplikasi gratis. Hanya instal aplikasi dari vendor tepercaya.

KEAMANAN DATA:

- ✓ **Aktifkan** fungsi penguncian dan penghapusan jarak jauh jika perangkat Anda mendukungnya.
- ✓ **Pastikan** Anda benar-benar menghapus data pribadi dari perangkat Anda sebelum menjual atau membuangnya.

KEAMANAN KONEKTIVITAS:

- ✓ **Nonaktifkan** Bluetooth dan Wi-Fi saat Anda tidak menggunakannya.
- ✓ **Pastikan** perangkat Anda tidak terhubung secara otomatis ke jaringan Wi-Fi baru.



Mengembangkan Pemikiran Keamanan Dunia Maya Anda

Keamanan dunia maya pribadi bukan hanya berkaitan dengan mengubah pengaturan, tetapi berkaitan juga dengan mengubah pemikiran dan perilaku Anda.

Hati-Hati dengan Penipuan Dunia Maya

Penjahat dunia maya diketahui menggunakan email, pesan, media sosial, atau panggilan telepon untuk mencoba menipu warga Australia. Mereka mungkin berpura-pura menjadi individu atau organisasi yang sepertinya Anda tahu, atau menurut Anda harus dipercaya.

Pesan dan panggilan mereka mencoba mengelabui Anda agar melakukan tindakan tertentu, seperti:

- **Mengungkap detail rekening bank, kata sandi, dan nomor kartu kredit**
- **Memberikan akses jarak jauh ke komputer Anda**
- **Membuka lampiran, yang mungkin berisi malware**
- **Mengirim uang atau kartu hadiah**

BAGAIMANA CARA MENGENALI PESAN PENIPUAN?

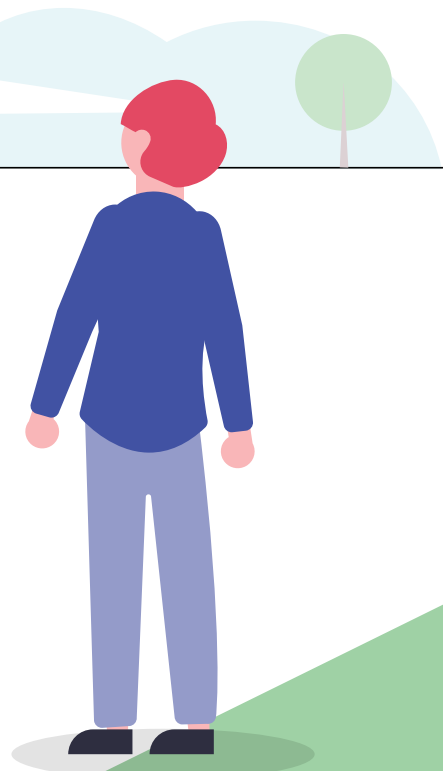
Mungkin sulit untuk mengenali pesan penipuan.

Penjahat dunia maya sering menggunakan teknik tertentu untuk mengelabui Anda. Pesan mereka mungkin berisi:

- **Otoritas** – Apakah pesan tersebut mengaku dari pihak resmi, seperti bank Anda?
- **Urgensi** – Apakah Anda diberi tahu ada masalah, atau waktu Anda untuk merespons atau membayar terbatas?
- **Emosi** – Apakah pesan tersebut membuat Anda panik, berharap, atau penasaran?
- **Kelangkaan** – Apakah pesan tersebut menawarkan sesuatu yang terbatas, atau menjanjikan kesepakatan yang bagus?
- **Peristiwa terkini** – Apakah pesan tersebut terkait dengan berita terkini atau peristiwa besar?

Untuk mempelajari selengkapnya tentang cara mengenali pesan phishing atau penipuan, ikuti kuis di situs web ACSC [cyber.gov.au](https://www.cyber.gov.au).

“Pesan penipuan dapat dikirim ke ribuan orang, atau menargetkan satu orang tertentu.”



Keamanan Dunia Maya Pribadi: Langkah Pertama

Apa yang harus saya lakukan jika saya mendapatkan pesan penipuan?

Jika Anda menerima pesan atau panggilan telepon penipuan, Anda harus mengabaikan, menghapus, atau melaporkannya ke Scamwatch ACCC di scamwatch.gov.au

Anda juga dapat menghubungi Saluran Siaga Keamanan Dunia Maya ACSC di **1300 CYBER1** (1300 292 371) jika Anda khawatir tentang keamanan dunia maya Anda.

Jika Anda terlibat dengan penipuan dan merasa rekening bank, kartu kredit, atau kartu debit Anda berisiko, segera hubungi lembaga keuangan Anda. Mereka mungkin dapat menutup akun Anda atau menghentikan transaksi.

Bagaimana jika saya tidak yakin apakah sebuah pesan berisi penipuan?

Jika Anda merasa sebuah pesan atau panggilan mungkin benar-benar berasal dari organisasi yang Anda percayai (seperti bank Anda), cari metode kontak yang dapat Anda percayai. Cari situs web resmi, hubungi nomor telepon yang diiklankan, atau kunjungi toko fisik atau cabang. Jangan gunakan tautan atau detail kontak dalam pesan yang dikirim kepada Anda atau diberikan melalui telepon karena itu bisa jadi penipuan.

Berpikirlah Sebelum Anda Mengklik

- ✓ **Berpikirlah sebelum Anda mengklik tautan di email, situs web, dan SMS.**
- ✓ **Selalu curigai lampiran yang Anda terima.**
- ✓ **Jika browser Anda memberi tahu Anda bahwa situs web tidak aman, segera tutup.**
- ✓ **Ingat: Tenaga TI, departemen pemerintah, atau perusahaan tidak akan menghubungi Anda dan menanyakan detail login Anda.**

Jika Anda merasa menjadi korban kejahatan dunia maya, laporkan melalui ReportCyber ACSC di cyber.gov.au atau hubungi Saluran Siaga Keamanan Dunia Maya kami di 1300 CYBER1 (1300 292 371).

Perbarui pengetahuan tentang ancaman terbaru: Daftar ke layanan peringatan online gratis dari ACSC di cyber.gov.au yang akan mengirim Anda peringatan saat kami mengidentifikasi ancaman dunia maya baru.

Luangkan Waktu untuk Berpikir Sebelum Anda Berbagi di Media Sosial

Berpikirlah sebelum Anda berbagi di internet!

Penjahat dunia maya dapat menggunakan informasi yang telah Anda posting secara publik di akun media sosial Anda dalam penipuan dan serangan dunia maya mereka.

Ingat, internet bersifat permanen dan Anda tidak akan pernah dapat sepenuhnya menghapus apa yang telah diposting.

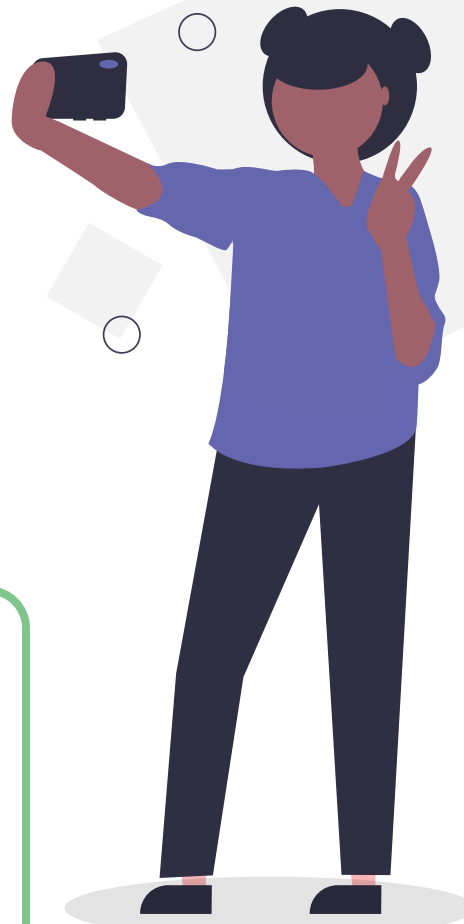
Bagaimana cara meluangkan waktu untuk berpikir sebelum memposting?

- **Pikirkan:** Bagaimana penjahat dunia maya dapat menggunakan informasi ini untuk mengincar saya atau akun saya?
- **Pikirkan:** Apakah saya merasa nyaman menunjukkan informasi atau gambar ini kepada orang asing secara offline?

INFORMASI APA YANG SEHARUSNYA TIDAK SAYA BAGIKAN?

Hindari berbagi informasi (termasuk foto) secara online yang dapat digunakan oleh penjahat dunia maya untuk: mengidentifikasi Anda, memanipulasi Anda melalui penipuan, atau mengetahui jawaban pertanyaan pemulihan akun Anda. Hal ini mungkin termasuk:

- **Tempat lahir dan tanggal lahir**
- **Alamat dan nomor telepon**
- **Perusahaan dan riwayat kerja**
- **Tempat Anda bersekolah**
- **Informasi pribadi lainnya** yang dapat digunakan untuk mengincar Anda



Daftar Periksa Ringkasan



Apakah Anda telah menyelesaikan seluruh panduan ini?

Gunakan daftar periksa praktis ini untuk melacak kemajuan Anda:

- ✓ **Saya telah mengaktifkan pembaruan otomatis untuk semua perangkat saya:**
 - Komputer (desktop dan laptop)
 - Ponsel
 - Tablet
- ✓ **Saya telah mengaktifkan autentikasi multifaktor pada akun saya yang paling penting:**
 - Semua akun perbankan dan keuangan online saya (misalnya bank Anda, PayPal)
 - Semua akun email (misalnya Gmail, Outlook, Hotmail, Yahoo!)
- ✓ **Saya mencadangkan perangkat saya secara berkala:**
 - Komputer (desktop dan laptop)
 - Ponsel
 - Tablet
- ✓ **Saya menggunakan frasa sandi yang unik dan kuat pada akun terpenting saya yang tidak dilindungi oleh MFA:**
 - Akun perbankan dan keuangan online
 - Akun email
- ✓ **Saya telah mengamankan perangkat seluler saya:**
 - Laptop
 - Ponsel
 - Tablet
- ✓ **menggunakan pemikiran keamanan dunia maya setiap hari:**
 - Saya dapat mengenali pesan penipuan
 - Saya tahu apa yang harus saya lakukan jika saya menerima pesan penipuan
 - Saya tahu cara memeriksa apakah sebuah pesan berisi penipuan jika saya tidak yakin
 - Saya berpikir sebelum saya mengeklik tautan dan lampiran
 - Saya berpikir sebelum membagikan sesuatu di media sosial
- ✓ **Saya tahu tempat meminta bantuan jika saya menjadi korban kejahatan dunia maya atau penipuan**



Daftar Istilah

Pemulihan akun

Sebuah proses di mana serangkaian pertanyaan atau metode verifikasi lainnya digunakan untuk memulihkan atau mendapatkan kembali akses ke akun atau untuk mengubah frasa sandi/kata sandi akun.

Aplikasi

Juga disebut sebagai aplikasi seluler, aplikasi adalah istilah untuk perangkat lunak yang biasa digunakan untuk smartphone atau tablet.

Lampiran

File yang dikirim bersama pesan email.

Aplikasi autentikator

Aplikasi yang digunakan untuk mengonfirmasi identitas pengguna komputer guna mengizinkan akses melalui autentikasi multifaktor (MFA).

Cloud

Jaringan server jarak jauh yang menyediakan kecanggihan penyimpanan dan pemrosesan yang sangat besar dan terdistribusi.

Penjahat dunia maya

Setiap individu yang secara ilegal mengakses sistem komputer atau akun untuk merusak atau mencuri informasi.

Perangkat

Perangkat komputasi atau komunikasi. Misalnya, komputer, laptop, ponsel, atau tablet.

Akhir dukungan

Akhir dukungan mengacu pada situasi di mana perusahaan menghentikan dukungan untuk produk atau layanan. Hal ini biasanya diterapkan pada produk perangkat keras dan perangkat lunak ketika perusahaan merilis versi baru dan mengakhiri dukungan untuk versi sebelumnya.

Malware

Perangkat lunak berbahaya yang digunakan untuk mendapatkan akses dan kontrol tidak sah atas komputer pengguna, mencuri informasi, dan mengganggu atau menonaktifkan jaringan.

Sistem operasi

Perangkat lunak yang diinstal pada hard drive komputer yang memungkinkan perangkat keras komputer untuk berkomunikasi dengan dan menjalankan program komputer. Contoh: Microsoft Windows, Apple macOS, iOS, Android.

Token fisik

Perangkat fisik yang biasanya dapat masuk ke gantungan kunci, yang mengeluarkan kode keamanan yang digunakan untuk mengonfirmasi identitas pengguna komputer yang menggunakan MFA.

Akses jarak jauh

Mendapatkan akses dan kontrol atas perangkat dan jaringan dari lokasi jarak jauh.

Perangkat lunak

Biasanya disebut sebagai program, kumpulan instruksi yang memungkinkan pengguna untuk berinteraksi dengan komputer, perangkat kerasnya, atau melakukan tugas.

PANDUAN BERIKUTNYA DALAM SERI KEAMANAN DUNIA MAYA PRIBADI

Karena Anda telah menyelesaikan *Keamanan Dunia Maya Pribadi: Panduan Langkah Pertama* dari ACSC, Anda harus memulai *Keamanan Dunia Maya Pribadi: panduan Langkah Berikutnya*, yang tersedia di cyber.gov.au.

Keamanan Dunia Maya Pribadi: Panduan Langkah Berikutnya menguraikan tindakan yang dapat Anda lakukan saat ini untuk lebih meningkatkan keamanan dunia maya Anda.



Penafian

Materi dalam panduan ini bersifat umum dan tidak boleh dianggap sebagai nasihat hukum atau dijadikan dasar bantuan dalam keadaan atau situasi darurat tertentu apa pun. Dalam segala hal yang penting, Anda harus mencari nasihat profesional independen yang sesuai sehubungan dengan keadaan Anda sendiri.

Commonwealth of Australia tidak bertanggung jawab atau berkewajiban atas kerusakan, kehilangan, atau biaya apa pun yang timbul sebagai akibat dari mengandalkan informasi yang tercantum dalam panduan ini.

Hak cipta

© Commonwealth of Australia 2021

Selain Lambang Negara dan jika dinyatakan lain, semua materi yang disajikan dalam publikasi ini disediakan di bawah lisensi Creative Commons Attribution 4.0 International (www.creativecommons.org/licenses).

Untuk menghindari keraguan, ini berarti bahwa lisensi ini hanya berlaku pada materi seperti yang tercantum dalam dokumen ini.



Detail ketentuan lisensi yang relevan tersedia di situs web Creative Commons sebagaimana pedoman hukum lengkap untuk lisensi CC BY 4.0 (www.creativecommons.org/licenses).

Penggunaan Lambang Negara

Ketentuan yang menjadi dasar dibolehkannya penggunaan Lambang Negara dijelaskan di situs web Department of the Prime Minister and Cabinet (www.pmc.gov.au/government/commonwealth-coat-arms).

Untuk informasi selengkapnya, atau untuk melaporkan insiden keamanan dunia maya, hubungi kami:
cyber.gov.au | 1300 CYBER1 (1300 292 371)



Australian Government
Australian Signals Directorate

ACSC Australian
Cyber Security
Centre