Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

CARA MENGGUNAKAN INTERNET DENGAN AMAN

PANDUAN BAGI LANSIA

cyber.gov.au

Pendahuluan

Dengan online, Anda dapat tetap berhubungan dengan teman dan keluarga, mempelajari berbagai topik, dan bahkan bermain game.

Sama seperti memasang sabuk pengaman sebelum berkendara, sebaiknya lakukan langkah-langkah ini sebelum menggunakan internet agar lebih aman.

Australian Cyber Security Centre (ACSC) ingin memastikan semua orang aman saat mereka online. Dokumen ini mencakup beberapa praktik keamanan dunia maya dasar yang dapat Anda terapkan untuk melindungi diri Anda sendiri saat mengakses internet.

Australian Cyber Security Centre (ACSC), sebagai bagian dari Australian Signals Directorate (ASD), memberikan saran, bantuan, dan tanggapan operasional guna 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 cyber.gov.au

Keamanan dunia maya bagi lansia

Kiat 1: Perbarui perangkat Anda

Memperbarui perangkat lunak Anda seperti menyervis mobil Anda. Ini meningkatkan kinerja perangkat Anda dan membuatnya lebih aman.

Penjahat dunia maya selalu menemukan cara baru untuk meretas perangkat. Mengatur perangkat Anda agar secara otomatis menginstal pembaruan dapat memperbaiki kelemahan apa pun di perangkat lunak Anda dan mencegah peretas.

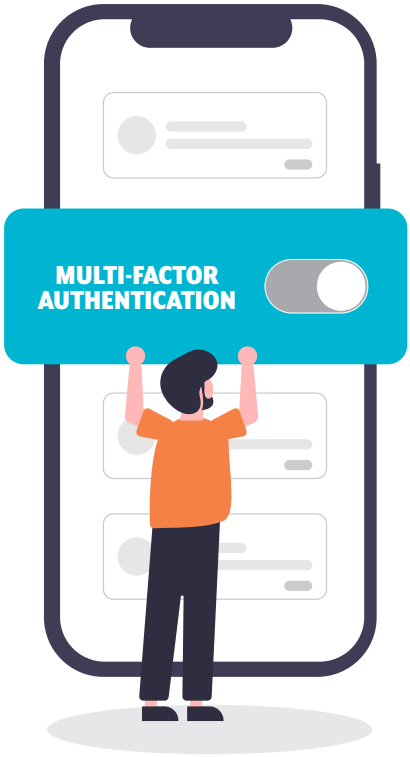
Untuk menemukan panduan langkah demi langkah dari kami tentang cara mengaktifkan pembaruan otomatis:

1. Buka **cyber.gov.au**
2. Klik **Individu & keluarga**
3. Klik **Panduan Langkah demi Langkah**
4. Cari **Mengaktifkan Pembaruan Otomatis**
5. Pilih antara perangkat Apple atau Windows.

TAHUKAH ANDA:

Pembaruan juga akan menambahkan fitur baru ke perangkat Anda dan menjadikannya berjalan lebih cepat.

Kiat 2: Aktifkan autentikasi multifaktor



Autentikasi multifaktor di akun Anda seperti layar keamanan di rumah Anda. Ini melindungi Anda dari penjahat yang mencoba masuk.

Dengan autentikasi multifaktor yang diaktifkan, Anda perlu untuk memberikan beberapa jenis informasi untuk mendapatkan akses ke akun Anda. Misalnya, Anda mungkin perlu memasukkan kata sandi dan kode pesan teks untuk login ke profil media sosial Anda.

Banyaknya lapisan akan mempersulit penjahat dunia maya untuk meretas. Mereka mungkin berhasil membobol satu bagian, seperti kata sandi Anda, tetapi mereka masih perlu mendapatkan bagian lain dari puzzle untuk mengakses akun Anda.

Untuk menemukan panduan langkah demi langkah dari kami tentang cara mengaktifkan pembaruan otomatis:

1. Buka **cyber.gov.au**
2. Klik **Individu & keluarga**
3. Klik **Panduan Langkah demi Langkah**
4. Cari **Mengaktifkan Autentikasi Dua Faktor**
5. Pilih panduan untuk jenis akun Anda (misalnya Facebook, Gmail, atau Apple ID).

INGAT:

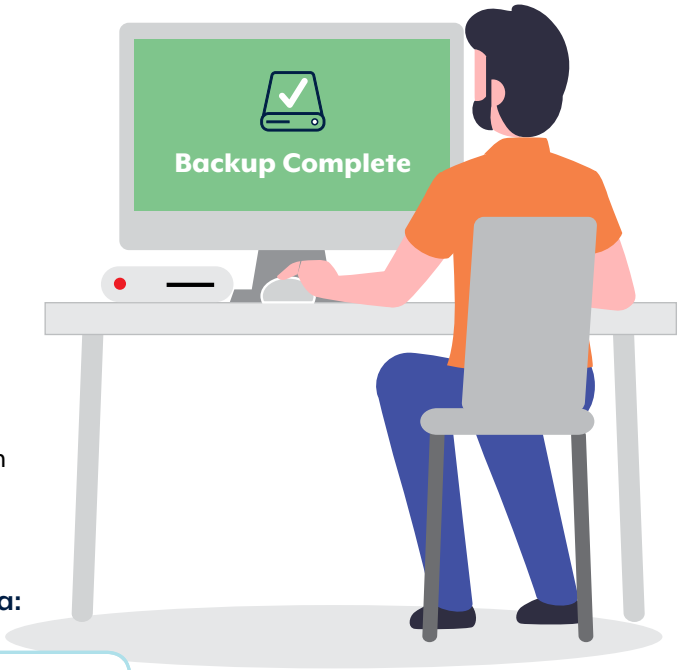
Jika Anda memerlukan bantuan untuk mengaktifkan autentikasi multifaktor, mintalah bantuan teman atau anggota keluarga.

Kiat 3: Cadangkan perangkat Anda

Melakukan 'pencadangan' adalah ketika Anda membuat salinan file penting dan menyimpannya di tempat yang aman. Ini seperti memfotokopi foto-foto berharga untuk disimpan di brankas jika Anda kehilangan yang asli.

Saat Anda mencadangkan komputer, ponsel, atau tablet, salinan file Anda disimpan secara online atau ke perangkat terpisah. Memiliki cadangan dari file penting dan foto berharga Anda akan membuat Anda tenang.

Jika ada yang tidak beres dengan perangkat Anda atau Anda diretas oleh penjahat dunia maya, Anda dapat dengan mudah memulihkan file dari cadangan Anda.



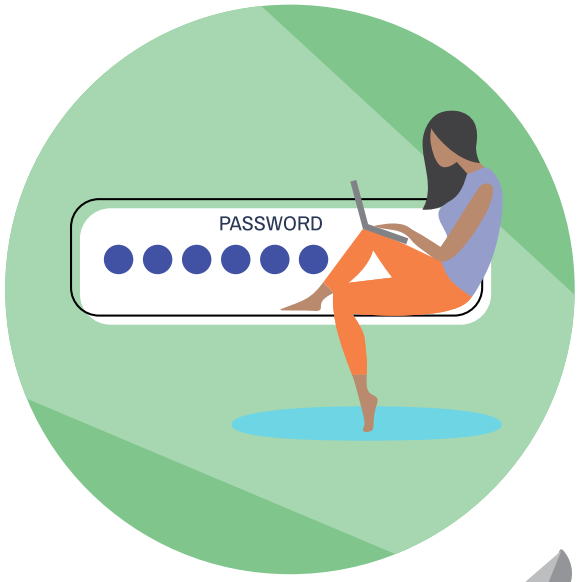
Untuk menemukan panduan langkah demi langkah dari kami tentang cara mencadangkan dan memulihkan file Anda:

1. Buka **cyber.gov.au**
2. Klik **Individu & keluarga**
3. Klik **Panduan Langkah demi Langkah**
4. Cari **Mencadangkan dan Memulihkan File Anda**
5. Pilih antara perangkat Apple atau Windows.

TAHUKAH ANDA:

Mencadangkan perangkat Anda secara berkala berarti Anda akan selalu memiliki akses ke file terbaru Anda.

Kiat 4: Gunakan frasa sandi

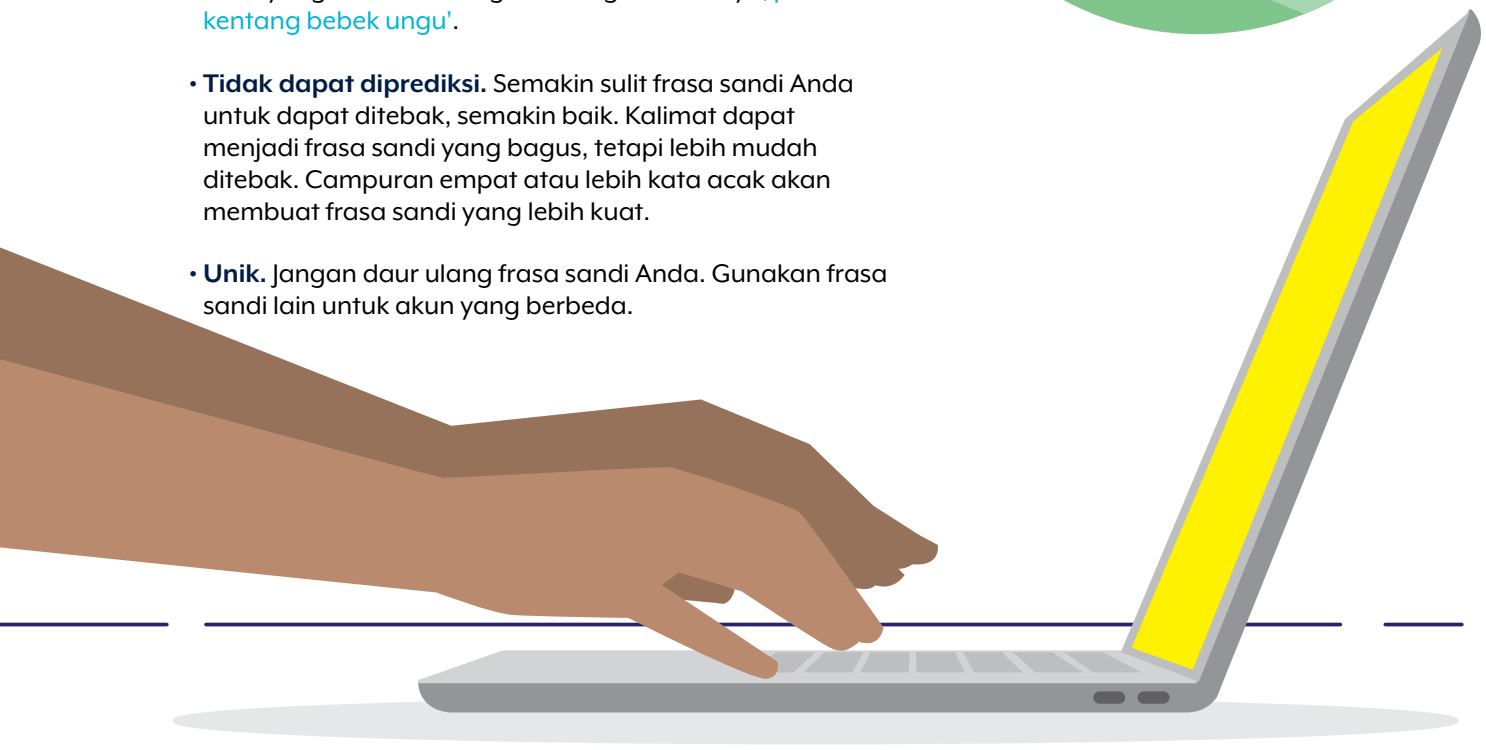


Jika kata sandi memberi gembok pada akun Anda, frasa sandi memberikan sistem keamanannya sendiri! Frasa sandi adalah versi yang lebih kuat dan lebih aman dari kata sandi.

Jika Anda tidak dapat mengaktifkan MFA, gunakan frasa sandi untuk mengamankan akun Anda. Frasa sandi menggunakan empat atau lebih kata acak sebagai kata sandi Anda. Ini menjadikan sandi sulit ditebak oleh penjahat dunia maya tetapi mudah Anda ingat.

Saat Anda membuat frasa sandi, buatlah kata sandi yang:

- **Panjang.** Semakin panjang, semakin baik. Buatlah setidaknya sepanjang 14 karakter. Empat atau lebih kata acak yang akan Anda ingat itu bagus. Misalnya,'perahu kentang bebek ungu'.
- **Tidak dapat diprediksi.** Semakin sulit frasa sandi Anda untuk dapat ditebak, semakin baik. Kalimat dapat menjadi frasa sandi yang bagus, tetapi lebih mudah ditebak. Campuran empat atau lebih kata acak akan membuat frasa sandi yang lebih kuat.
- **Unik.** Jangan daur ulang frasa sandi Anda. Gunakan frasa sandi lain untuk akun yang berbeda.



Pelajari selengkapnya tentang membuat frasa sandi yang aman di cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases

Kiat 5: Kenali dan laporkan penipuan

Semakin cepat Anda melaporkan penipuan, semakin cepat kami dapat bertindak.

Jika Anda yakin bahwa seseorang mencoba menggunakan internet untuk menipu Anda, lebih baik bersikap proaktif dan berhati-hati daripada mengambil risiko dimanfaatkan.

Jika sesuatu kedengarannya terlalu indah untuk jadi nyata, mungkin memang begitu. Meskipun sebuah pesan mungkin mengatakan Anda telah memenangkan hadiah atau bahwa komputer Anda mengandung virus, pesan itu tidak khusus untuk Anda.

Ini mungkin berasal dari penipu dan mereka ingin memanfaatkan Anda.

Kunjungi **scamwatch.gov.au** dan **cyber.gov.au** untuk melaporkan penipuan.

TAHUKAH ANDA:

Penjahat dunia maya itu licik dan mungkin menggunakan nama dan alamat email yang familier. Berhati-hatilah jika Anda:

- **diminta untuk segera membayar tagihan**
- **diminta untuk mengubah detail atau kata sandi Anda**
- **diminta untuk mengeklik tautan atau membuka lampiran.**

Kesimpulan

Sekarang setelah Anda dibekali dengan pengetahuan untuk menggunakan internet dengan lebih aman, Anda dapat menjelajah dengan percaya diri dan terus menikmati waktu online Anda.

Ingatlah, penjahat dunia maya selalu menemukan cara baru untuk menargetkan seseorang.

Tidak ada salahnya menambah pengetahuan keamanan dunia maya Anda seiring waktu dan mempelajari cara baru untuk tetap aman.

Kiat bonus

Ingin mempelajari selengkapnya tentang cara tetap aman saat online? Simak kiat-kiat berikut.

Pikirkan tentang apa yang Anda posting.

Pikirkan baik-baik informasi yang Anda bagikan secara online dan siapa yang akan melihatnya. Hanya terima permintaan pertemanan dari orang yang Anda kenal di kehidupan nyata.

Dapatkan peringatan tentang ancaman baru.

Mendaftarlah ke layanan peringatan gratis kami. Ini akan memberi tahu Anda setiap kali kami menemukan ancaman dunia maya baru.

Ini juga akan memberi Anda saran tentang apa yang harus dilakukan jika terjadi serangan.

Diskusikan mengenai keamanan dunia maya dengan keluarga dan teman.

Sekarang setelah Anda mahir dalam perkara keamanan dunia maya, bagikan apa yang telah Anda pelajari dengan keluarga dan teman Anda. Pengetahuan Anda dapat membantu mereka keluar dari situasi sulit di masa mendatang!

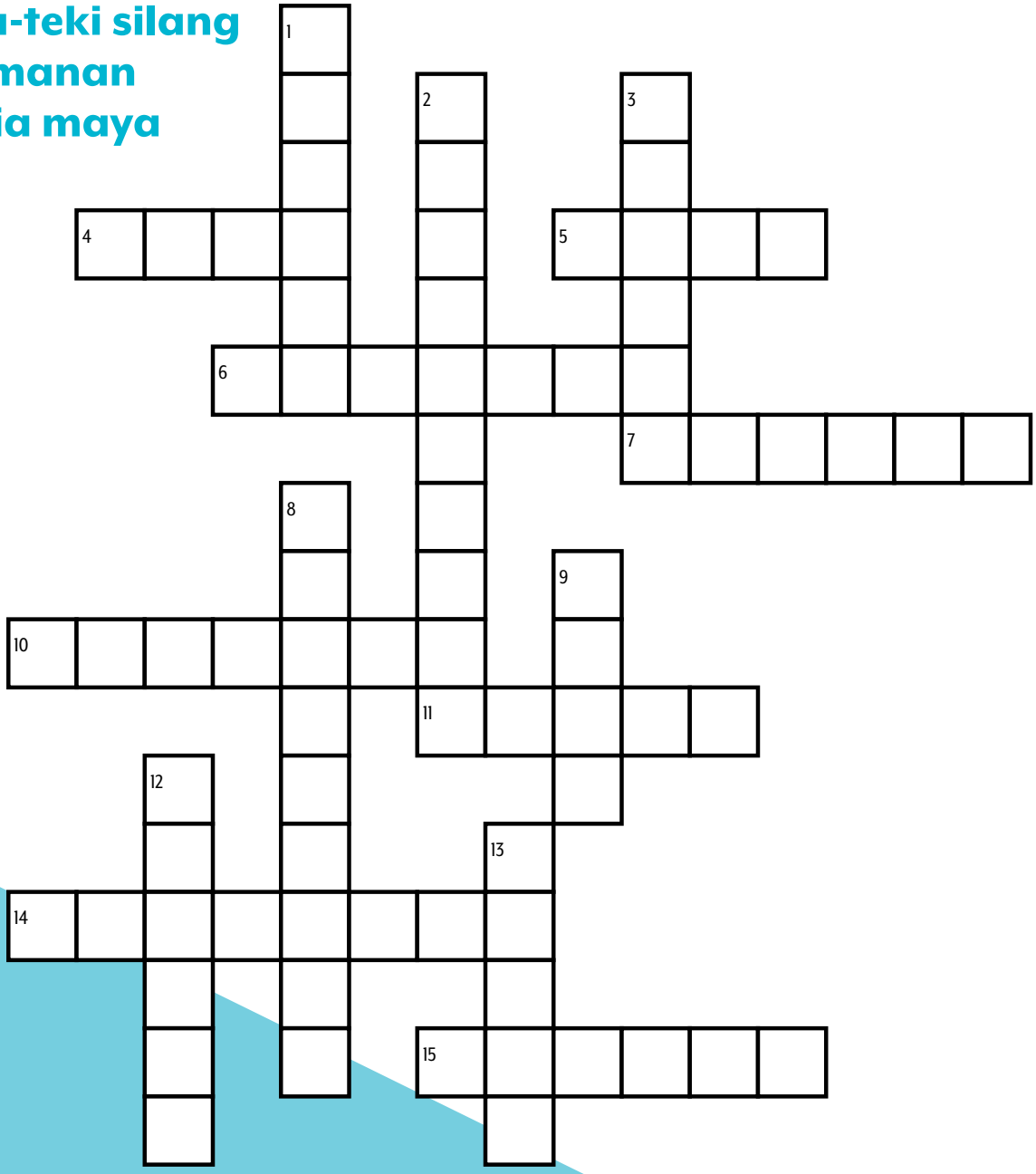
Hindari Wi-Fi publik saat Anda sedang menggunakan layanan perbankan atau berbelanja online.

Wi-Fi publik sangat cocok untuk menonton video atau membaca situs web, tetapi tetap lakukan aktivitas online apa pun yang melibatkan uang dengan koneksi internet rumah Anda. Wi-Fi publik bisa berisiko.

Laporkan kejahatan dan insiden dunia maya demi menjaga Australia tetap aman.

Jika Anda merasa telah menjadi korban kejahatan dunia maya, segeralah bertindak. Saran selengkapnya ada di cyber.gov.au

Teka-teki silang keamanan dunia maya



MENURUN

1. Tersambung ke internet
2. Kata sandi yang kuat
3. Seseorang yang menggunakan komputer untuk mencuri data
8. Perangkat lunak yang menghancurkan virus
9. Skema atau trik yang menipu
12. Salinan file komputer Anda
13. Berkaitan dengan, atau melibatkan komputer

MENDATAR

4. Teknologi jaringan nirkabel
5. Badan utama keamanan dunia maya Australia
6. Sebuah dokumen di World Wide Web
7. Untuk memberikan informasi tentang sesuatu
10. Versi perangkat lunak yang baru, lebih baik, atau lebih aman
11. Surat elektronik
14. Keadaan bebas dari bahaya atau ancaman
15. Alat yang dapat tersambung ke internet

Panduan tambahan

Untuk informasi selengkapnya, silakan lihat seri *Keamanan Dunia Maya Pribadi* kami: 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 ketiga panduan di **cyber.gov.au**

Catatan

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