Australian Government
Australian Signals Directorate

ASD 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

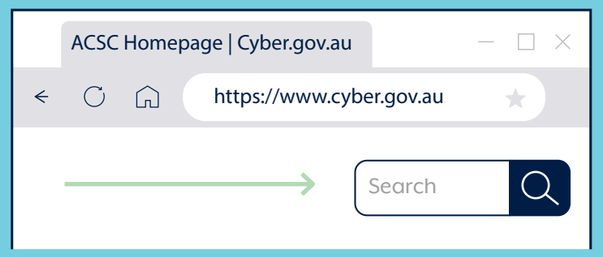
Keamanan dunia maya bagi lansia

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 informasi lebih lanjut, cari 'Updates' di cyber.gov.au



TAHUKAH ANDA:

Pembaruan juga dapat menambahkan fitur baru ke perangkat Anda dan membuatnya berjalan lebih cepat.

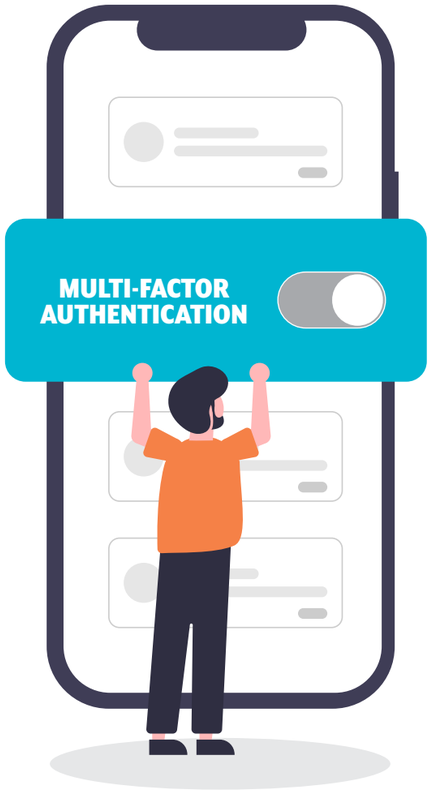
Kiat 2: Aktifkan autentikasi multifaktor

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 informasi lebih lanjut, cari 'Multi-factor authentication' atau 'MFA' di cyber.gov.au



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 informasi lebih lanjut, cari 'Backups' di cyber.gov.au

TAHUKAH ANDA:

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

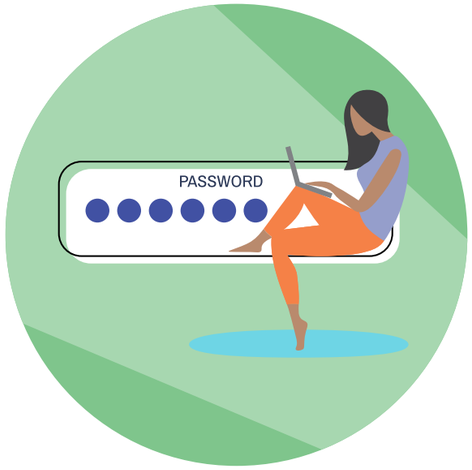
Kiat 4: Gunakan frasa sandi

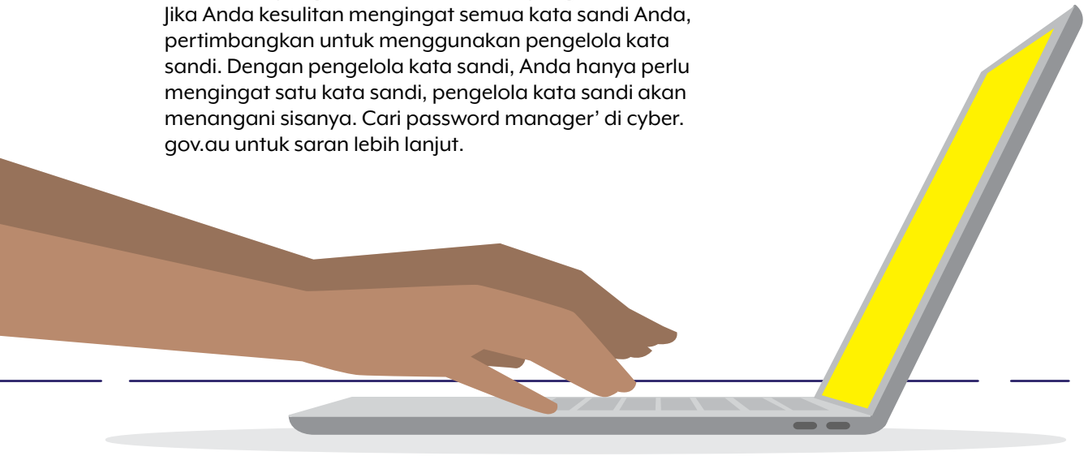
Jika kata sandi memberi gembok pada akun Anda, frasa sandi memberikan sistem keamanannya sendiri! Frasa sandi adalah versi yang lebih kuat dan lebih aman dari kata sandi.

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 mendaur ulang kata sandi Anda. Gunakan frasa sandi yang berbeda untuk akun yang berbeda. Jika Anda kesulitan mengingat semua kata sandi Anda, pertimbangkan untuk menggunakan pengelola kata sandi. Dengan pengelola kata sandi, Anda hanya perlu mengingat satu kata sandi, pengelola kata sandi akan menangani sisanya. Cari password manager' di cyber.gov.au untuk saran lebih lanjut.





Pelajari lebih lanjut tentang membuat frasa sandi yang aman dengan menelusuri 'Passphrases' di cyber.gov.au

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.

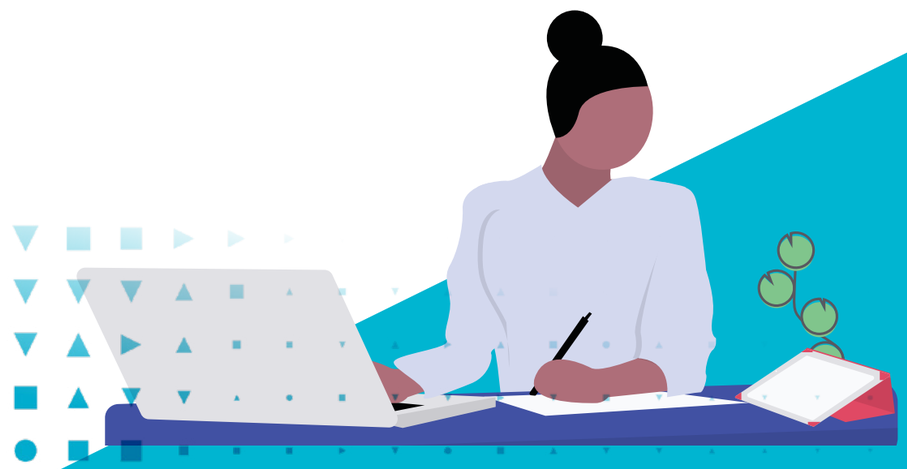
Ini mungkin berasal dari penipu dan mereka ingin memanfaatkan Anda.

Ingat, penipu sering kali berpura-pura menjadi orang atau organisasi yang Anda percayai. Waspadalah jika Anda menerima pesan yang sepertinya berasal dari seseorang yang Anda percayai, tetapi mereka menggunakan nomor telepon, alamat email, atau profil media sosial baru. Sebelum Anda menanggapi, verifikasi bahwa orang atau organisasi yang mengirim pesan kepada Anda benar-benar seperti yang mereka katakan dengan menghubungi mereka melalui saluran yang dapat Anda andalkan. Misalnya, jika Anda menerima SMS yang sepertinya berasal dari salah satu anak Anda, tetapi berasal dari nomor baru, jangan ditanggapi. Kirimi mereka pesan di media sosial untuk memeriksa apakah mereka benar-benar telah mengganti nomor teleponnya terlebih dahulu. Kunjungi scamwatch.gov.au untuk melaporkan penipuan. Jika Anda telah menjadi korban penipuan, buatlah laporan di cyber.gov.au/report.

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!

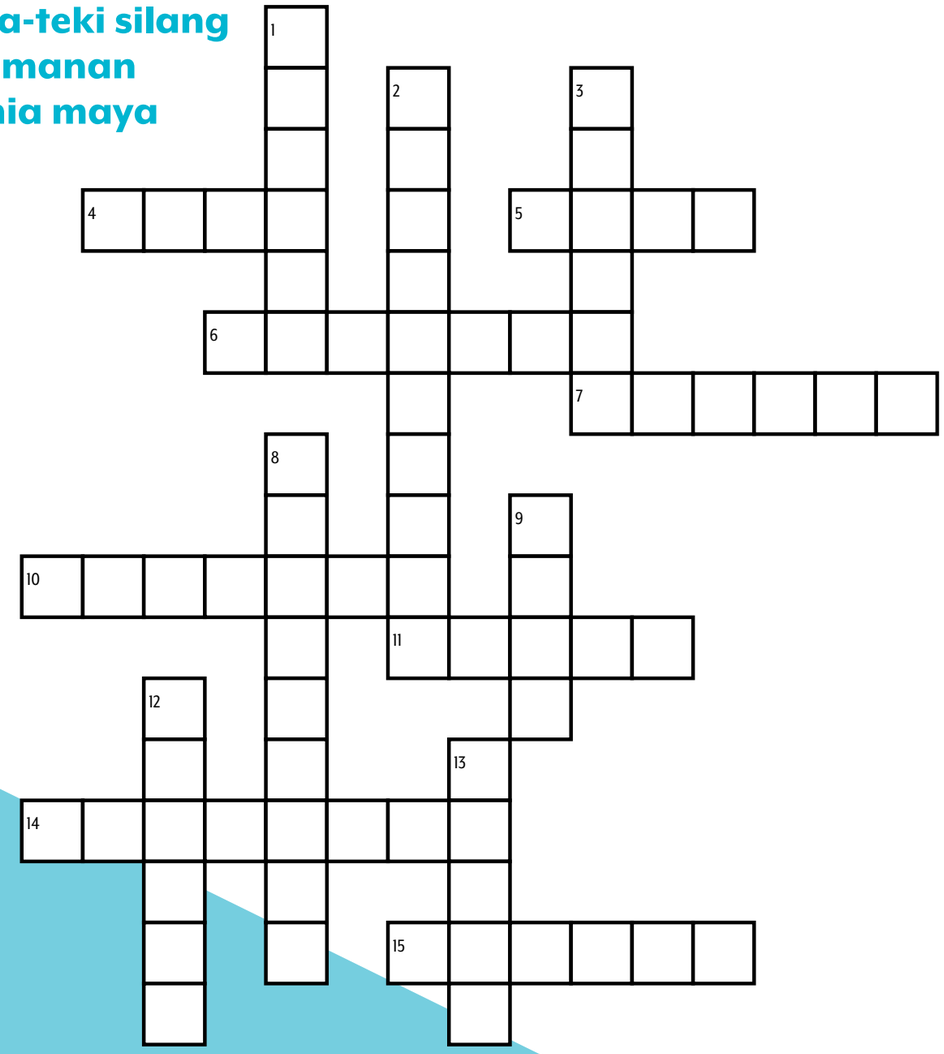
Hindari Wi-Fi publik saat Anda sedang menggunakan layanan perbankan atau berbelanja online.

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. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

MENDATAR

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the 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**

Jawaban teka-teki silang

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

Catatan

Penafian

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

Persemakmuran tidak bertanggung jawab atau berkewajiban atas kerusakan, kerugian, atau biaya apa pun yang ditimbulkan sebagai akibat dari ketergantungan pada informasi yang terkandung dalam panduan ini.

Hak cipta

© Commonwealth of Australia 2023
Dengan pengecualian Lambang Coat of Arms, kecualijika dinyatakan lain, semua materi yang disajikan dalam publikasi ini disediakan di bawah lisensi Creative Commons Attribution4.0 International (www.creativecommons.org/licenses).

Untuk menghindari ketidak-pastian, berarti lisensi ini hanya berlaku untuk materi sebagaimana diatur dalam dokumen ini.

Rincian ketentuan lisensi yang relevan tersedia di situs web Creative Commons seperti halnya kode hukum lengkap untuk lisensi CC BY 4.0 (www.creativecommons.org/licenses).

Penggunaan Lambang Coat of Arms

Persyaratan penggunaan Lambang Coat of Arms dirinci di situs web Departemen Perdana Menteri dan Kabinet (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)

Nomor ini hanya dapat digunakan di Australia.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre