Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

CARA BAGAIMANA UNTUK MENGGUNAKAN INTERNET DENGAN SELAMAT

SEBUAH PANDUAN BAGI WARGA EMAS

cyber.gov.au

Pengenalan

Melangkah ke dunia dalam talian memberi anda peluang untuk berhubung dengan kaum keluarga dan sahabat-handai, belajar tentang topik-topik yang anda minati malah bermain permainan yang anda sukai juga.

Sama seperti memasang tali pinggang keledar anda sebelum anda mula memandu, anda patut mematuhi beberapa langkah terlebih dahulu sebelum menggunakan internet supaya ia menjadi lebih selamat.

Pusat Keselamatan Siber Australia (Australian Cyber Security Centre) (ACSC) mahu memastikan keselamatan semua pengguna tatkala mereka berada dalam talian. Dokumen ini meliputi beberapa amalan keselamatan siber asas yang anda boleh gunakan untuk melindungi diri anda semasa anda mengakses internet.

Pusat Keselamatan Siber Australia (Australian Cyber Security Centre) (ACSC), sebagai sebahagian daripada Direktorat Semboyan Australia (Australian Signals Directorate) (ASD), menyampaikan nasihat, bantuan dan respons pengoperasian untuk menghalang, mengesan dan memulihkan kembali ancaman siber terhadap Australia. Pihak ACSC berada di sini untuk menolong Australia menjadi tempat yang paling selamat untuk berhubung dalam talian.

Untuk maklumat, panduan dan nasihat lanjut mengenai keselamatan siber, sila layari cyber.gov.au

Cara Bagaimana Untuk Menggunakan Internet Dengan Selamat

Keselamatan siber untuk warga emas

Petua 1: Kemaskinikan Alat Peranti anda

Mengemaskinikan perisian komputer anda adalah seperti menghantarkan kereta anda untuk diservis. Ia meningkatkan prestasi alat peranti anda dan menjadikannya lebih selamat.

Penjenayah siber senantiasa mencari kaedah baharu untuk menggodam alat-alat peranti. Sebarang kelemahan dalam perisian komputer anda boleh diperbaiki dan para penggodam boleh dikawal dengan mengaturkan agar alat peranti anda akan memasang sebarang pengemaskinian secara automatik.

Untuk mendapatkan maklumat lanjut, sila lakukan carian untuk 'Updates' pada cyber.gov.au

ADAKAH ANDA TAHU:
Pengemaskinian juga mungkin akan menambahkan ciri-ciri baru kepada alat peranti anda dan menjalankannya dengan lebih pantas.

Petua 2: Pasangkan pengesahan pelbagai-faktor

Pengesahan pelbagai-faktor pada akaun anda berfungsi sama seperti sebuah skrin keselamatan di rumah anda.
Ia melindungi anda daripada penjenayah yang ingin memecah masuk.

Bila pengesahan pelbagai-faktor diaktifkan, anda perlu memberi pelbagai jenis maklumat untuk mencapai akses kepada akaun anda. Contohnya, anda mungkin perlu memasukkan kata laluan anda serta sebuah kod pesanan teks untuk mendaftar masuk ke dalam profil media sosial anda.

Lapisan berganda ini menyukarkan penjenayah siber untuk menggodam ke dalamnya. Mereka mungkin dapat meneka sebahagian daripadanya, misalnya kata laluan anda, tetapi mereka akan masih perlu mendapatkan bahagian-bahagian lain teka-teki ini untuk mengakses akaun anda.

Untuk mendapatkan maklumat lanjut, sila lakukan carian untuk 'Multi-factor authentication' atau 'MFA' pada cyber.gov.au

INGAT:

Jika anda perlukan pertolongan untuk memasang pengesahan pelbagai-faktor, mintalah bantuan daripada seorang sahabat-handai atau ahli keluarga.

Petua 3: Buatkan salinan sandaran bagi alat peranti anda

Membuat sebuah 'salinan sandaran' berlaku bila anda membuat sebuah salinan fail-fail penting anda dan meletakkannya ke dalam satu tempat yang selamat. Ia adalah seperti membuat fotokopi gambar-gambar berharga anda untuk disimpan dalam peti besi sebagai langkah berhati-hati jika salinan asalnya hilang.

Bila anda membuat salinan sandaran bagi komputer, telefon atau tablet anda, salinan fail-fail anda akan disimpan dalam talian atau kepada sebuah alat peranti berasingan. Dengan adanya salinan sandaran fail-fail penting dan foto-foto yang dihargai anda ini, ia akan memberikan anda ketenteraman minda.

Jika sesuatu perkara yang tidak diingini berlaku dengan alat peranti anda atau anda digodam penjenayah siber, anda boleh mengembalikan fail-fail anda secara mudah daripada salinan sandaran anda.

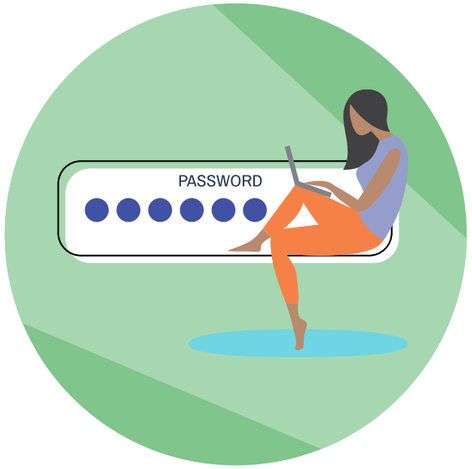
Untuk mendapatkan maklumat lanjut, sila lakukan carian untuk 'Backups' pada cyber.gov.au

ADAKAH ANDA TAHU:

Membuat salinan sandaran alat peranti anda dengan kerap **bererti anda senantiasa mempunyai akses kepada fail-fail anda yang paling terkini.**

Petua 4: Gunakan sebuah frasa laluan

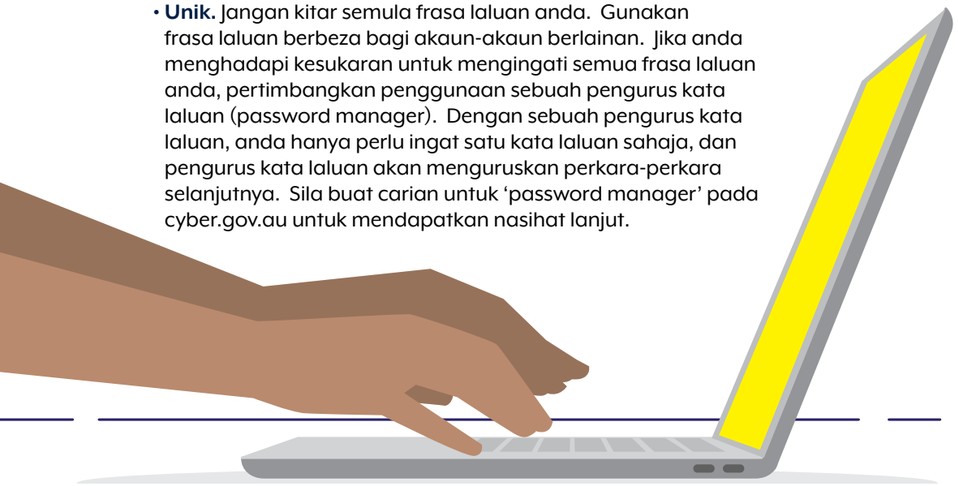
Jika sebuah kata laluan meletakkan mangga kunci pada akaun anda, sebuah kata frasa memberikannya sistem keselamatannya yang sendiri! Ia adalah versi kata laluan yang lebih kuat dan kukuh.



Jika anda tidak boleh memasang sebuah MFA, gunakan sebuah frasa laluan untuk meneguhkan akaun anda. Frasa laluan menggunakan empat perkataan rawak atau lebih sebagai kata laluan anda. Ini akan menyukarkan penjenayah siber untuk menekanya tetapi mudah bagi anda untuk mengingatinya.

Bila anda mencipta sebuah frasa laluan, pastikan ianya:

- **Panjang.** Lebih panjang, lebih baik. Sasarkan sekurang-kurangnya sepanjang 14 perkataan. Empat perkataan rawak atau lebih yang anda akan mudah ingat. Contohnya, 'ungu itik ubi kentang bot'.
- **Tidak boleh diramal.** Ia adalah jauh lebih baik untuk menggunakan frasa laluan yang tidak boleh diramalkan dengan mudah. Ayat-ayat boleh dijadikan frasa laluan yang baik, tetapi ianya lebih mudah untuk diteka. Campuran empat perkataan rawak atau lebih akan menguatkan lagi sebuah frasa laluan.
- **Unik.** Jangan kitar semula frasa laluan anda. Gunakan frasa laluan berbeza bagi akaun-akaun berlainan. Jika anda menghadapi kesukaran untuk mengingati semua frasa laluan anda, pertimbangkan penggunaan sebuah pengurus kata laluan (password manager). Dengan sebuah pengurus kata laluan, anda hanya perlu ingat satu kata laluan sahaja, dan pengurus kata laluan akan menguruskan perkara-perkara selanjutnya. Sila buat carian untuk 'password manager' pada cyber.gov.au untuk mendapatkan nasihat lanjut.



Pelajari dengan lebih lanjut cara bagaimana untuk mencipta frasa laluan yang lebih kukuh dengan membuat carian untuk 'Passphrases' pada cyber.gov.au

Petua 5: Mengenal pasti dan melaporkan penipuan dalam talian (scam)

ADAKAH ANDA TAHU:

Penjenayah siber pintar menipu dan mungkin akan menggunakan sebuah nama atau alamat e-mel yang anda sudah kenali. Berwaspada jika:

- **anda diminta untuk membayar sebuah bil dengan mustahak.**
- **anda diminta untuk mengubah butir-butir atau kata laluan anda.**
- **anda diminta untuk klikkan sebuah pautan atau membuka sebuah lampiran.**

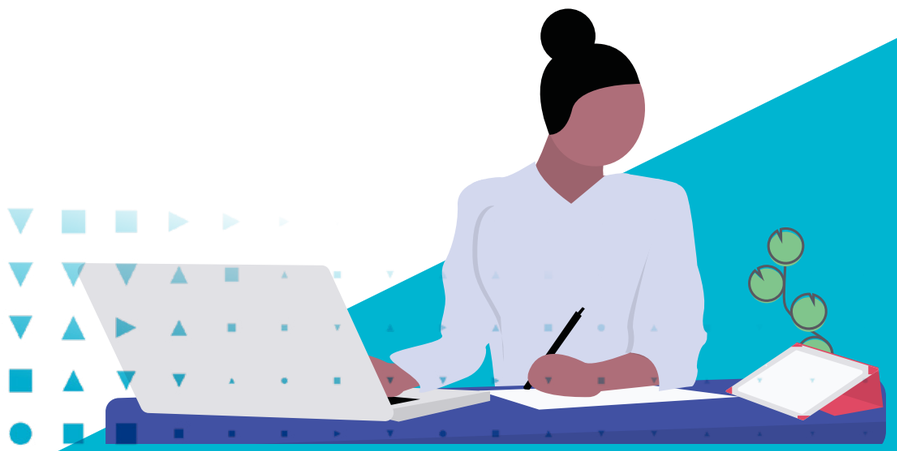
Lebih cepat anda melaporkan sebuah scam, lebih cepat kami boleh bertindak.

Jika anda percaya ada orang yang sedang cuba menggunakan internet untuk menipu anda, ia lebih baik untuk bertindak secara proaktif dan bersikap lebih berhati-hati daripada menghadapi risiko diambil kesempatan oleh orang lain.

Jika ia menawarkan sesuatu yang jauh lebih hebat daripada apa yang sebenarnya betul, kemungkinan besar begitulah hakikatnya. Walaupun sesuatu mesej mungkin berkata bahawa anda telah memenangi sebuah hadiah atau komputer anda mengandungi sebuah virus, mesej itu tidak unik kepada anda sahaja.

Ia mungkin datang daripada seorang penipu dalam talian (scammer) dan mereka mahu mengambil kesempatan terhadap anda.

Ingat, penipu dalam talian sering akan menyamar sebagai seorang atau organisasi yang anda boleh percaya. Berwaspada jika anda menerima sebuah mesej yang kelihatan seakan-akan daripada seorang yang anda percayai tetapi mereka menggunakan nombor telefon, alamat e-mel atau profil media sosial yang baharu. Sebelum anda jawab, tentusahkan bahawa orang atau organisasi yang mengirim mesej itu benar-benar siapa yang mereka dakwa, dengan menghubungi mereka melalui sebuah saluran yang anda memang boleh percayai. Contohya, jika anda menerima pesanan teks yang kelihatan seakan-akan dihantar oleh salah-seorang anak anda, tetapi ia datang daripada sebuah nombor baharu, jangan respon. Hantarkan mereka sebuah pesanan melalui media sosial untuk memeriksa terlebih dahulu adakah mereka benar-benar menukar nombor telefon mereka atau tidak.



Kesimpulan

Dengan berbekalkan maklumat tentang cara untuk menggunakan internet dengan lebih selamat ini, anda boleh melayari dan terus menikmati masa anda dalam talian dengan lebih yakin.

Tetapi ingat, penjenayah siber senantiasa berusaha untuk mencipta kaedah baharu untuk menipu orang.

Ia tidak merugikan jika anda boleh berusaha untuk memperbaharui pengetahuan keselamatan siber anda dari masa ke semasa dan untuk mempelajari cara baharu untuk kekal selamat.

Petua bonus

Mahu belajar cara-cara lanjut untuk kekal selamat dalam talian? Sila lihat petua-petua berikut.

Fikirkan dahulu tentang apa yang anda ingin hantarkan dalam talian.

Fikirkan betul-betul terlebih dahulu tentang maklumat yang anda ingin kongsikan dalam talian dan tentang siapa yang akan dapat melihatnya. Hanya terima permintaan untuk berkawan daripada orang yang anda tahu dalam kehidupan biasa anda.

Dapatkan khidmat amaran tentang ancaman baharu.

Daftarkan diri anda kepada perkhidmatan amaran percuma kami. Ia akan memaklumkan kepada anda apabila kami menemui sebuah ancaman siber baharu.

Ia juga akan memberi anda nasihat tentang apa yang perlu dibuat jika sebuah serangan berlaku.

Bercakaplah tentang keselamatan siber dengan ahli keluarga dan sahabat handai anda.

Dengan berbekalkan kemahiran tentang keselamatan siber ini, kongsikanlah apa yang anda telah pelajari dengan ahli keluarga dan sahabat handai anda. Pengetahuan anda mungkin boleh menolong mereka untuk mengelakkan diri mereka daripada sesuatu gejala buruk pada masa hadapan nanti!

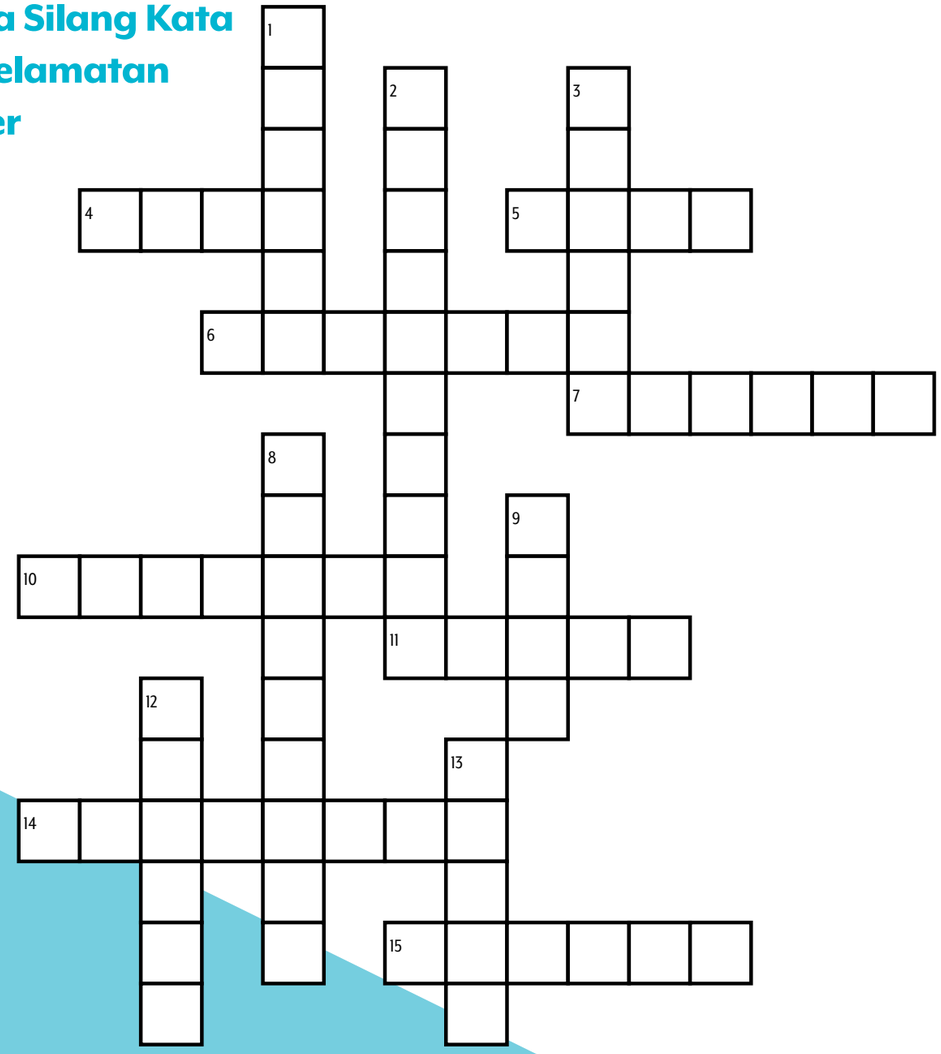
Elakkan daripada menggunakan Wi-Fi awam bila anda membuat urusan perbankan atau membeli-belah dalam talian.

Wi-Fi umum memang hebat untuk menonton video atau membaca laman web, tetapi pastikan anda hanya menggunakan hubungan internet di rumah anda untuk sebarang aktiviti dalam talian yang melibatkan wang. Wi-Fi awam mungkin berisiko.

Laporkan jenayah dan insiden siber untuk menjaga keselamatan Australia.

Jika anda fikir anda telah menjadi mangsa sebuah jenayah siber, bertindaklah dengan pantas. Nasihat lanjut boleh diperolehi di cyber.gov.au

Teka Silang Kata Keselamatan Siber



KE BAWAH

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

MELINTANG

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 Sampingan

Untuk maklumat lanjut, sila semak siri *Keselamatan Siber Peribadi kami*: tiga panduan yang direka untuk membantu rakyat biasa Australia untuk memahami dasar-dasar asas keselamatan siber dan cara bagaimana anda boleh mengambil tindakan untuk melindungi diri anda sendiri daripada ancaman siber yang lazim.

Anda boleh mengakses ketiga-tiga panduan di **cyber.gov.au**

Jawaban Teka Silang Kata:

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
Bahan di dalam panduan ini adalah bersifat umum dan tidak harus dianggap sebagai nasihat perundangan atau digantung sebagai bantuan dalam apa-apa keadaan atau kecemasan tertentu. Dalam sebarang hal mustahak, anda harus mendapatkan nasihat profesional bebas tentang apa yang anda sedang alami sendiri.

Pihak Komanwel tidak menerima tanggungjawab atau tanggungan ke atas sebarang kerosakan, kerugian atau perbelanjaan yang ditanggung akibat daripada pergantungan kepada maklumat yang terkandung dalam panduan ini.

Untuk maklumat lanjut, atau untuk melaporkan sebuah kejadian keselamatan siber, sila hubungi kami:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Nombor ini tersedia untuk digunakan di dalam Australia sahaja.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre