Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

KESELAMATAN SIBER PERIBADI

LANGKAH-LANGKAH PERTAMA

cyber.gov.au

Siri Keselamatan Siber Peribadi

Siri Keselamatan Siber Peribadi

Panduan ***Keselamatan Siber Peribadi: Langkah-langkah Pertama*** ialah panduan pertama dalam sebuah siri tiga panduan yang direka untuk membantu rakyat biasa Australia memahami dasar-dasar asas keselamatan siber. Pelajari cara bagaimana untuk bertindak bagi melindungi diri anda daripada ancaman siber yang lazim berlaku.

Langkah-langkah Pertama

Langkah-langkah Seterusnya

Langkah-langkah Lebih Maju

Isi Kandungan

PENGENALAN 1

Pasangkan pengemaskinian automatik 2

Aktifkan pengesahan pelbagai-faktor (multi-factor authentication) (MFA) 4

Kerap buatkan salinan sandaran bagi alat peranti anda 5

Gunakan frasa laluan untuk meneguhkan akaun-akaun penting anda 6

Kukuhkan alat peranti anda 7

Kembangkan pemikiran peneguhan siber anda 8

SENARAI SEMAK RINGKAS 11

KOSA KATA 12

Pengenalan

Apakah itu keselamatan siber peribadi?

Dalam dunia yang semakin dipacu teknologi, kami menggunakan alat peranti dan akaun setiap hari yang terdedah kepada ancaman siber:

- Alat peranti anda mungkin termasuk komputer, telefon bimbit, tablet dan alat peranti yang terhubung kepada internet yang lain.
- Anda juga mungkin menggunakan akaun-akaun dalam talian untuk e-mel, perbankan, membeli-belah, media sosial, permainan dalam talian dan lebih lagi.

Keselamatan siber peribadi adalah langkah-langkah berterusan yang anda boleh ambil untuk melindungi akaun-akaun dan alat peranti anda daripada ancaman siber.

Apakah itu ancaman siber?

Ancaman siber utama yang menjejaskan rakyat biasa Australia ialah **penipuan dalam talian (scam) dan perisian hasad (malware)**.

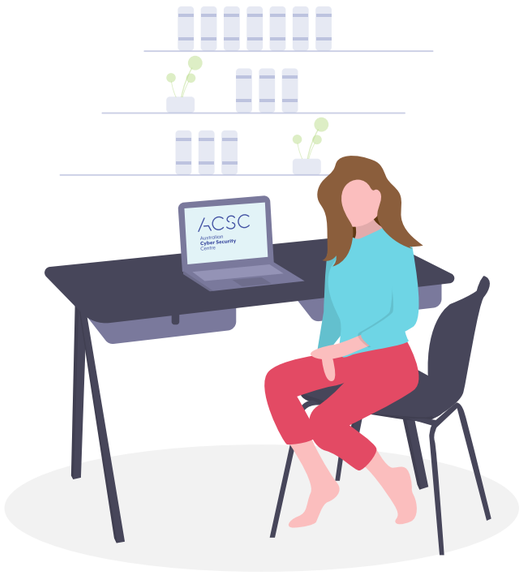
- **Perisian Hasad (Malware) ialah takrif umum yang digunakan untuk menjelaskan perisian berniat jahat** yang direkacipta untuk menyebabkan kerosakan. Ia boleh termasuk virus, program cecacing yang menerobosi sistem pengkomputeran untuk merosakkannya (worms), perisian pengintipan, program pengumpan yang menyamar sebagai program sahih (trojans), dan perisian tebusan (ransonware).
  Penjenayah siber menggunakan malware untuk mencuri maklumat dan wang anda, dan mengawal alat peranti dan akaun-akaun anda.
- **Penipuan dalam talian (Scam) ialah mesej-mesej yang dihantar penjenayah siber** yang direka untuk memanipulasi anda untuk menyerahkan maklumat sensitif, atau untuk mengaktifkan malware dalam alat peranti anda.

Serangan-serangan sebegini mungkin akan mendatangkan kesan peribadi dan kewangan yang signifikan ke atas mangsa-mangsanya. Ia juga semakin mengembang dari segi kecanggihan dan kekerapannya.

Bagaimana panduan ini boleh menolong melindungi saya daripada ancaman siber?

Jika ada sedang belajar tentang keselamatan siber buat pertama kali, atau anda ingin memastikan anda bergerak seiring dengan perkembangannya, panduan ini ialah tempat yang cukup baik untuk memulakannya.

Panduan Keselamatan Siber Peribadi: Langkah-langkah Pertama ialah panduan pertama dalam sebuah siri tiga panduan yang direka untuk membantu rakyat biasa Australia memahami dasar-dasar asas keselamatan siber.



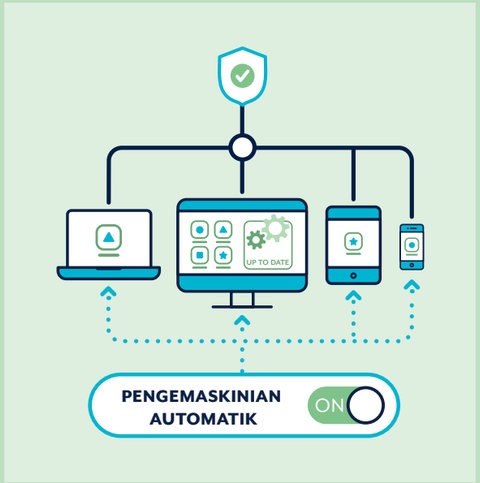
Keselamatan Siber Peribadi: Langkah-Langkah Pertama

Pasangkan pengemaskinian automatik

Apakah itu pengemaskinian?

Sebuah pengemaskinian ialah sebuah versi perisian (program, apps dan sistem pengoperasian) yang dipasangkan anda ke dalam komputer dan alat peranti anda yang telah ditambahbaik.

- **Pengemaskinian perisian menolong melindungi alat-alat peranti anda** dengan memperbaiki 'bugs' perisian (kesilapan pengkodan atau kelemahan-kelemahan). Penjenayah siber dan perisian hasad boleh menggunakan 'bugs' ini untuk mengakses alat peranti anda dan mencuri data peribadi, akaun-akaun, maklumat kewangan dan identiti anda.
- **'Bugs' perisian baharu kini sering ditemui** dan dieksploitasikan oleh penjenayah siber. Pengemaskinian perisian pada alat-alat peranti anda menolong melindungi anda daripada serangan siber.



Bagaimana saya boleh memasang pengemaskinian automatik?

Pengemaskinian automatik dipasang pada pengesetan alpa atau 'set dan lupakan' yang akan memasang pengemaskinian baharu sebaik sahaja ia disediakan.

- **Pasang dan sahkan pengemaskinian automatik** pada semua perisian dan alat peranti.
- **Cara bagaimana anda memasang pengemaskinian automatik mungkin berbeza** bergantung kepada perisian dan alat peranti berkenaan.
- **Tetapkan masa yang sesuai untuk pengemaskinian automatik** jika boleh, misalnya bila anda sedang tidur atau bila anda biasanya tidak menggunakan alat peranti anda.

Alat peranti anda mesti dihidupkan, dipasang ke sumber kuasa dan mempunyai ruang stor yang belum dipakai.

Petua: Jika anda menerima peringatan untuk mengemaskinikan perisian komputer alat peranti anda, anda patut berbuat demikian dengan secepat mungkin.

Maklumat lebih terperinci tentang cara bagaimana untuk memasang pengemaskinian automatik boleh ditemui dengan membuat carian untuk 'Updates' pada cyber.gov.au

Bagaimana pula jika pengesetan pengemaskinian automatik tidak disediakan?

Jika pengesetan pengemaskinian automatik tidak disediakan, anda patut kerap memeriksa untuk dan memasang pengemaskinian baharu melalui menu pengesetan perisian dan alat peranti anda.

Bagaimana pula jika alat peranti dan perisian lama saya tidak menerima sebarang pengemaskinian?

Jika alat peranti, sistem pengoperasian atau perisian anda sudah terlalu tua, ia mungkin tidak lagi disokong oleh pihak pengeluar atau pemajunya.

Bila produk-produk sampai ke tahap 'penamatan sokongan' ini ia tidak akan menerima pengemaskinian lagi. Ini boleh meninggalkan anda dalam keadaan terdedah kepada serangan siber. Contoh produk-produk yang sudah tamat sokongannya termasuk sistem pengoperasian Windows 7 dan iPhone 7.

Jika alat peranti, sistem pengoperasian atau perisian anda telah sampai ke penamatan sokongan ini, ACSC menyarankan agar anda menaiktarafkannya secepat mungkin untuk kekal berada dalam keadaan keselamatan yang kukuh.

Untuk maklumat lanjut, sila buatkan carian untuk 'End of support' pada cyber.gov.au

Keselamatan Siber Peribadi: Langkah-Langkah Pertama

Aktifkan pengesahan pelbagai-faktor (Multi-factor authentication) (MFA)

Apakah itu MFA?

Anda boleh gunakan pengesahan pelbagai-faktor multi-factor authentication (MFA) untuk meningkatkan keselamatan akaun-akaun paling penting anda. MFA memerlukan anda untuk menghasilkan sebuah kombinasi dua jenis pengesahan atau lebih sebelum akses diberi kepada sesuatu akaun.

- **Sesuatu yang anda tahu** (misalnya sebuah PIN, kata laluan atau frasa laluan)
- **Sesuatu yang anda ada** (misalnya sebuah kad pintar, token fizikal, app pengesahan, SMS atau e-mel)
- **Sesuatu yang mewakili diri anda** (misalnya cap jari, pengecaman wajah atau imbasan iris mata)

MFA menjadikannya lebih sukar bagi penjenayah siber untuk mendapatkan akses permulaan kepada akaun anda. Ia menambahkan lagi lapisan pengesahan, dan memerlukan masa, usaha dan sumber-sumber tambahan untuk memecahkannya.

Bagaimana boleh saya mengaktifkan MFA untuk melindungi akaun-akaun paling penting saya?

Langkah-langkah untuk mengaktifkan MFA berbeza bergantung kepada akaun, alat peranti atau aplikasi perisian berkaitan. Anda patut mengaktifkan MFA sekarang, bermula dengan akaun-akaun penting anda:

- Semua akaun perbankan dan kewangan dalam talian (misalnya bank anda, PayPal)
- Semua akaun e-mel (misalnya Gmail, Outlook, Hotmail, Yahoo!)

Jika anda mempunyai banyak akaun emelkan, utamakan akaun yang dikaitkan dengan perbankan dalam talian anda atau perkhidmatan-perkhidmatan penting yang lain.

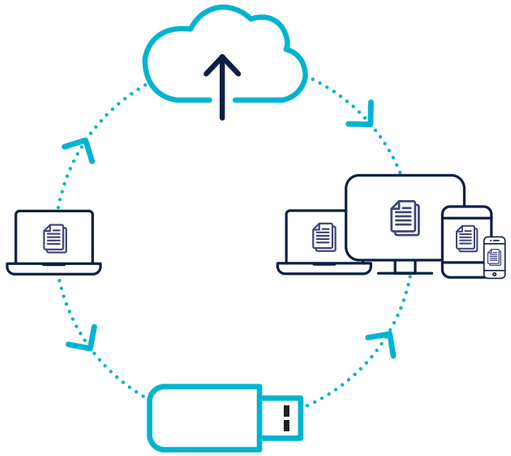
Anda boleh membaca lanjut tentang cara bagaimana untuk memasang pengesahan pelbagai-faktor dengan melakukan carian untuk 'Multi-factor authentication' atau 'MFA' pada cyber.gov.au

Kerap buatkan salinan sandaran bagi alat peranti anda

Apakah itu salinan sandaran (backup)?

Sebuah salinan sandaran ialah sebuah salinan digital maklumat. Ia meliputi bahan-bahan seperti foto, maklumat kewangan atau rekod-rekod yang anda telah simpankan ke dalam sebuah alat peranti simpanan luaran, atau ke awan.

Penyandaran maklumat anda merupakan sebuah langkah pencegahan supaya ia boleh dikembalikan sekiranya ia hilang, dicuri atau mengalami kerosakan.



Bagaimana boleh saya membuatkan salinan sandaran bagi alat peranti dan fail-fail saya?

Anda patut menyandarkan fail-fail dan alat peranti anda dengan kerap. Bagaimana ia akan dilakukan, sama ada secara harian, mingguan atau bulanan, terpulang sepenuhnya kepada anda. Bilangan kali anda patut membuat sandaran bergantung kepada jumlah:

- Fail-fail baharu yang dimuatkan ke dalam alat peranti anda,
- Perubahan yang anda ingin lakukan ke atas fail-failt tersebut.

Petua: Kerap periksakan sandaran anda supaya anda boleh membiasakan diri anda dengan proses pemulihannya. Senantiasa pastikan bahan sandaran anda berfungsi dengan betul.

Maklumat lebih terperinci tentang cara bagaimana untuk menyandarkan maklumat anda boleh ditemui dengan membuat carian untuk 'Backups' pada cyber.gov.au

Gunakan frasa laluan untun meneguhkan akaun-akaun penting anda

Pengesahan pelbagai-faktor (Multi-factor authentication) (MFA) ialah salah-satu cara yang paling berkesan untuk melindungi akaun-akaun anda daripada penjenayah siber. **Jika MFA tidak disediakan**, sebuah frasa laluan yang kuat dan unik boleh melindungi akaun anda dengan lebih baik berbanding dengan sebuah kata laluan yang ringkas.

Apakah itu frasa laluan?

Sebuah frasa laluan menggunakan empat perkataan rawak atau lebih sebagai kata laluan anda.

Contohnya: 'kristal bawang tanah liat pretzel'.

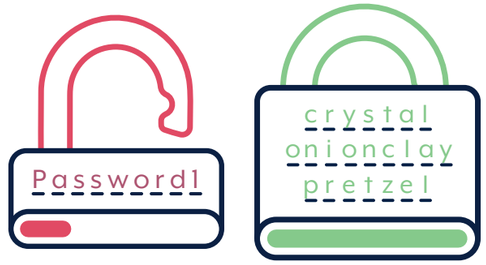
- **Frasa laluan adalah lebih kukuh** daripada kata laluan yang ringkas.
- Frasa laluan adalah sukar **untuk dileraikan oleh penjenayah siber**, tetapi senang untuk diingat oleh anda.

Bagaimana boleh saya ciptakan sebuah frasa laluan?

Ciptakan frasa laluan yang:

- **Panjang:** sekurang-kurangnya sepanjang 14 huruf, dengan menggunakan empat perkataan rawak atau lebih. Frasa laluan yang lebih panjang akan menjadikannya lebih kukuh.
- **Tidak boleh diramal:** gunakan campuran rawak empat perkataan yang tidak ada kaitan antara satu sama lain atau lebih. Jangan gunakan frasa, petikan atau lirik terkenal.
- **Unik:** tidak digunakan kembali secara ganda dalam pelbagai akaun.

Jika sesebuah laman web atau perkhidmatan memerlukan sebuah kata laluan kompleks yang mengandungi simbol, huruf besar, atau nombor, anda boleh memasukkanya ke dalam frasa laluan anda. Frasa laluan anda tetap harus panjang, tidak boleh diramal dan unik untuk menjamin keselamatan terbaik.



Akaun-akaun manakah yang saya patut perkukuhkan dengan sebuah frasa laluan?

Jika akaun-akaun paling penting anda tidak dilindungi dengan MFA, tukarkan kata laluan anda kepada frasa laluan yang kuat dan unik, bermula dengan:

- Akaun-akaun perbankan dan kewangan dalam talian
- Akaun-akaun e-mel

Jika anda mempunyai banyak akaun e-mel, utamakan akaun-akaun yang dikaitkan dengan perbankan dalam talian atau perkhidmatan-perkhidmatan penting anda yang lain.

Anda biasanya boleh menukar kata laluan anda kepada satu frasa laluan yang kuat dan unik melalui menu pengesetan akaun anda.

Petua: Jika anda menghadapi kesukaran untuk mengingati semua frasa laluan anda, pertimbangkan penggunaan sebuah pengurus kata laluan (password manager). Dengan adanya sebuah pengurus kata laluan, anda hanya perlu mengingati satu kata laluan, dan pengurus kata laluan berkenaan akan menguruskan segalanya. Sila lakukan carian untuk 'password manager' pada cyber.gov.au untuk nasihat lanjut.

Maklumat lebih terperinci tentang cara bagaimana untuk mewujudkan frasa laluan yang kukuh boleh ditemui dengan mencari 'Passphrases' pada cyber.gov.au

Perkukuhkan alat peranti anda

Pada hari ini, telefon pintar dan tablet digunapakai dalam kehidupan harian. Kita menggunakannya untuk berhubung, membeli-belah, bekerja, melakukan perbankan, menjejaki kecergasan kita dan menyelesaikan ratusan tugasan pada bila-bila masa, dan dari mana-mana lokasi.

Apa yang mungkin berlaku jika alat peranti mudah alih saya dikompromi, hilang atau dicuri?

- Ia mungkin digunakan oleh penjenayah siber untuk mencuri wang dan identiti anda. Mereka berbuat demikian dengan menggunakan maklumat yang disimpan di dalam alat peranti anda, termasuklah akaun-akaun media sosial dan e-mel.
- Anda mungkin akan hilang data yang tidak boleh dicari ganti seperti foto, catatan atau pesanan (jika ia tidak disandarkan terlebih dahulu).
- Seorang penjenayah siber mungkin boleh menggunakan nombor telefon anda untuk menipu orang lain dalam talian.

Bagaimana boleh saya memperkukuhkan alat peranti mudah alih saya?

Keselamatan alat peranti:

- **Kuncikan** alat peranti anda dengan sebuah frasa laluan, kata laluan, PIN atau kod laluan. Pastikan ia sukar diteka – tarikh lahir anda dan kuncian bercorak (pattern locks) mudah untuk dileraikan oleh penjenayah siber. Gunakan sebuah frasa laluan untuk keselamatan optimal (sila lihat mukasurat 6). Anda juga mungkin boleh menimbangkan penggunaan pengecaman wajah atau sebuah cap jari untuk membuka alat peranti anda.
- **Pastikan** alat peranti anda disetkan untuk dikunci secara automatik selepas satu tempoh masa ketiadaan aktiviti yang pendek.
- **Jangan** caskan alat peranti anda di sebuah stesen pengecasan awam dan elakkan alat pengecas daripada pihak ketiga.
- **Anggap** telefon anda seperti dompet anda. Pastikan ia selamat dan ada bersama ada pada setiap masa.

Keselamatan perisian dan app:

- **Gunakan** ciri pengemaskinian automatik alat peranti anda untuk memasang aplikasi baharu dan pengemaskinian sistem pengoperasian secepat mungkin bila ia disediakan.
- **Setkan** alat peranti itu untuk memerlukan sebuah frasa laluan/kata laluan sebelum aplikasi dipasang. Sistem pengawalan ibubapa (parental controls) juga boleh digunakan bagi tujuan ini.
- **Periksakan** kebenaran privasi dengan cermat bila memasang app baharu pada alat peranti anda, khususnya app percuma. Hanya pasangkan app daripada vendor yang boleh dipercayai.

Keselamatan data:

- **Bolehkan** fungsi-fungsi penguncian dan pemadaman jarak jauh, jika alat peranti menyokong ciri-ciri ini.
- **Pastikan** anda memadamkan data peribadi anda secara menyeluruh daripada alat peranti anda sebelum anda menjual atau membuangkannya.

Keselamatan ketersambungan:

- **Matikan** Bluetooth dan Wi-Fi bila anda tidak menggunakannya.
- **Pastikan** alat peranti anda tidak berhubung secara automatik ke jaringan-jaringan Wi-Fi baharu.

Maklumat lebih terperinci tentang cara bagaimana untuk memastikan telefon bimbit anda boleh dicari, boleh ditemui dengan mencari 'Secure your mobile phone' pada cyber.gov.au

Keselamatan Siber Peribadi: Langkah-Langkah Pertama

Kembangkan pemikiran peneguhan siber anda

Keselamatan siber peribadi bukan sekadar menukar pengesetan sahaja, ia juga mengenai merubah pemikiran dan tingkahlaku anda.

Awasi scam

Penjenayah siber diketahui menggunakan emel, mesej, media sosial atau panggilan telefon untuk cuba menipu rakyat Australia. Mereka mungkin menyamar sebagai seorang individu atau organisasi yang anda fikir anda tahu, atau anda fikir anda patut percayai.

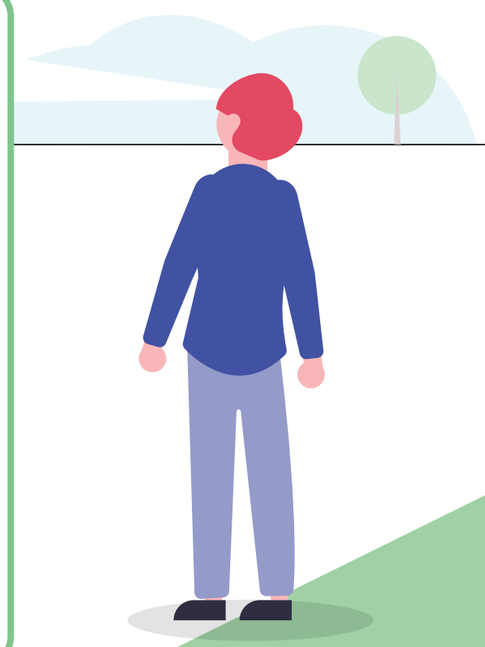
Mesej dan panggilan mereka akan cuba untuk menipu anda untuk melakukan tindakan tertentu, seperti:

- Mendedahkan butir-butir akaun bank, kata laluan, dan nombor-nombor kad kredit,
- Memberikan akses jarak jauh kepada komputer anda
- Membuka sebuah lampiran, yang mungkin mengandungi malware
- Menghantar wang atau kad hadiah

Bagaimana boleh saya mengenali mesej scam?

Ia mungkin sukar untuk mengenai mesej scam. Penjenayah siber sering menggunakan kaedah-kaedah tertentu untuk menipu anda. Mesej-mesej mereka mungkin mengandungi:

- **Pihak Berkuasa**: adakah mesej itu mendakwa ia datang daripada seorang pegawai rasmi, misalnya daripada bank anda?
- **Tindakan Mustahak**: adakah anda diberitahu ada sesuatu masalah, atau anda hanya mempunyai tempoh masa terhad untuk bertindak atau membayar?
- **Emosi**: adakah mesej itu menjadikan anda cemas, takut, menaruh harapan atau tergerak untuk ingin tahu dengan lebih lanjut?
- **Jarang ada**: adakah mesej itu menawarkan sesuatu yang sukar diperolehi, atau menjanjikan sebuah tawaran hebat?
- **Peristiwa semasa**: adakah mesej itu berkaitan sesuatu kisah berita semasa atau kejadian hebat?



Pelajari cara bagaimana untuk mengenali mesej pancingan (phishing) atau scam dengan melayari 'Learn the basics' pada cyber.gov.au

Apakah saya patut buat jika saya mendapat sebuah mesej scam?

Jika anda menerima mesej atau panggilan telefon scam, anda patut tidak menghiraukan, buang atau melaporkannya kepada ACCC Scamwatch di scamwatch.gov.au

Anda juga boleh menghubungi Talian Utama Keselamatan Siber ACSC pada **1300 CYBER1** (1300 292 371) jika anda berasa bimbang tentang keselamatan siber anda.

Jika anda terlibat dalam sebuah scam dan fikir bahawa akaun bank, kad kredit atau debit anda mungkin menghadapi risiko, hubungi institusi kewangan anda dengan segera. Mereka mungkin boleh menutup akaun anda atau menghentikan sesuatu transaksi.

Bagaimana kalau saya tidak pasti jika sesuatu mesej ialah sebuah scam?

Jika anda fikir sesuatu mesej atau panggilan mungkin sebenarnya datang daripada sebuah organisasi yang anda percayai (misalnya bank anda), cari satu cara untuk menghubungi mereka yang anda boleh percayai. Buatkan carian untuk laman web rasmi, panggil nombor telefon mereka yang diiklankan, atau pergi ke sebuah kedai atau cawangan fizikal. Jangan gunakan pautan atau butir-butir untuk menghubungi mereka yang ada di dalam mesej yang dikirimkan atau diberi kepada anda melalui telefon kerana ianya mungkin palsu.

Petua:
Fikir Sebelum Anda Klik

- **Fikir sebelum anda klik** pada pautan dalam e-mel, laman web dan SMS.
- **Selalu bersikap berwaspada** terhadap lampiran yang anda terima.
- **Jika pelayar komputer (browser) anda memberitahu anda bahawa sebuah laman web itu tidak selamat, tutupkannya dengan segera.**

Ingat: Tidak ada mana-mana orang IT, jabatan kerajaan atau perniagaan yang akan menghubungi anda dan meminta butir-butir pendaftaran masuk anda.

Jika anda fikir anda telah menjadi mangsa jenayah siber, laporkannya melalui ReportCyber ACSC pada cyber.gov.au/report atau sila panggil Talian Utama Keselamatan Siber kami pada 1300 CYBER1 (1300 292 371).

Anda juga boleh memastikan anda mengikuti perkembangan tentang ancaman terkini dengan melayani perkhidmatan amaran percuma ACSC. Sila buatkan carian 'Subscribe to the ACSC alert service' pada cyber.gov.au Kami akan menghantar anda sebuah amaran apabila kami mengenalpasti sebuah ancaman siber baharu.

Keselamatan Siber Peribadi: Langkah-Langkah Pertama

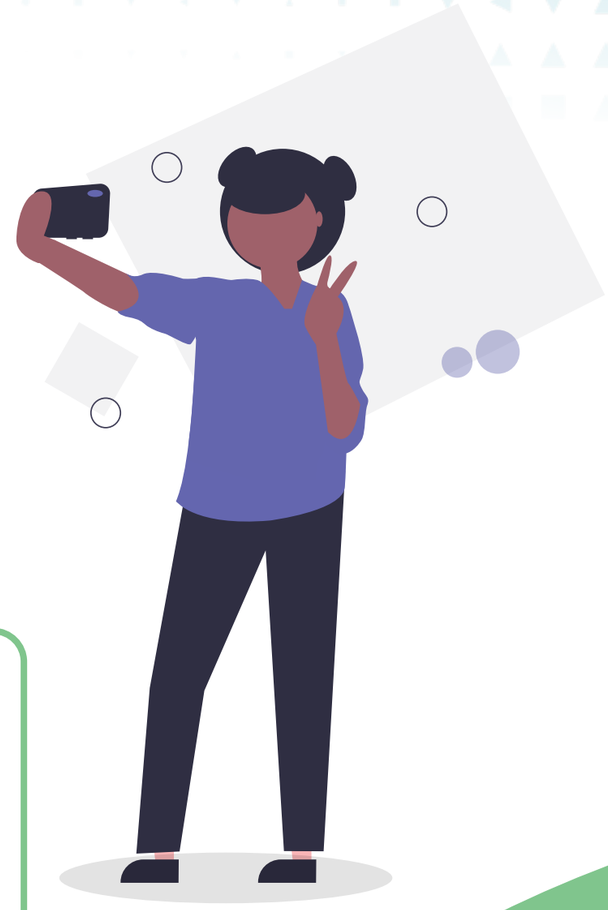
Berhenti dan berfikir dahulu sebelum anda berkongsi sesuatu dalam media sosial

Penjenayah siber boleh menggunakan maklumat yang anda telah hantarkan secara terbuka pada akaun/akaun-akaun media sosial anda dalam scam dan serangan siber mereka.

Ingat bahawa sebarang maklumat dalam internet akan kekal wujud buat selama-lamanya dan anda sama sekali tidak akan dapat memadamkan apa yang sudah dihantar.

Bagaimana boleh saya berhenti dan berfikir sebelum membuat hantaran?

- **Fikirkan:** Bagaimana seorang penjenayah siber boleh menggunakan maklumat ini untuk menyasarkan saya atau akaun-akaun saya?
- **Fikirkan:** Adakah saya akan berasa selesa untuk menunjukkan maklumat atau gambar ini kepada seorang yang saya tidak kenali langsung di luar talian?



Apakah maklumat yang saya patut henti kongsikan?

Elakkan daripada berkongsi maklumat (termasuk foto) dalam talian yang boleh diguna penjenayah siber untuk mengenalpasti anda, memanipulasi anda melalui sebuah scam atau meneka soalan pengembalian akaun anda. Ini mungkin termasuk maklumat anda seperti:

- Tempat lahir dan tarikh lahir.
- Alamat dan nombor telefon.
- Majikan dan latarbelakang kerjaya.
- Di mana anda bersekolah.
- Apa-apa maklumat peribadi lain yang boleh digunakan untuk menyasarkan anda.

Senarai semak ringkas

Sudahkah anda menyelesaikan semua perkara dalam panduan ini?

Gunakan senarai semak berguna ini untuk menjejaki kemajuan anda:

- **Saya sudah memasang pengemaskinian automatik bagi semua alat peranti saya:**
  - Komputer (komputer dan komputer riba)
  - Telefon bimbit
  - Tablet
- **Saya telah mengaktifkan pengesahan pelbagai-faktor pada akaun-akaun paling penting saya:**
  - Semua akaun perbankan dan kewangan dalam talian saya (misalnya bank anda, PayPal)
  - Semua akaun e-mel saya (misalnya Gmail, Outlook, Hotmail, Yahoo!)
- **Saya kerap menyandarkan alat peranti saya:**
  - Komputer (komputer dan komputer riba)
  - Telefon bimbit
  - Tablet
- **Saya menggunakan frasa laluan yang unik dan kuat pada akaun-akaun paling penting saya yang tidak dilindungi MFA:**
  - Perbankan atas talian dan akaun-akaun kewangan.
  - Akaun-akaun emel.
- **Saya telah memperkukuhkan alat-alat peranti mudah alih saya:**
  - Komputer riba
  - Telefon bimbit
  - Tablet
- **Saya menggunakan pemikiran peneguhan siber setiap hari:**
  - Saya boleh mengenali mesej scam
  - Saya tahu apa yang perlu dilakukan jika saya menerima sebuah mesej scam
  - Saya tahu bagaimana untuk memeriksa sama ada sebuah mesej ialah scam atau tidak jika saya tidak berasa pasti
  - Saya berfikir dahulu sebelum saya klik pada pautan dan lampiran
  - Saya berfikir dahulu sebelum saya berkongsi apa-apa pada media sosial
- **Saya tahu di mana saya boleh mendapatkan pertolongan jika saya menjadi mangsa sebuah jenayah siber atau scam**

Keselamatan Siber Peribadi: Langkah-Langkah Pertama

KOSA KATA

Pemulihan Akaun

Sebuah proses di mana satu set soalan atau kaedah penentusahan lain diguna untuk memulih atau mengembalikan akses kepada sesebuah akaun atau untuk menukar frasa laluan/kata laluan ke sesebuah akaun.

App

Juga dirujuk sebagai sebuah aplikasi mudah alih, sebuah app ialah takrif bagi sebuah perisian yang biasanya digunakan bagi sebuah telefon pintar atau tablet.

Lampiran

Sebuah fail yang dikepilkan kepada sebuah mesej e-mel.

App pengesahan (Authenticator app)

Sebuah app yang diguna untuk mengesahkan identiti seorang pengguna komputer bagi membenarkan akses melalui pengesahan pelbagai-faktor multi-factor authentication (MFA).

Awan (Cloud)

Sebuah jaringan komputer pelayan (server) jarak jauh yang menyediakan kuasa penyimpanan (stor) dan pemerosesan yang sungguh meluas dan teredar.

Penjenayah Siber

Mana-mana individu yang mengakses sebuah sistem komputer atau akaun secara haram untuk merosakkan atau mencuri maklumat.

Alat Peranti

Sebuah alat peranti komputer atau komunikasi. Contohnya, komputer, komputer riba, telefon bimbit atau tablet.

Penamatan Sokongan

Penamatan sokongan merujuk kepada sebuah keadaan di mana sesebuah syarikat menamatkan sokongan bagi sesuatu produk atau perkhidmatan. Ia lazimnya terpakai bagi produk perkakasan atau perisian apabila sesebuah syarikat mengeluarkan sebuah versi baharu dan menamatkan sokongan bagi versi-versi dahulunya.

Perisian Hasad (Malware)

Perisian berniat jahat yang digunakan untuk mencapai akses yang tidak dibenarkan dan untuk menguasai komputer seseorang pengguna, mencuri maklumat dan menjejaskan atau melumpuhkan sistem jaringan.

Sistem Pengoperasian

Perisian yang dipasang dalam sebuah pemacu keras (hard drive) yang membolehkan perkakasan komputer untuk berkomunikasi dengan dan menjalankan program-program komputer. Contohnya: Microsoft Windows, Apple macOS, iOS, Android.

Token Fizikal

Sebuah alat peranti fizikal yang biasanya boleh dipasang pada pemegang kunci, yang menjanakan sebuah kod keselamatan yang diguna untuk mengesahkan identiti seorang pengguna komputer dengan menggunakan MFA.

Akses Jarak Jauh

Menyampaikan capaian akses dan kawalan ke atas alat peranti dan jaringan daripada sebuah lokasi di luar tapak berkaitan.

Perisian Komputer

Biasanya dirujuk sebagai program, sekumpulan arahan yang membolehkan si pengguna untuk berinteraksi dengan sebuah komputer, perkakasannya atau untuk melakukan tugasan.

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