Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

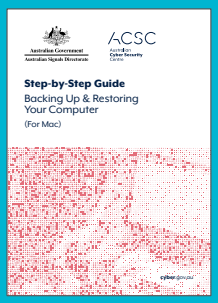
PANDUAN KEAMANAN DUNIA MAYA BISNIS KECIL

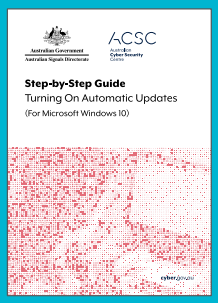
cyber.gov.au

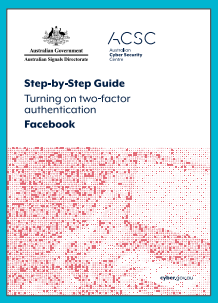
Panduan Tambahan

Untuk langkah-langkah keamanan dunia maya lainnya guna membantu menjaga bisnis Anda tetap aman, lihat rangkaian Keamanan Dunia Maya Bisnis Kecil kami di cyber.gov.au

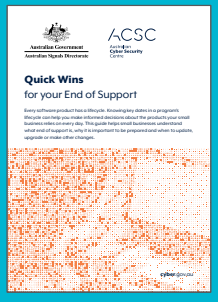
PANDUAN LANGKAH DEMI LANGKAH

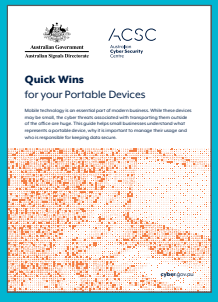


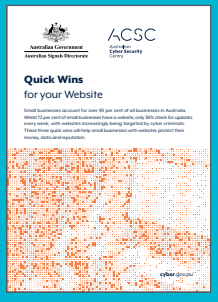




PANDUAN CEPAT TANGGAP







Daftar Isi

Kata Pengantar

Panduan ini telah dikembangkan untuk membantu bisnis kecil melindungi diri dari insiden keamanan dunia maya yang paling sering terjadi.

Insiden keamanan dunia maya dapat berdampak buruk pada bisnis kecil.

Sayangnya, kami di Australian Cyber Security Centre (ACSC) melihat dampak insiden keamanan dunia maya setiap hari, baik pada individu, bisnis kecil, maupun perusahaan besar.

Kami menyadari bahwa banyak pemilik dan penyelenggara bisnis kecil tidak memiliki waktu atau sumber daya untuk berfokus pada keamanan dunia maya. Namun, ada langkah-langkah sederhana yang dapat diterapkan oleh bisnis kecil untuk membantu mencegah insiden keamanan dunia maya yang paling sering terjadi.

Panduan Keamanan Dunia Maya Bisnis Kecil kami telah dirancang khusus untuk bisnis kecil guna memahami, mengambil tindakan, dan meningkatkan ketahanan keamanan dunia maya mereka melawan ancaman keamanan dunia maya yang terus berkembang. Bahasanya jelas, tindakannya sederhana, dan panduannya disesuaikan untuk bisnis kecil.

Untuk mendapat gambaran umum tentang dasar-dasar keamanan dunia maya, panduan ini adalah awal yang tepat. Jika Anda ingin meningkatkan keamanan dunia maya Anda lebih lanjut, Anda dapat menemukan informasi dan saran selengkapnya di situs web ACSC di: **cyber.gov.au**

ACSC hadir untuk membantu menjadikan Australia tempat paling aman untuk terhubung secara online.

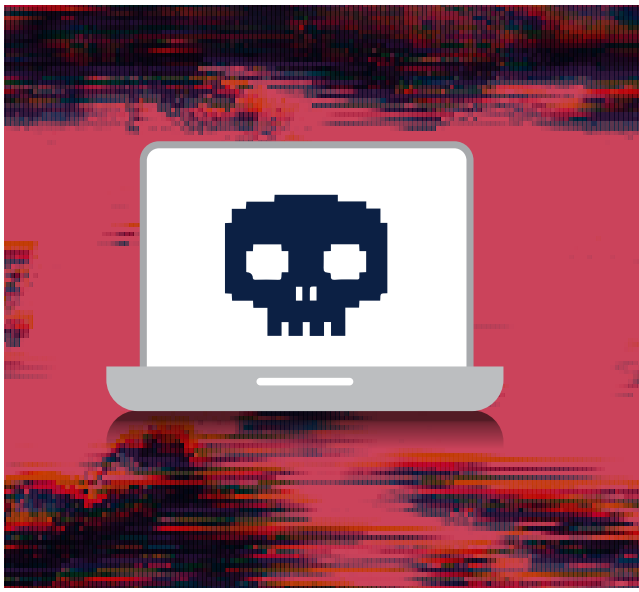
Australian Cyber Security Centre (ACSC), sebagai bagian dari Australian Signals Directorate (ASD), memberikan saran, bantuan, dan tanggapan operasional keamanan dunia maya untuk mencegah, mendeteksi, dan memulihkan ancaman dunia maya terhadap Australia.

Ancaman Dunia Maya: **Bidang Utama**

Bagi bisnis kecil, insiden keamanan dunia maya terkecil pun dapat memberikan dampak yang sangat merugikan.

Bagian ini dirancang untuk membantu agar usaha kecil tetap waspada dan siap. Bagian ini mengidentifikasi dan menjelaskan jenis ancaman dunia maya yang paling sering terjadi dan apa yang dapat Anda lakukan untuk melindungi bisnis Anda.

Perangkat Lunak Berbahaya (Malware)



Apa? Perangkat lunak tidak sah yang dirancang untuk menyebabkan kerusakan

Malware adalah istilah umum untuk perangkat lunak berbahaya termasuk ransomware, virus, spyware, dan trojan.

Mengapa? Mengganggu. Merusak. Menipu.

Malware membuka jalan bagi penjahat untuk mengakses informasi penting seperti nomor dan kata sandi bank atau kartu kredit.

Malware juga dapat **mengendalikan atau memata-matai** komputer pengguna. Hal-hal yang dapat saja dilakukan penjahat yang memiliki akses dan data tersebut mencakup:

- **Penipuan**
- **Pencurian identitas**
- **Mengganggu** bisnis
- **Mencuri** data sensitif atau kekayaan intelektual
- **Menyedot** sumber daya komputer untuk aktivitas kriminal yang lebih luas

Siapa? Siapa pun, di mana pun

Pembuat malware dapat berada di mana saja di dunia ini.

Yang mereka butuhkan hanyalah komputer, keterampilan teknis, dan niat jahat. Penjahat dapat dengan mudah mengakses alat murah untuk menggunakan malware melawan Anda.

Penjahat melemparkan jaring yang lebar dan memburu yang paling rentan. Dengan menerapkan langkah-langkah keamanan dunia maya dan tetap waspada terhadap ancaman, Anda dapat melindungi bisnis Anda agar tidak menjadi sasaran empuk.

MELINDUNGI DARI MALWARE

- Perbarui secara otomatis sistem operasi, perangkat lunak, dan aplikasi Anda
- Cadangkan secara berkala data penting Anda
- Latih staf Anda untuk mengenali tautan dan lampiran yang mencurigakan

Pesan Penipuan (Phishing)

Apa? Email, pesan, atau panggilan 'licik' yang dirancang untuk mengelabui penerima agar kehabisan uang dan data

Penjahat akan sering menggunakan email, media sosial, panggilan telepon, atau pesan teks untuk mencoba menipu bisnis di Australia.

Penjahat tersebut mungkin berpura-pura menjadi individu atau organisasi yang sepertinya Anda tahu, atau menurut Anda harus dipercaya.

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

- **Membayar faktur palsu** atau mengubah detail pembayaran untuk faktur yang sah
- **Mengungkap detail rekening bank**, kata sandi, dan nomor kartu kredit (terkadang dikenal sebagai penipuan 'phishing', penjahat dunia maya dapat meniru merek dan logo resmi dari bank dan situs web agar tampak tepercaya)
- **Memberikan akses jarak jauh** ke komputer atau server Anda
- **Membuka lampiran**, yang mungkin berisi malware
- **Membeli kartu hadiah** dan mengirimkannya ke penipu

Di mana? Email, Media Sosial, Panggilan Telepon, Pesan Teks

Penipuan phishing tidak terbatas pada email. Penipuan ini semakin canggih dan sulit dikenali.

Berhati-hatilah terhadap permintaan uang yang mendesak, perubahan rekening bank, lampiran yang tidak diharapkan, dan permintaan untuk memeriksa atau mengonfirmasi detail login.

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

Siapa? Bisnis di Australia

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

Namun, ada teknik umum yang akan digunakan penjahat untuk mencoba menipu staf Anda. Pesan mereka mungkin berisi:

- **Otoritas:** Apakah pesan itu mengaku dari pihak resmi atau atasan di perusahaan?
- **Urgensi:** Apakah Anda diberi tahu ada masalah, atau waktu Anda untuk merespons atau membayar terbatas?
- **Emosi:** Apakah pesan tersebut membuat Anda merasa 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?

Jika Anda merasa sebuah pesan atau panggilan mungkin benar-benar berasal dari organisasi yang Anda percayai (seperti bank atau pemasok Anda), cari metode kontak yang dapat Anda percayai.

Cari situs web resmi atau hubungi nomor telepon mereka yang diiklankan. Jangan gunakan tautan atau detail kontak dalam pesan yang dikirim kepada Anda atau diberikan melalui telepon karena itu bisa jadi penipuan.

Ransomware

Apa? Jenis malware yang mengunci komputer atau file Anda sampai uang tebusan dibayarkan

Ransomware bekerja dengan mengunci atau mengenkripsi file Anda, sehingga Anda tidak dapat lagi menggunakan atau mengaksesnya. Kadang, ransomware bahkan dapat menghentikan operasi perangkat Anda. Ransomware dapat menginfeksi perangkat Anda dengan cara yang sama seperti malware lainnya. Contoh:

- Mengunjungi situs web yang tidak aman atau mencurigakan
- Membuka tautan, email, atau file dari sumber yang tidak dikenal
- Memiliki keamanan yang buruk di jaringan atau perangkat Anda (termasuk server)

Mengapa? Uang

Ransomware memberi pendapatan pada penjahat dunia maya dengan risiko rendah dan imbalan tinggi. Mudah dikembangkan dan disebarkan. Tebusan biasanya dibayarkan menggunakan mata uang digital online atau mata uang kripto seperti Bitcoin, yang sangat sulit dilacak. Selain itu, sebagian besar bisnis kecil tidak siap menghadapi serangan ransomware sehingga menguntungkan penjahat dunia maya.

Siapa? Bisnis kecil, menengah, dan besar

Bisnis kecil bisa sangat rentan karena cenderung tidak menerapkan langkah-langkah keamanan dunia maya yang dapat membantu mencegah dan pulih dari ransomware.

JANGAN PERNAH MEMBAYAR TEBUSAN

Membayar uang tebusan tidak menjamin file milik korban akan dipulihkan, tidak pula mencegah publikasi atau penjualan data curian untuk digunakan dalam kejahatan lain. Tindakan itu juga meningkatkan kemungkinan korban menjadi sasaran lagi.

Jika Anda mengalami insiden ransomware dan memerlukan dukungan, hubungi Saluran Siaga 24/7 ACSC di 1300 CYBER1 (1300 292 371).

Terlepas dari keputusan untuk membayar uang tebusan, korban dianjurkan untuk melaporkan insiden ransomware ke ACSC di cyber.gov.au. Berbagi informasi tentang insiden membantu melindungi bisnis lainnya di Australia.

MENCEGAH DAN PULIH DARI RANSOMWARE

- Cadangkan secara berkala data penting Anda
- Perbarui secara otomatis sistem operasi, perangkat lunak, dan aplikasi Anda
- Bila memungkinkan, wajibkan autentikasi multifaktor untuk mengakses layanan (halaman 12)
- Audit dan amankan perangkat Anda (termasuk server jika Anda memilikinya) dan layanan apa pun yang terhubung internet di jaringan Anda (Remote Desktop, File Shares, Webmail). Diskusikan hal ini dengan profesional TI jika Anda ragu.

Pertimbangan Perangkat Lunak: **Bidang Utama**

Mengelola perangkat lunak, data, dan akun online Anda dapat secara tajam meningkatkan perlindungan bisnis Anda dari jenis ancaman dunia maya yang paling sering terjadi.

Misalnya, sistem operasi Anda adalah bagian perangkat lunak terpenting di komputer Anda. Sistem operasi mengelola perangkat keras komputer Anda dan semua programnya sehingga perlu diperbarui secara berkala guna memastikan Anda selalu menggunakan versi yang paling aman.

Tingkatkan ketahanan, selalu ketahui info terbaru, dan tetap aman dengan pertimbangan perangkat lunak untuk bisnis kecil ini.

Pembaruan Otomatis

Apa? Pembaruan Perangkat Lunak

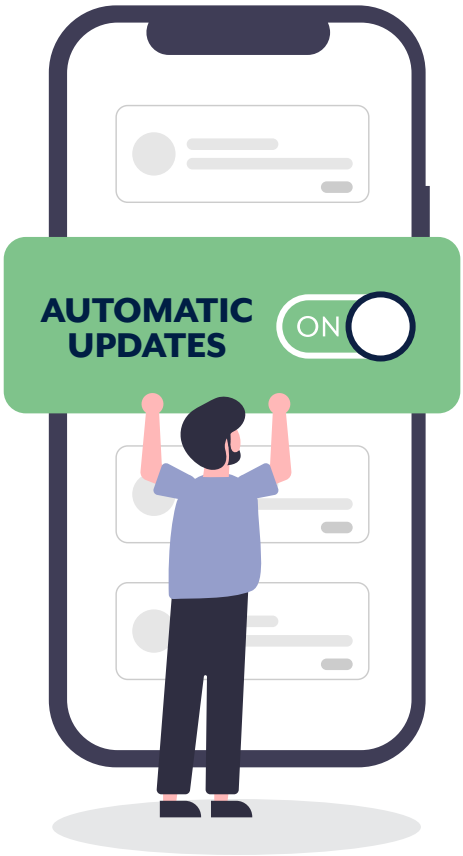
Pembaruan merupakan peningkatan versi dari perangkat lunak (program, aplikasi, dan sistem operasi) yang telah diinstal pada server, komputer, dan perangkat seluler Anda. **Pembaruan otomatis** merupakan sistem default atau **'tetapkan dan lupakan'** yang memperbarui perangkat lunak Anda segera saat tersedia.

Mengapa? Keamanan

- Menjaga sistem operasi dan aplikasi Anda tetap terbarui adalah **salah satu cara terbaik untuk melindungi diri Anda** dari insiden keamanan dunia maya
- Memperbarui perangkat lunak Anda secara berkala akan **mengurangi kemungkinan penjahat dunia maya menggunakan kelemahan yang diketahui** untuk menjalankan malware atau meretas perangkat Anda
- **Menghemat waktu dan menenangkan pikiran Anda,** pembaruan otomatis adalah bagian penting untuk menjaga keamanan perangkat dan data Anda

Kapan? Hari ini & setiap hari

- **Aktifkan pembaruan otomatis**, terutama untuk sistem operasi
- **Periksa pembaruan secara berkala** jika pembaruan otomatis tidak tersedia
- Jika Anda menerima permintaan untuk memperbarui sistem operasi atau perangkat lunak lain, Anda harus **menginstal pembaruan itu sesegera mungkin**
- **Tetapkan waktu yang sesuai untuk pembaruan otomatis** guna menghindari gangguan pada bisnis sehari-hari
- Jika Anda menggunakan **perangkat lunak antivirus, pastikan pembaruan otomatis diaktifkan**



CATATAN:

Jika perangkat keras atau perangkat lunak Anda terlalu lama, perangkat tersebut mungkin tidak dapat diperbarui dan dapat membuat bisnis Anda rentan terhadap masalah keamanan.

ACSC menyarankan untuk meningkatkan perangkat atau perangkat lunak Anda sesegera mungkin.

Mulai tahun 2020, Windows 7, Microsoft Office 2010, dan Windows Server 2008 telah mencapai akhir dukungan dan sudah tidak aman.

Untuk informasi selengkapnya, *baca panduan Cepat Tanggap dari ACSC tentang* Akhir Dukungan yang tersedia di cyber.gov.au

Pencadangan Otomatis

Apa? Cadangan data

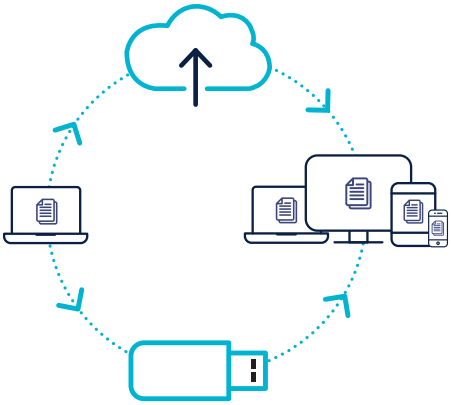
Cadangan adalah salinan digital dari informasi terpenting bisnis Anda, misalnya detail pelanggan dan catatan keuangan. Cadangan dapat disimpan ke perangkat penyimpanan eksternal atau ke cloud.

Pencadangan otomatis merupakan sistem default atau 'tetapkan dan lupakan' yang mencadangkan data Anda secara otomatis, tanpa campur tangan manusia.

Memutuskan dan mencabut perangkat penyimpanan cadangan dengan aman setelah setiap pencadangan akan memastikan perangkat tetap aman selama insiden dunia maya.

Mengapa? Pemulihan sederhana

- **Pencadangan adalah tindakan pencegahan** agar data Anda dapat diakses jika sewaktu-waktu hilang, dicuri, atau rusak
- **Memungkinkan bisnis Anda pulih** dari insiden dunia maya (seperti ransomware) dan meminimalkan waktu henti
- **Melindungi kredibilitas bisnis Anda** dan membantu memenuhi kewajiban hukum^



Kapan? Hari ini & setiap hari

- **Pilih sistem cadangan yang tepat untuk bisnis Anda.** Pertimbangkan apa saja yang tidak merugikan jika hilang dalam skenario terburuk guna membantu memandu persyaratan seperti seberapa sering Anda mencadangkan
data Anda
- **Uji cadangan Anda secara berkala** dengan mencoba memulihkan data
- **Selalu pastikan setidaknya satu cadangan terputus dari perangkat Anda,** sebaiknya di tempat di luar lokasi untuk jaga-jaga jika terjadi bencana alam atau pencurian
- **Jangan hubungkan cadangan Anda ke perangkat yang terinfeksi** dengan ransomware atau virus

^ Industri tertentu memiliki kewajiban untuk menyimpan catatan selama periode waktu tertentu.
Pastikan Anda mengetahui persyaratan penyimpanan data Anda.

Autentikasi Multifaktor

Apa? Tindakan keamanan yang meminta dua bukti identitas atau lebih agar memberi Anda akses

Autentikasi multifaktor (MFA) biasanya meminta kombinasi dari:

- **sesuatu yang Anda ketahui** (kata sandi/frasa sandi,PIN, pertanyaan rahasia)
- **sesuatu yang Anda miliki** (kartu pintar, token fisik, aplikasi autentikator)
- **sesuatu yang menjadi identitas Anda** (sidik jari atau biometrik lainnya).

Mengapa? Keamanan yang jauh lebih kuat

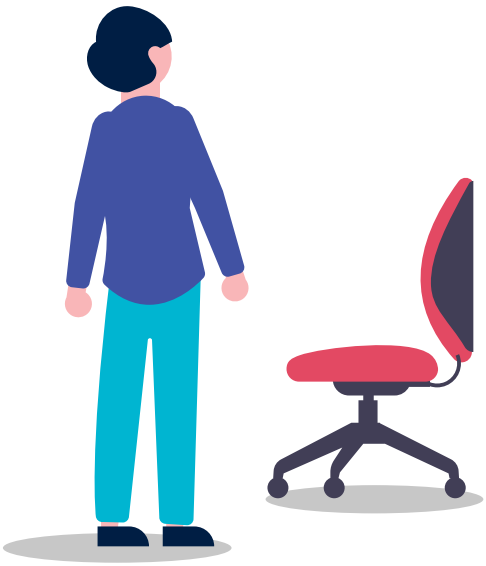
MFA adalah salah satu cara paling efektif untuk mencegah akses tidak sah ke informasi dan akun Anda yang berharga.

Banyaknya lapisan akan sangat menyulitkan penjahat untuk menyerang bisnis Anda. Penjahat mungkin berhasil mencuri satu bukti identitas seperti kata sandi Anda, tetapi mereka masih harus mendapatkan dan menggunakan bukti identitas lainnya untuk mengakses akun Anda.

Di mana? Mengakses akun penting

Bisnis kecil harus sedapat mungkin menerapkan MFA pada akun penting, dengan memprioritaskan akun keuangan dan email. Beberapa opsi MFA termasuk, tetapi tidak terbatas pada:

- Token fisik
- Pin acak
- Biometrik/sidik jari
- Aplikasi autentikator
- Email
- SMS



Karyawan dan Prosedur: **Bidang Utama**

Bisnis, sekecil apa pun, perlu mengetahui dan secara sadar menerapkan langkah-langkah keamanan dunia maya di setiap tingkat.

Proses internal dan tenaga kerja Anda adalah garis pertahanan terakhir, dan salah satu garis pertahanan terpenting dalam melindungi bisnis Anda dari ancaman keamanan dunia maya.

Mengingat bisnis kecil sering kekurangan sumber daya untuk staf TI yang khusus, bagian ini membahas cara mengelola akses ke informasi dalam bisnis Anda, mengamankan akun bisnis Anda, dan melatih staf Anda tantang cara mencegah, mengenali, dan melaporkan insiden keamanan dunia maya.

Kontrol Akses

Apa? Mengelola siapa yang dapat mengakses apa yang ada dalam lingkungan komputasi bisnis Anda

Kontrol akses adalah cara untuk membatasi akses ke sistem komputasi. Kontrol akses membantu melindungi bisnis Anda dengan membatasi akses ke:

- File dan folder
- Aplikasi
- Basis data
- Kotak surat
- Akun online
- Jaringan

Mengapa? Untuk meminimalkan risiko akses tidak sah ke informasi penting

Biasanya, staf tidak memerlukan akses penuh ke semua data, akun, dan sistem dalam bisnis untuk menjalankan peran mereka.

Akses ini harus dibatasi jika memungkinkan, sehingga karyawan dan penyedia eksternal tidak membahayakan bisnis Anda secara tanpa sengaja atau dengan niat jahat.

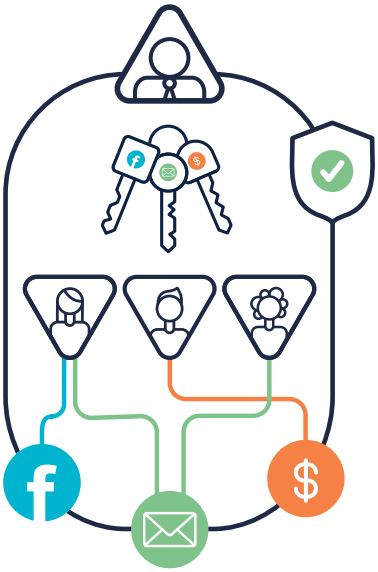
Dengan sistem dan prosedur kontrol akses, pemilik bisnis atau operator dapat:

- **Memutuskan siapa yang boleh mengakses** file, basis data, dan kotak surat tertentu
- **Mengontrol segala akses yang diizinkan ke penyedia eksternal** misalnya akuntan, penyedia hosting situs web
- **Membatasi siapa yang memiliki akses ke akun** seperti situs web pemasok dan media sosial
- **Mengurangi kemungkinan kerusakan** jika ada akun, perangkat, atau sistem yang dibobol
- **Mencabut akses ke sistem dan data** saat karyawan berganti peran atau keluar dari perusahaan

Siapa? Prinsip hak istimewa paling rendah

Bergantung pada sifat bisnis Anda, prinsip hak istimewa paling rendah adalah pendekatan paling aman untuk sebagian besar bisnis kecil.

Prinsip tersebut memberi pengguna izin minimum yang mereka butuhkan untuk melakukan pekerjaan mereka. Hal ini juga mengurangi risiko 'orang dalam' yang membahayakan bisnis Anda secara tanpa sengaja atau dengan niat jahat.



PRINSIP KONTROL AKSES

- **Pindahkan karyawan Anda dari akun 'Administrator' ke akun standar di perangkat bisnis**
- **Tinjau izin akses pada file dan folder digital**
- **Jangan berbagi akun atau frasa sandi/ kata sandi di antara staf**
- **Ingatlah untuk mencabut akses, menghapus akun, dan/atau mengubah frasa sandi/kata sandi saat seorang karyawan keluar, atau jika Anda mengganti penyedia**

Frasa Sandi

Apa? Versi kata sandi yang lebih aman

Autentikasi multifaktor (MFA, lihat halaman 12) adalah salah satu cara paling efektif untuk melindungi akun Anda dari penjahat dunia maya. Namun jika MFA tidak tersedia, maka Anda harus menggunakan frasa sandi untuk melindungi akun Anda.

Frasa sandi menggunakan empat kata acak atau lebih sebagai kata sandi Anda. Misalnya, 'kristal bombai tanah pretzel'.

Mengapa? Aman dan mudah untuk diingat

Frasa sandi sulit untuk dipecahkan oleh penjahat dunia maya, tetapi mudah untuk Anda ingat.

Buat frasa sandi yang:

- **Panjang:** Semakin panjang frasa sandi Anda, semakin baik. Buatlah setidaknya 14 karakter.
- **Tidak dapat diprediksi:** gunakan campuran kata-kata acak yang tidak berkaitan. Jangan pakai frasa, kutipan, atau lirik terkenal.
- **Unik:** Jangan gunakan kembali frasa sandi 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.

Di mana? Akun dan perangkat Anda

Jika Anda tidak dapat menggunakan MFA pada akun atau perangkat, penting untuk menggunakan frasa sandi agar tetap aman. Dalam situasi ini, frasa sandi yang aman mungkin menjadi satu-satunya penghalang yang melindungi informasi berharga Anda dari musuh.

Ingatlah untuk menjadikan frasa sandi Anda unik karena menggunakan kembali kata sandi akan memudahkan penjahat dunia maya untuk meretas banyak akun.

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

PERTIMBANGKAN MENGGUNAKAN PENGELOLA KATA SANDI

Dengan pengelola kata sandi (yang juga dapat digunakan untuk menyimpan frasa sandi), kebiasaan keamanan dunia maya yang baik dapat dilakukan. Memiliki frasa sandi yang unik untuk setiap akun yang berharga mungkin terdengar berlebihan; namun, menggunakan pengelola kata sandi untuk menyimpan frasa sandi Anda akan membebaskan Anda dari tuntutan mengingat frasa sandi mana untuk akun apa. Pastikan pengelola kata sandi yang Anda gunakan berasal dari sumber tepercaya dan bereputasi baik serta dilindungi dengan frasa sandinya sendiri yang kuat dan mudah diingat.

Pelatihan Karyawan

Apa? Edukasi untuk melindungi staf dan bisnis Anda dari ancaman dunia maya

Ajari diri Anda dan staf Anda cara mencegah, mengenali, dan melaporkan kejahatan dunia maya.

Latih karyawan Anda tentang dasar-dasar keamanan dunia maya, termasuk memperbarui perangkat mereka, mengamankan akun mereka, dan mengidentifikasi pesan penipuan.

Anda juga harus mempertimbangkan untuk menerapkan rencana **respons insiden keamanan dunia maya** untuk memandu bisnis dan staf Anda jika terjadi insiden dunia maya.

Tindakan ini akan membantu Anda memahami perangkat dan proses penting Anda, serta kontak utama yang dapat Anda gunakan untuk merespons dan memulihkan.

Mengapa? Karyawan dapat menjadi garis pertahanan pertama dan terakhir melawan ancaman keamanan dunia maya

Pelatihan dapat mengubah kebiasaan dan perilaku staf dan menciptakan pertanggungjawaban bersama dalam menjaga keamanan bisnis Anda.

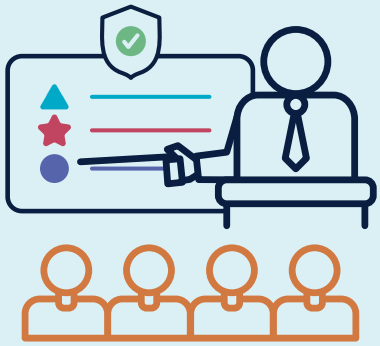
Keamanan dunia maya adalah tanggung jawab semua orang.

Kapan? Kesadaran dan pelatihan keamanan dunia maya secara berkala

Keamanan dunia maya terus berkembang.

Memastikan semua orang tetap tahu info terbaru tentang ancaman keamanan dunia maya dapat mencegah penjahat agar tidak memperoleh akses ke uang, akun, atau data Anda.

> "Ajari diri Anda dan staf Anda cara mencegah, mengenali, dan melaporkan kejahatan dunia maya."



KIAT KESADARAN KEAMANAN DUNIA MAYA

- Latih staf Anda untuk mengenali tautan dan lampiran yang mencurigakan
- Berikan pelatihan keamanan dunia yang diperbarui secara berkala
- Buat rencana respons insiden keamanan dunia maya
- Dorong budaya keamanan dunia maya yang kuat
- Bagikan contoh pesan penipuan untuk membantu staf mengidentifikasi ancaman keamanan dunia maya

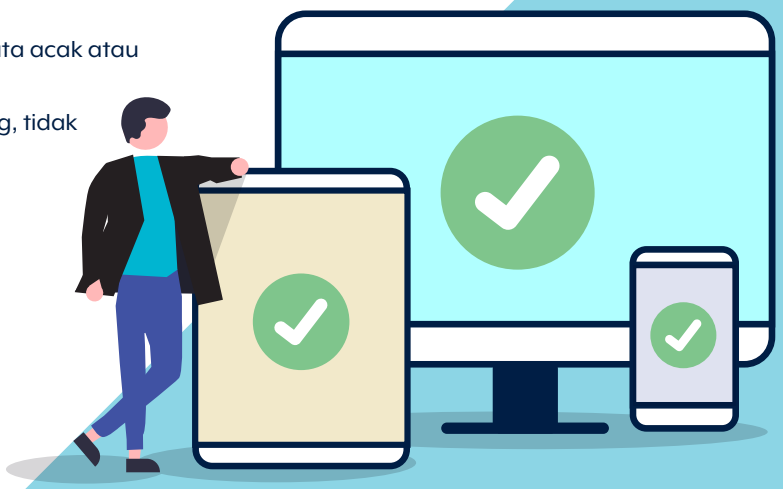
Daftar Periksa Ringkasan

Pertimbangan Perangkat Lunak

- **Perbarui secara otomatis sistem operasi, perangkat lunak, dan aplikasi Anda**
  - Jika Anda menerima permintaan untuk memperbarui sistem operasi atau perangkat lunak lain, Anda harus menginstal pembaruan itu sesegera mungkin
  - Tetapkan waktu yang sesuai untuk pembaruan otomatis guna menghindari gangguan pada bisnis sehari-hari
- **Cadangkan secara berkala data penting Anda**
  - Uji cadangan Anda secara berkala dengan mencoba memulihkan data
  - Selalu pastikan setidaknya satu cadangan tidak terhubung ke perangkat Anda
- **Aktifkan MFA di akun penting bila memungkinkan**
  - MFA adalah salah satu cara paling efektif untuk melindungi informasi dan akun Anda yang berharga
  - Prioritaskan akun keuangan dan email untuk efek maksimal

Karyawan dan Prosedur

- **Kelola siapa yang dapat mengakses apa yang ada dalam bisnis Anda**
  - Gunakan prinsip hak istimewa paling rendah untuk izin akses
  - Ingatlah untuk menghapus akun dan/atau mengubah frasa sandi/kata sandi ketika seorang karyawan keluar
- **Jika MFA tidak dapat digunakan, gunakan frasa sandi untuk melindungi akun dan perangkat**
  - Frasa sandi menggunakan empat kata acak atau lebih sebagai kata sandi Anda
  - Frasa sandi paling efektif jika panjang, tidak dapat diprediksi, dan unik
- **Latih staf Anda tentang dasar-dasar keamanan dunia maya**
  - Aktivitas ini mungkin mencakup memperbarui perangkat mereka, mengamankan akun mereka, dan mengidentifikasi pesan penipuan
  - Berikan pelatihan keamanan dunia yang diperbarui secara berkala



Daftar Istilah

Perangkat Lunak Antivirus
Program perangkat lunak yang dirancang untuk melindungi komputer atau jaringan Anda dari virus komputer.

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).

Biometrik
Identifikasi seseorang berdasarkan pengukuran fitur biologis mereka, misalnya sidik jari atau suara.

Bitcoin
Mata uang digital (mata uang kripto), digunakan di Internet untuk berbagai layanan.

Serangan Brute Force
Jenis serangan yang menghasilkan banyak sekali kombinasi karakter per detik. Serangan ini efektif untuk melawan kata sandi pendek atau satu kata.

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

Penjahat dunia maya
Setiap individu yang secara ilegal meretas sistem komputer untuk merusak atau mencuri informasi.

Data
Data adalah informasi termasuk file, teks, angka, gambar, suara, atau video.

Pengaturan Default
Sesuatu yang telah ditentukan sebelumnya oleh komputer, sistem operasi, atau program untuk pengguna.

Serangan Dictionary
Jenis serangan yang menghasilkan banyak sekali upaya potensial berdasarkan aturan dan basis data. Serangan ini efektif terhadap frasa sandi yang tidak terlalu rumit dan umum digunakan.

Enkripsi
Proses menjadikan data tidak dapat dibaca oleh orang lain dengan tujuan mencegah orang lain mendapatkan akses ke isinya.

Jaringan
Kumpulan komputer, server, mainframe, perangkat jaringan, periferal, atau perangkat lain yang terhubung satu sama lain untuk memungkinkan berbagi data.

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.

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

Spyware
Program yang dirancang untuk mengumpulkan informasi secara diam-diam tentang aktivitas pengguna di perangkat mereka.

Token
Kode aman yang dibuat oleh perangkat fisik atau aplikasi autentikator untuk digunakan selama autentikasi multifaktor. Token juga dapat mengacu pada perangkat fisik yang menghasilkan kode aman yang cukup kecil untuk masuk ke gantungan kunci atau berbentuk seperti kartu kredit.

Trojan
Jenis malware yang sering menyamar sebagai perangkat lunak yang sah, tetapi berisi kode berbahaya yang digunakan oleh penjahat dunia maya untuk mendapatkan akses ke sistem pengguna.

Virus
Program yang dirancang untuk menyebabkan kerusakan, mencuri informasi pribadi, mengubah data, mengirim email, menampilkan pesan, atau kombinasi dari tindakan tersebut.

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.

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