



Australian Government



Bertindak sekarang.
Tetap aman.

Cara tetap aman di internet

Versi Mudah Dibaca



Cara menggunakan panduan ini



Kami adalah Pemerintah Australia.

Kami menulis panduan ini.



Kami menulis beberapa kata dengan **huruf tebal**.

Kami menjelaskan arti kata-kata tersebut.

Daftar kata-kata ini juga terdapat di halaman 28.



Anda dapat meminta bantuan seseorang yang Anda percayai untuk:

- membaca panduan ini
- mencari informasi lebih lanjut.



Ini adalah ringkasan Mudah Dibaca (Easy Read) dari panduan lain.

Ringkasan ini hanya mencakup ide-ide terpenting.



Anda dapat menemukan panduan lainnya di situs web kami.

www.actnowstaysecure.gov.au

Apa isi panduan ini?

Tentang panduan ini	4
Jaga keamanan akun Anda	6
Periksa pengaturan Anda untuk melindungi informasi Anda	10
Lindungi perangkat Anda	16
Penipuan	20
Berani bersuara	25
Daftar kata	28
Hubungi kami	30

Tentang panduan ini



Kita semua perlu memikirkan bagaimana caranya agar tetap aman di internet.

Ini disebut keamanan **siber**.



Siber berarti sesuatu yang berhubungan dengan internet.



Panduan ini menjelaskan beberapa hal yang dapat Anda lakukan untuk melindungi diri Anda secara online.

Misalnya, dari **kejahatan siber**.



Kejahatan siber adalah jika penjahat menggunakan internet untuk melakukan kejahatan. Misalnya, mereka mungkin menggunakan internet untuk:

- mencuri informasi pribadi Anda
- mengambil alih akun atau profil online Anda.

Kejahatan siber dapat terjadi di perangkat apa pun.



Ini termasuk:

- komputer Anda
- HP (Ponsel Pintar) Anda
- jam tangan pintar Anda.



Ada beberapa hal yang dapat Anda lakukan agar tetap aman dari kejahatan siber.



Kami menjelaskan apa yang dapat Anda lakukan di halaman-halaman berikut.

Jaga keamanan akun Anda



Anda harus memikirkan bagaimana Anda dapat menjaga keamanan akun online Anda.

Gunakan frasa sandi yang kuat dan berbeda



Frasa sandi adalah jenis kata sandi yang lebih kuat.

Frasa sandi sangat sulit ditebak oleh orang lain.



Menggunakan frasa sandi yang kuat dan berbeda adalah salah satu cara terbaik untuk melindungi akun Anda.



Anda harus menggunakan frasa sandi yang berbeda untuk masing-masing akun online Anda.



Frasa sandi yang kuat meliputi:

- 4 kata acak atau lebih
- 15 huruf dan angka atau lebih.



Anda dapat menyertakan beberapa huruf besar.



Anda juga dapat menggunakan simbol seperti:

- tanda hubung
- tanda dolar
- tanda email @.



Anda seharusnya jangan gunakan informasi pribadi apa pun dalam frasa sandi Anda.



Misalnya:

- ulang tahun Anda
- nama anggota keluarga atau hewan peliharaan Anda.

Gunakan langkah tambahan untuk masuk ke akun Anda



Anda bisa melindungi akun online Anda dengan autentikasi multifaktor (**multi-factor authentication /MFA**).

MFA adalah saat Anda menggunakan 2 atau lebih cara berbeda untuk masuk ke akun Anda setiap kali.



Misalnya, Anda mungkin perlu memasukkan frasa sandi Anda terlebih dahulu.

Kemudian Anda memasukkan kode yang Anda dapatkan di HP Anda.

Anda mungkin memiliki pilihan untuk:



- menggunakan aplikasi di HP Anda untuk mendapatkan kode



- mendapatkan kode melalui email



- mendapatkan kode melalui pesan teks (SMS).



MFA mempersulit orang lain untuk mengakses akun online Anda.

Bahkan andaikata mereka mengetahui frasa sandi Anda.

Periksa pengaturan Anda untuk melindungi informasi Anda



Anda dapat memeriksa apakah pengaturan Anda melindungi informasi Anda secara online.



Ini termasuk pengaturan pada:

- akun online Anda
- perangkat Anda
- aplikasi Anda.



Anda dapat:

- mengubah pengaturan Anda
- memilih aplikasi mana yang dapat menggunakan informasi Anda.

Anda mungkin dapat menemukan 'pengaturan' (settings) di perangkat Anda dengan:



- mencari ikon roda gigi
atau
- mengetikkan 'pengaturan' (settings) ke bilah pencarian perangkat Anda.



Anda dapat menemukan pengaturan di aplikasi atau akun online dengan membuka menu.

Menu sering kali terlihat seperti 3 garis lurus.



Beberapa pengaturan ini dapat membagikan informasi tentang:

- siapa Anda
- di mana Anda berada
- di mana Anda tinggal.



Membagikan informasi pribadi secara online dapat membuat Anda berisiko terhadap kejahatan siber.



Pelaku kejahatan siber dapat menggunakan informasi Anda untuk berpura-pura menjadi Anda.

Misalnya, mereka mungkin menggunakan informasi seperti:



- di mana Anda tinggal



- nama anggota keluarga Anda



- nama hewan peliharaan Anda.



Anda dapat mengatur akun Anda sehingga hanya orang yang Anda kenal yang dapat melihat profil media sosial Anda.

Misalnya, profil Facebook.



Pengaturan ini biasanya disebut pengaturan privasi (privacy settings).



Anda juga dapat mengontrol **pengaturan lokasi** Anda.

Pengaturan lokasi menunjukkan di mana perangkat Anda berada.



Anda dapat mengaktifkan atau menonaktifkan pengaturan lokasi.

Anda juga dapat memilih aplikasi mana yang dapat menggunakan pengaturan lokasi Anda.



Anda dapat melakukan hal ini untuk:

- akun online Anda
- perangkat Anda
- aplikasi Anda.

Beberapa aplikasi juga mungkin meminta izin untuk:



- menggunakan kamera Anda



- melihat foto Anda.



Anda sebaiknya hanya mengizinkan aplikasi yang Anda kenal untuk menggunakan kamera dan foto Anda.

Lindungi perangkat Anda



Anda sebaiknya mempertimbangkan bagaimana cara melindungi perangkat Anda untuk membantu menjaga keamanan Anda saat online.

Misalnya, HP atau jam tangan pintar Anda.



Ini penting untuk perangkat yang terhubung ke internet.

Perbarui perangkat Anda.



Anda dapat memperbarui perangkat Anda untuk menjaga keamanannya saat online.

Misalnya, HP dan laptop Anda.



Perangkat Anda mungkin menyebut ini sebagai pembaruan perangkat lunak (software update).



Pembaruan membantu perangkat melindungi dirinya dari kejahatan siber.



Anda dapat mengatur perangkat agar diperbarui secara otomatis.



Anda dapat mempelajari lebih lanjut tentang cara memperbarui perangkat Anda di situs web kami.

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

Jaringan Wi-Fi publik



Anda harus berhati-hati saat menggunakan **Wi-Fi publik**.



Wi-Fi publik adalah internet nirkabel gratis yang dapat Anda gunakan di tempat umum.



Misalnya, di sebuah:

- kafe
- bandara
- hotel.



Anda harus berhati-hati dengan informasi apa yang Anda masukkan ke dalam situs web saat menggunakan Wi-Fi publik.



Misalnya:

- rincian bank Anda
- akun email Anda
- profil media sosial Anda.



Ada pelaku kejahatan siber yang dapat menggunakan Wi-Fi publik untuk:

- melihat apa yang Anda lakukan secara online
- mencuri informasi Anda.

Ini karena:



- siapa saja dapat menggunakannya



- lebih sulit untuk melindungi perangkat Anda.



Anda dapat mempelajari cara tetap aman saat menggunakan Wi-Fi publik di situs web kami.

[www.actnowstaysecure.gov.au/](http://www.actnowstaysecure.gov.au/cyber-safe-actions)
[cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

Penipuan



Kami menyebutnya **penipuan (scam)** jika seseorang mencoba:

- menipu Anda
- mengambil uang Anda.



Seorang **penipu (scammer)** adalah seseorang yang melakukan penipuan.

Penipu mungkin mencoba menipu Anda melalui:



- pesan teks atau panggilan telepon
- email
- media sosial
- situs web.



Mereka mungkin tampak ramah.

Namun mereka bisa menipu Anda agar memberinya informasi Anda.

Mereka dapat menggunakan informasi ini untuk:



- masuk ke akun online Anda



- pura-pura menjadi Anda



- mencuri uang Anda.

Penipu juga dapat:



- membuat akun palsu untuk menipu Anda



- membagikan tautan dan iklan agar Anda mengkliknya.

Cara mengenali penipuan

Itu mungkin merupakan penipuan jika seseorang:



- meminta Anda melakukan sesuatu dengan cepat



- menawarkan banyak uang kepada Anda



- meminta uang dari Anda



- meminta Anda mengklik tautan.



Penipu juga mungkin berpura-pura menjadi organisasi yang Anda kenal dan percayai. Misalnya, bank Anda.



Penipu melakukan ini agar Anda mau membagikan informasi pribadi Anda kepada mereka.



Anda sebaiknya berhenti berbicara dengan orang tersebut jika Anda merasa mereka adalah penipu.



Anda harus memeriksa apakah orang tersebut benar-benar seperti yang mereka katakan.

Anda dapat menghubungi orang atau organisasi tersebut menggunakan detail yang Anda percayai dan Anda temukan sendiri.



Bertindak dengan cepat untuk melindungi diri Anda jika ada sesuatu yang terasa tidak benar.

Melaporkan penipuan



Scamwatch membantu orang Australia:

- memahami penipuan
- melaporkan penipuan.



Scamwatch juga membantu orang Australia yang telah mengalami penipuan.



Anda dapat melaporkan penipuan di situs web Scamwatch.

www.scamwatch.gov.au/report-a-scam

Berani bersuara



Anda sebaiknya berbicara tentang bagaimana orang lain dapat melindungi diri mereka sendiri saat online.

Hal ini termasuk:



- melaporkan kejahatan siber



- berbagi pengetahuan Anda dengan keluarga dan teman.



Kami akan menjelaskan bagaimana Anda dapat berani bersuara di halaman-halaman berikutnya.

Laporkan kejahatan siber

Melaporkan kejahatan siber membantu pemerintah:



- mempelajari bagaimana penjahat siber mencoba menyerang orang



- melindungi lebih banyak orang.



Anda dapat melaporkan kejahatan siber di situs web ReportCyber.

www.cyber.gov.au/report

Bicaralah dengan keluarga dan teman tentang cara tetap aman di internet



Anda harus berbagi kiat-kiat tentang cara tetap aman di internet dengan keluarga dan teman Anda.

Anda juga dapat belajar dari mereka.



Anda dapat melindungi diri sendiri dan orang-orang di sekitar Anda dengan membagikan pengetahuan Anda tentang cara tetap aman di internet.



Ini juga penting jika Anda berbagi perangkat dengan orang lain.

Daftar kata

Daftar ini menjelaskan arti kata-kata yang **dicetak tebal** dalam panduan ini.



Siber

Siber berarti sesuatu yang berhubungan dengan internet.

Kejahatan siber



Kejahatan siber adalah jika penjahat menggunakan internet untuk melakukan kejahatan.

Misalnya, mereka mungkin menggunakan internet untuk:

- mencuri informasi pribadi Anda
- mengambil alih akun online Anda.



Pengaturan lokasi

Pengaturan lokasi menunjukkan di mana perangkat Anda berada.



Autentikasi multifaktor (Multi-factor authentication / MFA)

MFA adalah jika Anda menggunakan 2 atau lebih cara berbeda untuk masuk ke akun Anda setiap kali.



Frasa sandi

Frasa sandi adalah jenis kata sandi yang lebih kuat.

Sangat sulit ditebak orang lain.



Wi-Fi publik

Wi-Fi publik adalah internet nirkabel gratis yang dapat Anda gunakan di tempat umum.



Penipuan (scam)

Kami menyebutnya penipuan jika seseorang mencoba:

- menipu Anda
- mengambil uang Anda.



Penipu (scammer)

Seorang penipu adalah seseorang yang melakukan penipuan (scam).

Hubungi kami



Anda dapat menghubungi Australian Cyber Security Hotline (Hotline Keamanan Siber Australia).

1300 292 371



Anda dapat mengunjungi situs web kami.

www.actnowstaysecure.gov.au



Anda dapat melaporkan kejahatan siber di situs web ReportCyber.

www.cyber.gov.au/report



Information Access Group membuat dokumen Mudah Dibaca ini menggunakan foto stok dan gambar khusus. Gambar-gambar tersebut tidak boleh digunakan kembali tanpa izin. Untuk pertanyaan apa pun tentang gambar-gambar tersebut, silakan kunjungi www.informationaccessgroup.com. Sebutkan nomor pekerjaan 6342.
