Ringkasan presentasi online

Australian Government

Be Connected

Every Australian online.

# Dapatkah Anda mengenali penipuan?

Salah satu langkah penting untuk menghindari penipuan adalah bersikap waspada dan memahami cara kerjanya. Setiap tahun, warga lanjut usia di Australia, kehilangan jutaan dollar karena penipuan.

Internet memberikan peluang besar untuk eksplorasi dan sekaligus menjadi sarana penghubung antar satu orang dengan lainnya. Namun kita harus waspada karena tidak semua orang tersebut adalah yang mereka klaim.

Setelah anda mengetahui trik penipuan di dunia siber, maka akan lebih mudah untuk mengenali jenis-jenis penipuan siber.

## Penipuan phishing

Penipuan phishing adalah upaya penipu untuk mengelabui Anda agar percaya bahwa mereka berasal dari organisasi terpercaya atau orang yang Anda kenal agar Anda memberikan informasi pribadi seperti nomor rekening bank, kata sandi, dan nomor kartu kredit Anda.

Pesan phishing dirancang agar tampak asli dan seringkali meniru format yang digunakan oleh organisasi yang dipalsukan oleh penipu, termasuk merek dan logo mereka. Penipuan ini dapat muncul dalam berbagai bentuk, termasuk email, pesan teks, atau panggilan telepon. Misalnya, Anda mungkin menerima:

- pesan teks dari bank Anda yang meminta Anda untuk mengonfirmasi kata sandi Anda
- email dari penyedia internet Anda yang meminta Anda untuk memperbarui detail Anda
- pesan teks dari anggota keluarga yang menggunakan nomor telepon baru yang memberi tahu Anda bahwa mereka kehilangan telepon mereka dan membutuhkan Anda untuk segera mengirimkan uang
- panggilan telepon dari lembaga keuangan Anda untuk memberi tahu Anda tentang 'aktivitas yang tidak sah atau mencurigakan di akun Anda', atau bahwa akun Anda akan ditutup jika Anda tidak memperbarui detail Anda
- pemberitahuan Facebook dari seseorang yang Anda kenal yang merekomendasikan situs web.

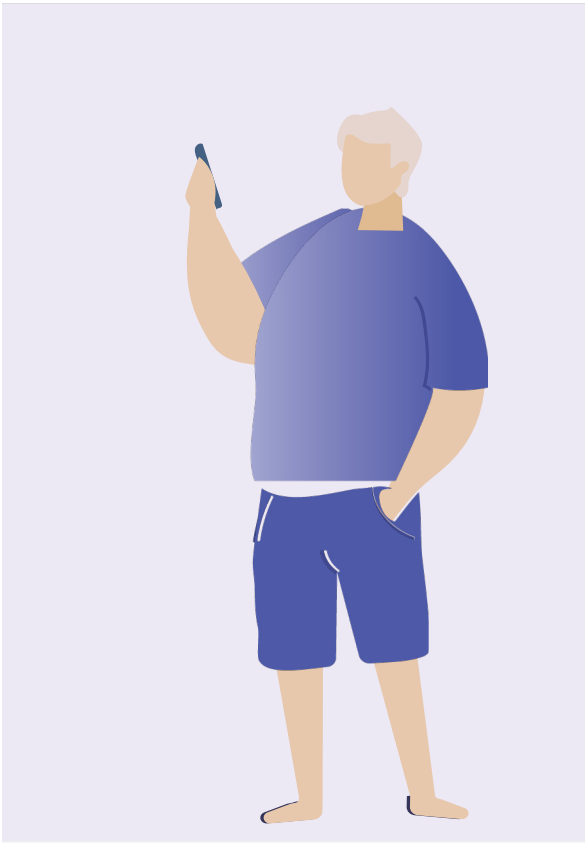
## Penipuan pajak dan Medicare

Penipu menyamar sebagai Kantor Pajak Australia (ATO), Medicare, dan organisasi pemerintah lainnya untuk mencoba menipu Anda agar membayar uang dan membagikan informasi pribadi.

ATO tidak akan pernah mengirim email, SMS, atau menelepon untuk meminta Anda:

- memberikan informasi pribadi seperti nomor berkas pajak, kartu kredit, atau detail bank Anda
- membayar biaya untuk menerima pengembalian pajak Anda, atau untuk terhindar dari penangkapan karena penggelapan pajak
- mengklik tautan untuk memasukkan data pribadi Anda
- mengunduh file atau menginstal perangkat lunak.

Jika Anda kurang yakin apakah komunikasi tersebut berasal dari ATO, hubungi hotline penipuan ATO 1800 008 540 atau kunjungi ato.gov.au/scams.



## Cara melindungi diri

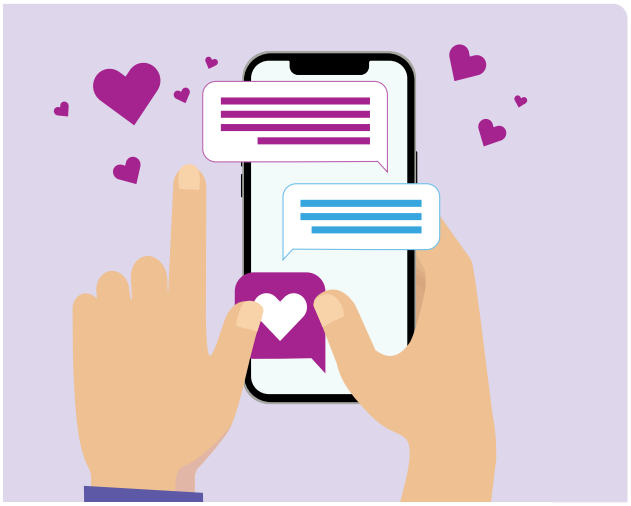
- Jangan terburu-buru. Baca ulang pesannya. Tanyakan pada diri Anda, apakah pesan atau panggilan itu masuk akal?
- Apakah alamat emailnya resmi atau ada yang kurang tepat?
- Kepada siapa pesan itu ditujukan? Bersikaplah curiga jika ditujukan kepada ‘Pelanggan yang terhormat' dan bukan nama Anda.
- Apakah ada kesalahan pengetikan atau kesalahan tata bahasa di email tersebut? Ini bisa menjadi pertanda bahwa email tersebut berasal dari penipu.
- Jangan gunakan detail kontak yang diberikan dalam pesan itu, karena bisa jadi palsu.
- Lakukan pencarian di internet untuk nomor telepon dan situs web resmi organisasi tersebut.
- Jangan mengklik tautan atau membuka lampiran apa pun karena dapat mengunduh virus ke perangkat Anda – cukup tekan hapus.
- Jangan berikan data pribadi seperti nomor berkas pajak (TFN), tanggal lahir, rekening bank, atau rincian kartu kredit.

**Waspada**: Penipu mungkin akan mencoba untuk mempermainkan emosi Anda agar Anda langsung bereaksi tanpa berpikir matang tentang situasi tersebut. Taktik mereka bisa menggunakan ancaman atau denda, bahwa ada pengeluaran/ debit yang tidak sah dari akun Anda, atau bahkan berpura-pura menjadi anggota keluarga Anda yang sedang membutuhkan.

# Penipuan persahabatan dan romantis

Penipu sering memanfaatkan orang yang sedang mencari teman atau pasangan romantis, biasanya melalui situs web kencan, aplikasi, media sosial, atau bahkan permainan daring dengan berpura-pura menjadi calon teman kencan. Tujuan mereka adalah mendapatkan kepercayaan Anda agar Anda bersedia memberikan uang, hadiah, foto intim, atau informasi pribadi.

## Apa yang dapat Anda dilakukan agar sigap dan aman?

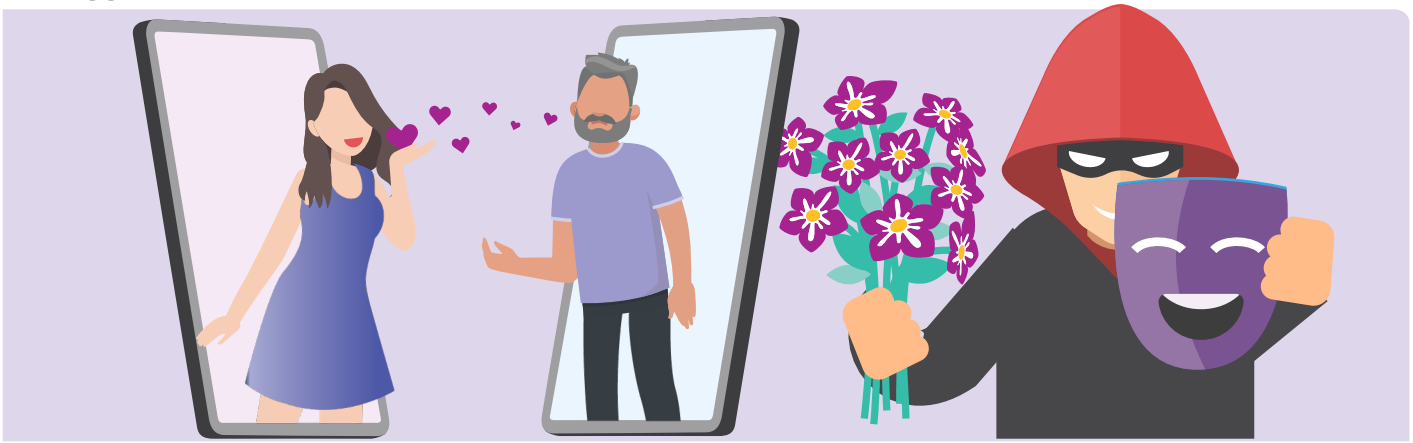


Waspadalah terhadap orang yang::

- mengungkapkan rasa sayang yang mendalam kepada Anda dengan sangat cepat
- setelah berhasil mendapatkan kepercayaan Anda, – sering kali menunggu selama berminggu-minggu, berbulan-bulan atau bahkan bertahun-tahun – menceritakan kisah yang rumit dan meminta uang atau pinjaman, meminta hadiah atau detil rekening bank/kartu kredit Anda
- menghindari pertemuan langsung dengan Anda dan memberi alasan mengapa mereka tidak dapat datang menemui Anda
- memiliki profil daring yang tidak sesuai dengan apa yang mereka ceritakan tentang diri mereka sendiri.

## Cara melindungi diri

- Jangan pernah mengirim uang atau memberikan detil kartu kredit, detail akun online, atau data pribadi kepada orang yang belum pernah Anda temui secara langsung.
- Lakukan pencarian gambar Google akan foto orang tersebut untuk membantu menentukan apakah mereka benar-benar orang yang mereka katakan atau apakah foto tersebut diambil dari internet. Buka images.google.com dan klik ikon kamera.
- Bersikaplah waspada ketika mereka mulai menyinggung masalah keuangan atau membutuhkan uang untuk situasi darurat.
- Waspadalah terhadap hal-hal kecil seperti salah pengejaan dan tata bahasa serta cerita mereka yang tidak konsisten.
- Jangan membagi foto atau video intim. Penipu seringkali memeras target mereka dengan menggunakan materi tersebut.



# Penipuan bantuan teknis

Penipuan ini biasanya dimulai dari telepon atau email yang nampaknya berasal dari perusahaan telekomunikasi atau perusahaan komputer besar, seperti Telstra, NBN, atau Microsoft, untuk memberitahu Anda bahwa komputer atau internet Anda bermasalah dan mereka dapat memperbaikinya. Selanjutnya, mereka akan meminta akses jarak jauh ke komputer Anda dengan alasan untuk 'menemukan masalahnya' atau membujuk Anda agar membeli perangkat lunak atau layanan yang sebenarnya tidak diperlukan untuk 'memperbaiki' komputer tersebut.

## Cara melindungi diri

- Jika Anda tiba-tiba menerima panggilan telepon tentang komputer Anda dan diminta akses jarak jauh – langsung tutup telepon.
- Jangan pernah memberikan akses jarak jauh ke komputer Anda kepada penelepon tak dikenal.
- Jangan bagikan data pribadi Anda seperti rekening bank atau detil kartu kredit Anda.
- Jangan membeli perangkat lunak dari panggilan atau email yang tak dikenal.
- Abaikan pesan pop-up yang meminta Anda untuk menghubungi dukungan teknis.

# Tips handal untuk menghindari penipuan

**Stop**

- Jeda atau berhenti sejenak sebelum memberikan uang atau informasi pribadi kepada siapa pun.
- Penipu akan menawarkan bantuan atau meminta untuk memverifikasi identitas Anda. Mereka menyamar seakan dari organisasi yang dikenal dan dipercaya seperti lawan bisnis Anda, polisi, instansi pemerintah, atau layanan penanggulangan penipuan.

**Pikir**

- Tanyakan pada diri Anda, apakah pesan atau panggilan itu palsu?
- Jangan pernah mengklik tautan dalam pesan dan bertanya kepada teman atau anggota keluarga apa yang akan mereka lakukan. Hubungi bisnis atau instansi pemerintah dengan menggunakan informasi kontak dari situs web resmi mereka atau melalui aplikasi. Jika Anda tidak yakin, katakan tidak, tutup telepon, atau hapus.

**Lindungi**

- Bertindak cepat jika ada yang terasa salah.
- Segera hubungi bank Anda jika Anda kehilangan uang atau data pribadi, atau jika Anda melihat beberapa aktivitas yang tidak biasa pada kartu atau rekening Anda. Cari bantuan dari organisasi seperti IDCARE dan laporkan kejahatan online ke ReportCyber. Bantu orang lain dengan melaporkan penipuan ke Scamwatch.

# Tolong, sepertinya saya tertipu

Jika Anda merasa menjadi korban penipuan, jangan malu dan jangan menyimpannya untuk diri sendiri.Ada beberapa langkah yang dapat diambil untuk memperbaiki masalah tersebut:

- Segera hubungi bank atau lembaga keuangan Anda untuk menghentikan pembayaran lebih lanjut kepada penipu.
- Jika Anda mengalami kejahatan siber dan kehilangan uang secara daring, Anda dapat melaporkannya ke polisi melalui ReportCyber atau kunjungi: cyber.gov.au
- Jika Anda khawatir informasi pribadi Anda telah terekspose dan disalahgunakan, hubungi
- Identitas Nasional Australia dan Layanan Dukungan Siber IDCARE di 1300 432 273 atau idcare.org
- laporkan penipuan tersebut ke ACCC melalui halaman scamwatch.gov.au/report-a-scam. Hal ini akan membantu memperingati orang lain tentang penipuan terkini, memantau tren, dan menghentikan penipuan bila memungkinkan.
- Sebarkan informasi tersebut ke teman dan keluarga Anda untuk melindungi mereka.

**Ingat**: Selalu ada orang yang dapat membantu – baik itu orang-orang di cyber.gov.au atau scamwatch.gov.au, teman atau anggota keluarga yang mengerti teknologi, atau bahkan klub komputer lokal.

Untuk terus mengikuti informasi terkini tentang penipuan yang harus dihindari, berlangganan untuk peringatan email Scamwatch.

# Luangkan waktu untuk mengunjungi situs Be Connected

Be Connected adalah situs web lengkap dengan sumber daya gratis yang dirancang khusus untuk mendukung warga lanjut usia Australia agar dapat terhubung secara daring dengan aman dan menjelajahi dunia digital dengan nyaman. Situs ini juga berguna bagi keluarga dan organisasi masyarakat yang ingin membantu anggota masyarakat lanjut usia mengakses semua manfaat internet.


**kunjungi beconnected.esafety.gov.au**

Australian Government | eSafety Commissioner

Program ini dibuat oleh eSafety sebagai bagian dari inisiatif Be Connected.