Menjaga diri dari Penipuan

CommBank memprioritaskan kepercayaan dan keamanan. Kami melihat semakin banyak pelanggan yang ditekan atau dikelabui oleh penipu agar mengirimkan uang kepada mereka. Penipuan tersebut ada yang sangat canggih dan dilakukan dalam berbagai bentuk. Anda perlu hati-hati dan perlu memberi tahu kami jika ada sesuatu yang terasa tidak beres. Informasi selengkapnya tentang cara melindungi diri Anda dan melaporkan penipuan, baca **commbank.com.au/safe**.

Autentikasi dan Verifikasi

- Isi pemeriksaan keamanan di aplikasi CommBank.
- Aktifkan autentikasi multifaktor untuk menambahkan tahap pemeriksaan dalam membuktikan identitas Anda.
- Gunakan **CallerCheck** untuk memverifikasi identitas penelepon yang mengaku dari bank.
- Gunakan **CustomerCheck** di cabang untuk memverifikasi diri Anda kepada staf kami.
- **NameCheck** akan menunjukkan jika detail akun pada pembayaran pertama kali tampaknya tidak benar.

Kata Sandi & Informasi Pribadi

- Jangan pernah membagikan kata sandi atau PIN, dan berhati-hatilah saat membagikan informasi pribadi.
- Jangan pernah memberikan NetCode Anda kepada siapa pun, termasuk staf CommBank.
- Anda dapat mengubah kata sandi di NetBank dan CommBank kapan saja.
- Buat kata sandi yang kuat dan ubah secara berkala. Untuk tips kami tentang pembuatan kata sandi, buka commbank.com.au/password-security.

Keamanan Alat dan Pembayaran

- Selalu perbarui perangkat lunak antivirus dan lindungi komputer Anda dari ancaman umum.
- Gunakan metode pembayaran yang aman seperti menempelkan atau memasukkan kartu Anda.
- Jangan pinjamkan perangkat Anda yang memiliki akses ke dompet digital Anda.

Email, SMS, dan Online

- Jangan klik tautan dalam email atau SMS yang mencurigakan.
- Jika tidak yakin akan pesan tertentu, diskusikan dengan seseorang yang Anda percayai atau hubungi organisasi tersebut secara langsung melalui detail kontak resmi.
- Tutuplah telepon jika ada panggilan telepon otomatis, mencurigakan, atau mengancam dari pihak ketiga.
- Berhati-hatilah terhadap kontak tak dikenal di media sosial dan platform online.

Berhenti. Periksa. Tolak.

Berhenti. Apakah ada yang terasa tidak beres? Jika ragu, hal terbaik yang harus dilakukan adalah berhenti. Tarik napas.
Periksa. Tanyakan pada orang yang Anda percayai atau hubungi organisasi tersebut secara langsung menggunakan rincian resmi mereka.
Tolak. Matikan teleponnya, hapus emailnya, dan blokir nomor teleponnya. Ganti kata sandi Anda.

Jika Anda yakin Anda adalah korban penipuan, segera hubungi CommBank di **13 22 21**, atau **+61 2 9999 3283** dari luar negeri.

Jika tidak bisa berbahasa Inggris, tersedia Layanan Penerjemahan dan Juru Bahasa gratis dari pemerintah untuk membantu Anda berkomunikasi dengan kami. Layanan ini tersedia dalam lebih dari 150 bahasa. Kami dapat mengatur layanan ini ketika Anda menelepon atau mengunjungi kami di cabang.

Informasi penting tentang penipuan umum

Investasi (Termasuk Kripto)

Para penipu memikat orang dengan menjanjikan keuntungan tinggi, sering kali berupa kripto atau peluang investasi lainnya. Penipu mungkin mencoba menghubungi Anda melalui telepon, email, atau platform media sosial.

Tips untuk melindungi diri sendiri:

- Jika kedengarannya terlalu muluk-muluk, mungkin hal itu adalah penipuan.
- Berhati-hatilah akan penawaran yang tidak diminta dan tekanan untuk berinvestasi atau bertindak cepat.
- Verifikasi terlebih dahulu keabsahan perusahaan atau broker di website ASIC.

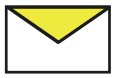
Akses Jarak Jauh

Saat penipu menelepon Anda dan mencoba mendapatkan akses ke rekening atau perangkat Anda, dengan berpura-pura berasal dari perusahaan atau organisasi tepercaya.

Tips untuk melindungi diri sendiri:

- Jangan pernah mengunduh perangkat lunak akses jarak jauh atas permintaan atau di bawah tekanan dari penelepon pihak ketiga.
- Anda selalu dapat menghubungi kembali suatu organisasi menggunakan detail kontak resmi mereka, yang terdapat di situs web resmi mereka.
- Jika ada yang menelepon Anda dan mengaku dari CommBank, Anda selalu dapat meminta kami untuk memverifikasi panggilan tersebut melalui fitur CallerCheck dalam aplikasi.

Penyusupan Email Bisnis



Penipu dapat menyasar suatu bisnis menggunakan email dari alamat yang disusupi, atau email yang dibuat seolah-olah berasal dari kontak tepercaya seperti: asisten, pelanggan, pengacara, manajer, atau pemasok Anda.

Tips untuk melindungi diri sendiri:

- Sebelum melakukan pembayaran pertama kali atau mengubah detail pembayaran, hubungi organisasi tersebut melalui nomor kontak resmi mereka untuk mengonfirmasi detailnya terlebih dahulu.
- Gunakan fitur NameCheck saat melakukan pembayaran, untuk melihat apakah nama rekening sesuai dengan BSB dan nomor rekening yang diberikan.
- Latih karyawan untuk mengenali dan melaporkan upaya phishing.

Phishing dan Smishing

Penipu menggunakan email atau SMS penipuan yang mungkin menyertakan tautan yang mengarahkan Anda ke situs web palsu atau meminta informasi pribadi sensitif.

Tips untuk melindungi diri sendiri:

- Jangan klik tautan dalam email atau SMS yang mencurigakan.
- Anda dapat memastikan keaslian pesan dengan menghubungi organisasi tersebut secara langsung, menggunakan metode kontak resmi yang tersedia.
- Laporkan pesan mencurigakan apa pun dari CommBank ke hoax@cba.com.au

Informasi penting tentang penipuan umum

Hubungan

Penipu membuat profil palsu untuk menjalin hubungan dan memanipulasi korban untuk mengirimkan uang atau informasi pribadi mereka.

Tips untuk melindungi diri sendiri:

- Jangan pernah mengirim uang, atau membagikan kata sandi, kartu kredit, atau detail akun kepada siapa pun yang tidak Anda percayai.
- Periksa calon mitra Anda secara online melalui Google atau aplikasi media sosial. Coba telusuri gambar tersebut untuk mengidentifikasi apakah foto yang dikirimkan kepada Anda adalah milik orang lain.
- Bicarakan dengan keluarga dan teman tentang hubungan online Anda. Mereka mungkin dapat memberikan perspektif dan mengidentifikasi tanda-tanda peringatan yang mungkin tidak Anda sadari.

Belanja Online

Penipu membuat toko online atau iklan untuk memikat pembeli agar membeli produk yang tidak nyata atau palsu.

Tips untuk melindungi diri sendiri:

- Berbelanjalah hanya di situs web yang bereputasi dan aman serta berhati-hatilah terhadap tawaran apa pun yang tampaknya terlalu muluk-muluk.
- Gunakan metode pembayaran yang aman dan hindari transfer langsung ke penjual.
- Jangan terburu-buru atau tertekan oleh karena adanya "penawaran terbatas" atau "hitung mundur" pada akhir masa penjualan.

Kesempatan Kerja

Ketika ada tawaran pekerjaan yang kelihatan hanya memerlukan sedikit atau tanpa usaha untuk mendapatkan keuntungan finansial yang besar, atau menjanjikan keuntungan uang dengan cepat.

Tips untuk melindungi diri sendiri:

- Verifikasi perusahaan dan penawaran melalui jalur resmi, dan periksa perusahaan tersebut untuk memastikan perusahaan tersebut resmi dan memang sedang melakukan perdagangan.
- Berhati-hatilah terhadap tawaran pekerjaan melalui media sosial, obrolan terenkripsi, email, telepon, atau surat dari orang yang belum pernah Anda temui atau perusahaan yang tidak Anda ketahui.
- Perusahaan resmi tidak akan pernah meminta Anda melakukan pembayaran di muka atau menggunakan informasi perbankan pribadi Anda untuk memfasilitasi perdagangan atau dana perusahaan.

Ancaman dan Denda

Penipu menyamar sebagai pihak berwenang atau organisasi tepercaya untuk memeras uang melalui ancaman denda atau tindakan hukum.

Tips untuk melindungi diri sendiri:

- Tutup telepon jika ada yang mengancam dan hubungi organisasi mereka secara langsung.
- Organisasi resmi tidak akan pernah meminta Anda membayar dengan metode yang tidak biasa seperti dengan kartu hadiah atau kartu toko, voucher iTunes, transfer uang, atau Bitcoin.
- Jika Anda mengkhawatirkan keselamatan Anda, hubungi saluran bantuan polisi.

Diterbitkan 01/06/2024