National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

Tetap aman saat online

Mengapa keamanan siber penting bagi saya?

Internet dan sosial media adalah platform mengagumkan yang membantu kita berbagi informasi dan tetap terhubung dengan teman dan keluarga.

Namun, pelaku kejahatan dan organisasi yang melanggar hukum juga menggunakannya untuk mengejar uang Anda, informasi Anda atau untuk mengintimidasi Anda.

Mereka dapat melakukan kegiatan mereka di mana saja dari seluruh dunia, berbicara dengan fasih dalam sebagian besar bahasa, dan membuat situs web yang meyakinkan. Mereka akan menghubungi Anda melalui email, media sosial, dan SMS dan mereka akan mencoba untuk membuat Anda ketakutan dan cemas, sehingga Anda tidak bisa berpikir jernih.

Semua hal ini berarti Anda perlu siaga dan selalu waspada dengan taktik apa pun yang mereka gunakan.

Apa saja beberapa masalah umum yang mungkin saya temukan di online?

Berikut ini adalah beberapa situasi paling umum yang kami perhatikan.

- Anda mendapat email atau SMS mencurigakan yang meminta Anda mengeklik tautan.
    - Sering kali tautan ini mengarahkan ke situs web palsu yang dirancang untuk mencuri login atau perincian keuangan Anda.
- Anda menerima panggilan telepon mencurigakan yang meminta informasi pribadi.
    - Dalam hal ini si penelepon akan berpura-pura dari bank Anda dan meminta informasi.
- Anda dihubungi oleh seseorang yang berpura-pura sebagai petugas yang berwenang, berupaya agar Anda melakukan sesuatu.
    - Sering kali sang petugas melakukan semacam ancaman.
- Seseorang menerobos salah satu atau beberapa akun online Anda (misalnya: email atau media sosial).
    - Jika seseorang menerobos akun online Anda, mereka bisa mencuri informasi, mengalihkan pembayaran, dan kemungkinan menyasar teman atau keluarga Anda dengan berpura-pura menjadi diri Anda.
- Perincian kartu kredit Anda dicuri, atau Anda ditipu sehingga membayar uang dalam penjualan atau investasi palsu.
    - Para penipu berharap Anda akan tergiur dan mau membayar tanpa berpikir. Atau mungkin situs web sungguhan mengalami pelanggaran data dan perincian informasi Anda tersebar secara online.

Kemungkinan skenario lainnya di sini:
Dapatkan bantuan sekarang - Kuasai Online Anda

Cara agar saya tetap aman saat online?

- **Kata sandi yang panjang dan unik.**
    - Semakin panjang kata sandi maka akan semakin aman.
    - Buatlah kata sandi yang mudah diingat dan memiliki lebih dari 16 karakter dengan menggabungkan empat kata secara acak menjadi satu (misalnya: SepatuJalanBadakKampung) dan tambahkan nomor, huruf besar, dan simbol jika diwajibkan (misalnya: 2SepatuJalan"Badak"Kampung&).
    - Hal yang penting adalah jangan mengulangi kata sandi Anda. Jika pelaku kejahatan memperoleh kata sandi Anda, dia akan mencobanya di akun yang lain.
    - Gunakan manajer kata sandi untuk mengingat kata sandi Anda dan untuk membuat kata sandi baru.
    - Buat kata sandi yang kuat - Kuasai Online Anda
- **Aktifkan pengamanan autentikasi dua faktor.**
    - Ini adalah informasi tambahan – biasanya dalam bentuk kode di ponsel – yang diperlukan untuk masuk ke situs web.
    - Cara ini sangat ampuh dan dapat menggagalkan hampir semua upaya untuk menerobos akun Anda.
    - Saran kami Anda gunakan 'aplikasi pengautentikasi' yang mendukung.
    - Buat autentikasi dua faktor (2FA) - Kuasai Online Anda
- **Jaga privasi saat online.**
    - Pilihan terbaik agar tetap aman di media sosial adalah dengan mengaktifkan pengaturan privasi Anda.
    - Ini akan menghentikan orang yang tidak dikenal, termasuk pelaku kejahatan siber, sehingga mereka tidak dapat melihat postingan Anda atau mengirimkan pesan kepada Anda.
    - Tetap berhat-hati sewaktu memposting informasi tentang diri sendiri, keluarga atau teman Anda.
    - Pastikan mereka yang mengaku sebagai kontak adalah memang demikian.
    - Waspada dengan permintaan pertemanan palsu. Hati-hati dengan orang yang tidak dikenal yang mengaku sebagai wartawan atau profesi lainnya.
    - Lindungi privasi Anda saat online - Kuasai Online Anda
- **Pastikan semuanya telah diperbarui.**
    - Ketika Anda memperbarui ponsel, komputer atau perangkat lunak Anda, secara bersamaan langkah ini juga akan menutup celah keamanan yang mungkin ada.
    - Pelaku kejahatan selalu mencari cara untuk menerobos masuk dan menemukan bagian yang membutuhkan perbaikan kerentanan.
    - Mulai ulang perangkat Anda secara rutin.
    - Terus lakukan pembaruan - Kuasai Online Anda

- **Waspadai penipuan.**
    - Nasihat terbaik adalah waspada dengan semua penipuan ini dan tetap berhati-hati jika pelaku kejahatan berupaya atau menghubungi Anda di platform online apa pun.
    - Jika terasa ada yang salah, jangan berurusan dengan orang yang menghubungi Anda itu. Khususnya perlu berhati-hati jika mereka minta uang, walaupun terlihat ramah.
    - Amati apakah ada keanehan pada tautan atau alamat email (misalnya: bank Anda tidak akan mengirimkan email kepada Anda dari akun gmail).
    - *Jangan pernah* mengeklik tautan yang ada di pesan teks.
    - Unduh aplikasi ke perangkat Anda hanya dari toko aplikasi resmi.
    - Jika Anda ragu, langsung hubungi organisasinya dan jangan gunakan tautan atau nomor telepon apa pun yang diberikan.
    - Selalu waspada akan risiko keamanan online untuk diri sendiri, komunitas Anda, maupun kelompok di mana Anda bergabung.
- **Lindungi informasi Anda.**
    - Gunakan aplikasi pengiriman pesan yang terenkripsi, seperti Signal. Dengan begitu orang lain tidak dapat membaca pesan Anda.
    - Hanya bagikan informasi Anda dengan situs web yang beralamat dengan awalan HTTPS. Huruf S adalah singkatan dari "secure" (aman) dan artinya semua informasi yang dikirimkan antara Anda dan situs web tersebut akan dienkripsi.
    - Pertimbangkan untuk menggunakan virtual private network (VPN) yang dapat melindungi data dan menyembunyikan lokasi Anda.
    - Pastikan izin dan data apa saja yang dapat diakses oleh aplikasi Anda. Misalnya, aplikasi kebugaran tidak memerlukan akses ke kontak Anda.

Apa yang bisa saya lakukan jika saya ditipu atau mengalami hal yang lebih buruk?

Ada banyak tempat untuk memperoleh bantuan. Semua organisasi ini tidak akan memberikan perincian informasi Anda kepada pihak lain, kecuali Anda memberikan izin.

- Anda bisa melaporkan insiden siber ke NCSC melalui portal CERT NZ dan kami dapat membantu atau menghubungkan Anda dengan instansi lainnya:
  Laporkan insiden | CERT NZ
- Jika kehilangan uang, Anda harus langsung menghubungi bank.
- SMS penipuan dapat diteruskan, tanpa biaya, ke nomor 7726, sebuah layanan yang disediakan oleh Department of Internal Affairs.