National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

Menjaga keselamatan dalam talian

Mengapa keselamatan siber penting untuk saya?

Internet dan media sosial ialah platform hebat yang membantu kami berkongsi maklumat dan kekal berhubung dengan rakan dan keluarga.

Walau bagaimanapun, penjenayah dan organisasi lain yang menyalahi undang-undang juga menggunakannya untuk cuba mendapatkan wang anda, maklumat anda atau untuk menakutkan anda.

Mereka boleh beroperasi dari mana-mana sahaja di dunia, fasih bercakap kebanyakan bahasa dan mencipta tapak web palsu yang meyakinkan. Mereka akan menghubungi anda melalui e-mel, media sosial dan mesej teks dan mereka akan cuba membuat anda berasa takut atau cemas, menjadikan anda tidak berfikir dengan jelas.

Semua ini bermakna anda perlu bersedia dan sentiasa sedar tentang helah yang mereka gunakan.

Apakah beberapa isu biasa yang mungkin saya temui dalam talian?

Berikut adalah beberapa situasi yang paling biasa kita lihat.

- Anda mendapat e-mel atau mesej teks yang mencurigakan yang meminta anda mengklik pautan.
    - Pautan ini selalunya membawa kepada tapak web palsu yang direka untuk mencuri log masuk atau butiran kewangan anda.
- Anda mendapat panggilan yang mencurigakan dan meminta maklumat peribadi.
    - Seperti di atas, pemanggil akan berpura-pura dari bank anda dan meminta maklumat.
- Anda menerima komunikasi daripada seseorang yang berpura-pura menjadi orang yang berkuasa, cuba mendorong anda melakukan sesuatu.
    - Biasanya orang itu akan mengugut anda.
- Seseorang masuk ke satu atau lebih akaun dalam talian anda (contohnya: e-mel atau media sosial).
    - Jika seseorang masuk ke akaun dalam talian anda, mereka boleh mencuri maklumat, mengubah hala pembayaran dan berpotensi menyasarkan rakan atau keluarga anda dengan berpura-pura menjadi anda.
- Butiran kad kredit anda dicuri, atau anda ditipu daripada wang dalam penjualan atau pelaburan palsu.
    - Penipu berharap anda akan melihat tawaran yang baik dan ingin membayar tanpa berfikir. Atau mungkin tapak web sebenar terperangkap dalam pelanggaran data dan butiran anda bocor dalam talian.

Terdapat lebih banyak senario di sini: Dapatkan
Get help now - Own Your Online (Dapatka bantuan sekarang - Miliki Dalam Talian Anda)

Bagaimanakah saya boleh kekal selamat dalam talian?

- **Kata laluan yang panjang dan unik.**
    - Lebih panjang kata laluan, lebih kuat ia.
    - Cipta kata laluan yang tidak dapat dilupakan dengan lebih daripada 16 aksara dengan menggabungkan empat perkataan rawak bersama-sama (contohnya: TriangleRhinoOperationShoes) dan menambah nombor, huruf besar dan simbol jika diperlukan (contohnya: Triangle&"Rhino"Operation2Shoes).

    - Yang penting, jangan ulangi kata laluan anda. Jika penjenayah mendapat salah satu kata laluan anda, mereka akan mencubanya pada akaun lain.
    - Gunakan pengurus kata laluan untuk mengingati kata laluan anda dan untuk membuat kata laluan baharu.
    - Cipta kata laluan yang baik - Miliki Dalam Talian Anda (Own Your Online)

- **Gunakan pengesahan dua faktor (2FA).**
    - Ini adalah maklumat tambahan – biasanya kod pada telefon anda – yang anda perlukan untuk log masuk ke tapak web.
    - Teknik ini sangat kuat dan boleh menghentikan kebanyakan percubaan untuk masuk ke akaun anda.
    - Kami mengesyorkan menggunakan 'app pengesah', di mana ini disokong.
    - Sediakan pengesahan dua faktor (2FA) - Miliki Dalam Talian Anda (Own Your Online)
- **Kekal peribadi dalam talian.**
    - Pilihan terbaik untuk kekal selamat di media sosial ialah menggunakan tetapan privasi anda.
    - Ini akan menghentikan orang rawak, termasuk penjenayah siber, dapat melihat siaran anda atau menghantar mesej kepada anda.
    - Tetap berhati-hati menyiarkan maklumat peribadi tentang diri anda, keluarga anda atau rakan anda.
    - Pastikan kenalan adalah orang yang dikatakan.
    - Berhati-hati dengan permintaan rakan palsu. Berhati-hati dengan orang yang mendakwa sebagai wartawan atau orang lain yang anda tidak kenali.
    - Lindungi privasi anda dalam talian - Miliki Dalam Talian Anda (Own Your Online)
- **Pastikan semuanya dikemaskinikan.**
    - Apabila anda mengemas kini telefon, komputer atau perisian anda, ia menutup sebarang lubang yang mungkin terdapat pada keselamatan juga.
    - Penjenayah sentiasa mencari cara untuk masuk dan kemas kini membetulkan kelemahan.
    - Mulakan semula peranti anda dengan kerap.
    - Ikuti perkembangan terkini anda - Miliki Dalam Talian Anda (Own Your Online)
- **Berhati-hati dengan penipuan.**
    - Nasihat terbaik adalah untuk mengetahui penipuan-penipuan ini dan berhati-hati terhadapnya.
    - Jika ada yang tidak kena, jangan berhubung dengan orang yang menghubungi anda. Terutamanya, berhati-hati jika mereka meminta wang, walaupun mereka kelihatan mesra.
    - Cari pautan pelik dan alamat e-mel (contohnya: bank anda tidak akan menghantar e-mel kepada anda daripada akaun Gmail).
    - *Jangan sekali-kali* mengklik pautan dalam mesej teks.
    - Hanya muat turun app ke peranti anda daripada gedung app rasmi.
    - Jika tidak pasti, hubungi organisasi yang menghubungi anda secara langsung dan jangan ikuti sebarang pautan atau nombor telefon yang anda hantar.
    - Cuba sentiasa peka tentang risiko keselamatan dalam talian untuk diri anda, komuniti anda dan mana-mana kumpulan yang anda sertai.
- **Lindungi maklumat anda.**
    - Gunakan app pemesejan yang disulitkan, seperti Signal. Ini akan menghalang sesiapa sahaja daripada dapat membaca mesej anda.

- Hanya kongsi maklumat dengan tapak web jika alamat bermula dengan HTTPS. S bermaksud "selamat" dan bermaksud sebarang maklumat yang dihantar antara anda dan tapak web disulitkan.
- Pertimbangkan untuk menggunakan rangkaian persendirian maya (VPN) yang boleh melindungi data anda dan menyembunyikan lokasi anda.
- Semak data dan kebenaran yang boleh diakses oleh apl anda. Contohnya, app kecergasan tidak memerlukan akses kepada kenalan anda.

Apakah yang perlu saya lakukan jika saya ditipu atau lebih teruk lagi?

Terdapat banyak tempat yang boleh anda pergi untuk mendapatkan bantuan. Organisasi ini tidak akan berkongsi butiran anda dengan orang lain, melainkan anda memberikan persetujuan anda.

- Anda boleh melaporkan insiden siber kepada NCSC melalui portal CERT NZ dan kami boleh membantu atau menghubungi anda dengan agensi lain:
  Laporkan insiden (Report an incident) | CERT NZ
- Jika anda kehilangan wang, anda harus menghubungi bank anda dengan segera.
- Mesej teks penipuan boleh dimajukan, secara percuma, ke 7726, perkhidmatan yang dikendalikan oleh Jabatan Hal Ehwal Dalam Negeri.