National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

Pastikan organisasi anda selamat dalam talian

Mengapa keselamatan siber penting untuk kumpulan dan organisasi komuniti?

Halaman ini mempunyai nasihat dan beberapa langkah yang anda boleh ambil untuk melindungi kumpulan komuniti atau organisasi anda daripada ancaman keselamatan siber. Terdapat juga panduan berasingan untuk individu.

Nasihat ini berdasarkan ancaman yang paling biasa dan serius.

- Kemas kini – pastikan perisian pada peranti anda dikemas kini supaya tiada lubang dalam keselamatan.
    - Pastikan peranti kumpulan komuniti atau organisasi anda dikemaskini. Ini termasuk telefon, komputer, penghala WiFi dan apa sahaja yang bersambung ke Internet – termasuk peranti pintar.
    - Gunakan kemas kini automatik jika tersedia.
- Pengesahan dua faktor (2FA) – menambah keselamatan tambahan pada akaun anda dengan memerlukan kata laluan dan satu langkah lagi, seperti kod daripada aplikasi pada telefon anda.
    - Nota: Ini dipanggil pengesahan berbilang faktor (MFA), pengesahan dua langkah (2SV) dan banyak nama lain.
    - Gunakan 2FA pada semua akaun kumpulan komuniti atau organisasi anda.
    - Jika boleh, cuba gunakan bentuk 2FA yang tahan pancingan data, yang bermaksud anda tidak boleh ditipu untuk menyerahkannya. Ini mungkin kunci keselamatan fizikal atau sesuatu seperti cap jari atau ID muka.
- Beri perhatian kepada akaun dalam talian anda – pastikan bekas ahli tidak menyimpan akses mereka kepada akaun selepas meninggalkan kumpulan komuniti atau organisasi.
    - Jika anda mempunyai lebih daripada seorang yang mengakses akaun yang sama, pastikan mereka semua mempunyai log masuk yang berbeza dan semuanya menggunakan 2FA.
    - Simpan senarai semua akaun pengguna dan matikan mana-mana akaun yang tidak diperlukan, seperti apabila kakitangan meletak jawatan.
    - Simpan daftar mana-mana peranti yang telah anda berikan kepada ahli anda dan pastikan ia dipulangkan, dan set semula status kilangnya jika orang itu meninggalkan organisasi. Anda juga mungkin perlu menukar kod fizikal untuk akses bangunan.
- Semak siapa yang mempunyai akses kepada akaun dalam talian anda – orang dalam kumpulan komuniti atau organisasi anda seharusnya mempunyai akses kepada perkara yang mereka perlukan sahaja.
    - Jika akaun seseorang dicerobohi, langkah ini menghadkan bahaya yang boleh dilakukan oleh penyerang.

    - Semak dan alih keluar kebenaran laluan yang tidak diperlukan dengan kerap.
    - Jika anda mempunyai satu akaun "admin" yang digunakan oleh berbilang orang, perhatikan untuk aktiviti luar biasa. Cuba hadkan mempunyai akaun seperti ini, terutamanya untuk tugas harian.
    - Peraturan ini juga digunakan untuk akses pentadbir kepada peranti, seperti mesin penghala.
- Semak kontrak anda dengan pembekal perkhidmatan – jika anda telah mengupah sesiapa untuk menjalankan perkhidmatan IT untuk anda.
    - Pastikan mereka mempunyai perlindungan keselamatan siber untuk memenuhi keperluan kumpulan komuniti atau organisasi anda.
- Ketahui cara semua akaun dan sistem anda berfungsi bersama – memahami sambungan membantu anda mengetahui tempat penyerang boleh masuk.
    - Semak sambungan antara sistem anda, contohnya, e-mel, storan awan dan platform perakaunan.
    - Pertimbangkan untuk menggunakan Rangkaian Peribadi Maya (VPN) untuk keselamatan dalam talian tambahan. Menggunakan VPN menyembunyikan aktiviti dalam talian anda daripada sesiapa sahaja yang mungkin cuba menjejaki anda. Ini amat bagus jika mana-mana ahli kumpulan komuniti atau organisasi anda berhubung dari jauh.
- Pastikan orang anda 'cerdas siber' – orang dalam kumpulan komuniti atau organisasi anda lebih cenderung untuk disasarkan daripada sistem anda.
    - Latih semua kakitangan dalam keselamatan siber asas. Halaman web "Own Your Online" website Own Your Online (Miliki Dalam Talian Anda) | NCSC mempunyai pelbagai nasihat dan petua untuk membantu memastikan diri anda selamat dalam talian dan cara mengesan penipuan.
    - Ingatkan mereka bahawa ini penting untuk akaun peribadi mereka dan juga akaun yang mereka gunakan untuk organisasi anda.
    - Kami mempunyai panduan untuk individu juga. Keeping safe online (Menjaga keselamatan dalam talian) | Ministry for Ethnic Communities (Kementrian Komuniti Etnik)
- Rancang untuk insiden – menyediakan pelan tindak balas adalah penting untuk mengelakkan orang ramai daripada panik apabila insiden berlaku.
    - Pelan tindak balas insiden menerangkan siapa yang melakukan apa semasa kejadian. Templat tersedia di sini Incident Management (Pengurusan Insiden) | NCSC
    - Sertakan rancangan untuk tindakan yang perlu dilakukan jika telefon, komputer atau sistem lain gagal. Pastikan rancangan ini dikemas kini.
    - Simpan butiran hubungan semua orang yang diperlukan dan butiran sandaran jika cara utama untuk menghubungi mereka rosak (seperti e-mel).
    - Simpan pelan di tempat di luar sistem anda juga, sekiranya anda tidak dapat mencapainya.