National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

Pagpapanatiling ligtas ng inyong organisasyon sa online

Bakit mahalaga ang cyber security para sa mga grupong pangkomunidad at organisasyon?

Ang pahinang ito ay may mga payo at ilang mga hakbang na inyong magagawa upang protektahan ang inyong grupong pangkomunidad o organisasyon laban sa mga banta sa cyber security. Mayroon ding hiwalay na gabay para sa mga indibidwal upang panatilihing ligtas ang kanilang sarili sa online.

Ang mga payong ito ay batay sa mga pinaka-karaniwan at pinakamalubhang banta.

- Mga update – panatilihing up to date ang software sa inyong mga device upang matapalan ang anumang butas sa security.
    - Panatilihing up to date ang mga device ng inyong grupong pangkomunidad o organisasyon. Kabilang dito ang mga telepono, kompyuter, WiFi router, at anumang bagay na nakakonekta sa internet – pati mga smart device.
    - Gamitin ang awtomatikong pag-update (automatic updates) hangga't maaari.
- Two-factor authentication (2FA) – nagbibigay ng karagdagang seguridad sa inyong mga account sa pamamagitan ng paghiling ng password at isa pang hakbang, gaya ng code mula sa isang app sa inyong telepono.
    - Tandaan: Ito ay tinatawag ding multi-factor authentication (MFA), two-step verification (2SV) at marami pang ibang mga tawag.
    - I-on ang 2FA sa lahat ng mga account ng inyong grupong pangkomunidad o organisasyon.
    - Hangga't maaari, sikaping gumamit ng isang uri ng 2FA na lumalaban sa phishing, ibig sabihin, hindi ka malolokong ibigay ito. Ito ay maaaring isang pisikal na security key o isang bagay tulad ng fingerprint o face ID.
- Subaybayan ang mga account ninyo sa online – tiyakin na ang mga dating miyembro ay hindi na nakaka-access sa mga account matapos silang umalis sa grupong pangkomunidad o organisasyon.
    - Kung mayroon kayong mahigit sa isang tao na uma-access sa mismong account na iyon, tiyakin na iba-iba ang kanilang log in, at lahat ay may 2FA na naka-on.
    - Gumawa ng listahan ng lahat ng mga user account at gawing hindi na aktibo ang alinmang hindi na kailangan, gaya halimbawa kung umalis na sa grupo o organisasyon ang mga tauhan.
    - Gumawa ng rehistro ng anumang mga device na inyong ibinigay sa inyong mga miyembro at tandaang ibalik sa inyo ang mga ito at gawan ng factory reset ang mga device kung umalis na sa organisasyon ang taong iyon. Maaaring kailanganin din ninyong palitan ang mga pisikal na code para sa pag-access sa gusali.
- Tingnan kung sino ang may access sa inyong mga account sa online – ang mga tao sa inyong grupong pangkomunidad o organisasyon ay dapat lamang maka-access sa mga bagay na kailangan nila.

- Kung maha-hack ang account ng isang tao, malilimitahan ng mga hakbang na ito ang pinsala na maaaring gawin ng umaatake.
- Regular na tingnan at alisin ang mga hindi kinakailangang pahintulot (permissions).
- Kung kayo ay may isa lamang "admin" account na ginagamit ng maraming tao, subaybayan ito para sa hindi pangkaraniwang aktibidad. Sikaping limitahan ang pagkakaroon ng ganitong uri ng mga account, lalo na para sa mga pang-araw-araw na gawain.
- Ang mga tuntuning ito ay nakalapat din sa pag-access ng administrator sa mga device, gaya ng mga router.

- Rebyuhin ang inyong mga kontrata sa mga tagapagbigay ng serbisyo (service providers) – kung kumuha kayo ng sinuman para magpatakbo ng mga serbisyong IT para sa inyo.
  - Tiyakin na mayroon silang umiiral na mga proteksyon sa cyber security upang matugunan ang mga pangangailangan ng inyong grupong pangkomunidad o organisasyon.
- Alamin kung paano gumagana nang magkakasama ang lahat ng inyong mga account at sistema – ang pag-unawa sa mga koneksyon ay tutulong sa inyo na malaman kung saan maaaring makapasok ang umaatake.
  - Rebyuhin ang mga koneksyon ng inyong mga sistema, halimbawa, email, cloud storage, at mga accounting platform.
  - Pag-isipang gumamit ng Virtual Private Network (VPN) para sa karagdagang kaligtasan sa online. Sa paggamit ng VPN, itatago nito ang inyong aktibidad sa online mula sa sinuman na maaaring magtangkang subaybayan kayo. Lalo itong mainam kung ang sinumang miyembro ng inyong grupong pangkomunidad o organisasyon ay remote ang pagkonekta.
- Panatilihing 'cyber smart' ang inyong mga miyembro – ang mga tao sa inyong grupong pangkomunidad o organisasyon ay mas malamang na matarget kaysa sa inyong mga sistema.
  - Sanayin ang lahat ng tauhan sa mga importanteng cyber security. Ang website ng Own Your Online Own Your Online | NCSC ay may malawak na hanay ng mga payo at tip na makatutulong panatilihin kayong ligtas sa online at kung paano makikilala ang mga scam.
  - Ipaalala sa kanila na mahalaga ito para sa kanilang mga personal na account pati na rin sa mga account na kanilang ginagamit para sa inyong organisasyon.
  - Mayroon kaming gabay para sa mga indibidwal upang panatilihin ding ligtas ang kanilang sarili sa online.
- Magplano para sa isang insidente – mahalagang magkaroon ng umiiral na planong pantugon upang maiwasang matakot ang mga tao kapag may nangyaring insidente.
  - Ang isang planong pantugon sa insidente (incident response plan) ay naglalarawan kung sino ang gagawa ng ano sa oras ng isang insidente. Ang mga template ay available dito Incident Management | NCSC
  - Magsali ng plano kung ano ang gagawin kung hindi gagana ang mga telepono, kompyuter, o iba pang mga sistema. Panatilihing up to date ang planong ito.

- Magkaroon ng mga detalye ng pagkontak sa lahat ng mga kailangang tao at mga detalye ng backup kung ang pangunahing paraan ng pagkontak sa kanila ay sira (gaya ng email).
- Ilagay din ang plano sa labas ng inyong sistema, sakaling hindi ninyo ito makuha.