National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

Pananatiling ligtas sa online

Bakit mahalaga ang cyber security sa akin?

Ang internet at social media ay kahanga-hangang mga platform na tumutulong sa atin na magbahagi ng impormasyon at manatiling nakikipag-ugnayan sa mga kaibigan at pamilya.

Subali't ang mga ito ay ginagamit din ng mga kriminal at iba pang labag sa batas na mga organisasyon upang tangkaing kunin ang iyong pera, ang iyong impormasyon o upang takutin ka.

Sila ay gumagana saanman sa mundo, matatas magsalita ng karamihan sa mga wika at lumilikha ng mga nakakukumbinsing website na peke. Kokontakin ka nila sa pamamagitan ng email, social media at text message at sisikapin nilang takutin o gawin kang balisa, kaya hindi ka na makapag-isip nang malinaw.

Ang lahat ng ito ay nangangahulugan na dapat kang maging handa at laging may kamalayan sa mga panlilinlang na ginagamit nila.

Ano ang ilan sa mga karaniwang isyu na maaari kong makita sa online?

Ang mga ito ay ilan sa mga pinaka-karaniwang sitwasyon na nakikita natin.

- Makakatanggap ka ng kahina-hinalang email o text message na humihiling na i-click mo ang link.
    - Ang mga link na ito kadalasan ay hahantong sa mga pekeng website na idinisenyo para nakawin ang iyong login o mga detalye ng iyong pananalapi.
- Makakatanggap ka ng kahina-hinalang tawag na humihiling ng personal na impormasyon.
    - Ang tumatawag ay nagpapanggap na siya ay mula sa iyong bangko at humihingi ng impormasyon.
- Makakatanggap ka ng komunikasyon mula sa isang tao na nagpapanggap na isang taong may awtoridad, at tatangkaing ipagawa sa iyo ang isang bagay.
    - Kadalasan, ang taong ito ay magbabanta.
- May nakapasok na isa o mahigit pa sa iyong mga online account (halimbawa, email o social media).
    - Kung may nakapasok sa iyong online account, maaari niyang nakawin ang impormasyon, mag-redirect ng mga pagbabayad, at maaaring ma-target ang iyong mga kaibigan o pamilya sa pamamagitan ng pagpapanggap na siya ay ikaw.
- Nanakaw ang mga detalye ng iyong credit card, o na-scam ka ng pera sa isang pekeng pagbebenta o pamumuhunan.
    - Umaasa ang mga scammer na makakakita ka ng magandang alok at gugustuhin mong magbayad nang hindi nag-iisip. O baka naman ang tunay na website ay nasangkot sa isang paglabag sa mga datos (data breach) at ang iyong mga detalye ay nabunyag sa online.

May karagdagan pang mga sitwasyon dito:
Get help now - Own Your Online

Paano ako mananatiling ligtas sa online?

- **Mga password na mahaba at bukod-tangi.**
    - Kung mas mahaba ang password, mas matatag ito.
    - Gumawa ng memorableng password na mas higit pa sa 16 na character sa pamamagitan ng pagkakabit-kabit ng apat na hindi pinipiling mga salita (halimbawa: TriangleRhinoOperationShoes), tapos ay dagdagan ng mga numero, malalaking titik at simbolo kung kailangan (halimbawa: Triangle&"Rhino"Operation2Shoes).
    - Mas mahalaga, huwag uulitin ang iyong mga password. Kapag nakuha ng isang kriminal ang isa sa iyong mga password, tatangkain niyang gamitin ito sa iba pang mga account.
    - Gumamit ng password manager para matandaan mo ang iyong mga password at para lumikha ng mag bagong password.
    - Gumawa ng mababuting password – Own Your Online
- **I-on ang two-factor authentication.**
    - Karagdagang impormasyon ito – karaniwan ay isang code sa iyong telepono – kailangan mong mag-log in sa isang website.
    - Ang paraang ito ay labis-labis na matatag at makakapigil sa karamihan ng mga pagtatangkang pasukin ang iyong mga account.
    - Inererekomenda namin ang paggamit ng 'authenticator app', kung saan ito ay sinusuportahan.
    - Mag-set up ng two-factor authentication (2FA) - Own Your Online
- Manatiling pribado sa online.
    - Ang pinakamahusay na opsyon para manatiling ligtas sa social media ay ang pag-turn on ng iyong mga privacy setting.
    - Pipigilan nito ang mga ala-suwerteng mga tao, kabilang ang mga cybercriminal, na makita ang iyong mga post o magpadala sa iyo ng mga message.
    - Lagi pa ring mag-ingat sa pagpo-post ng mga personal na impormasyon tungkol sa iyo, sa iyong pamilya o sa iyong mga kaibigan.
    - Tiyakin na totoong sila nga ang sinasabing mga contact.
    - Maging alerto sa mga pekeng humihiling na maging friend mo. Mag-ingat sa mga taong sinasabi na sila ay mga mamamahayag (journalists) o iba pang tao na hindi mo masyadong kilala.
    - Protektahan ang iyong pagkapribado sa online - Own Your Online
- **Laging i-update ang lahat.**
    - Kapag nag-update ka ng iyong telepono, kompyuter o software, babarahan din nito ang anumang mga butas na mayroon sa seguridad.

- Ang mga kriminal ay laging naghahanap ng mga paraan para makapasok at naaayos ng mga update ang mga kahinaan.
- Mag-restart ka ng iyong device nang madalas.
- Laging mag-update - Own Your Online

- **Maging alerto sa mga scam.**
  - Ang pinakamainam na payo ay magkaroon ng kamalayan sa mga scam na ito at maging alerto sa mga ito kung tatangkain ng mga kriminal na kontakin ka sa anumang online platform.
  - Kung may anumang bagay na tila mali, huwag makipag-usap sa taong kumontak sa iyo. Lalo pang maging maingat kung hihingi siya ng pera, kahit na tila mabait siya.
  - Mag-ingat sa mga kakaibang link at email address (halimbawa, hindi magpapadala ng email sa iyo ang iyong bangko mula sa isang Gmail account).
  - *Huwag na huwag* mag-click sa mga link sa mga text message.
  - Mag-download lamang ng mga app sa iyong device mula sa mga opisyal na app store.
  - Kung nagdududa ka, kontakin mo nang direkta ang organisasyon at huwag susundan ang anumang mga link o numero ng telepono na ipinadala sa iyo.
  - Sikaping manatiling may kamalayan sa mga panganib sa online security para sa iyong sarili, sa inyong komunidad, at sa anumang grupo na kinabibilangan mo.
- **Protektahan ang iyong impormasyon.**
  - Gumamit ng mga encrypted messaging app, gaya ng Signal. Pipigilan nito ang sinuman na makabasa ng iyong mga mensahe.
  - Magbahagi lamang ng impormasyon sa isang website kung ang address nito ay nagsisimula sa HTTPS. Ibig sabihin ng S ay "secure" at nangangahulugan na ang anumang impormasyong ipapadala mo at ng website sa isa't isa ay encrypted.
  - Pag-isipang gumamit ng virtual private network (VPN) na maaaring magprotekta ng iyong mga datos at magtago ng iyong lokasyon.
  - Tingnan kung anong mga datos at pahintulot (permissions) ang naa-access ng iyong mga app. Halimbawa, hindi kailangang ma-access ng isang fitness app ang iyong mga contact.

Ano ang dapat kong gawin kung ako ay na-scam o mas grabe pa?

Marami kang mapupuntahang mga lugar para sa tulong. Lahat ng mga organisasyong ito ay hindi magbabahagi ng iyong mga detalye kaninuman, maliban kung nagbigay ka ng pahintulot.

- Maaari kang magsumbong ng mga insidenteng cyber sa NCSC sa pamamagitan ng CERT NZ portal at matutulungan ka namin o iuugnay ka sa ibang ahensya:
  Magsumbong ng insidente | CERT NZ
- Kung nawalan ka ng pera, dapat mong kontakin kaagad ang iyong bangko.
- Ang mga scam text message ay maaaring ipadala, nang libre, sa 7726, isang serbisyong pinapatakbo ng Department of Internal Affairs.