Manatiling Ligtas Laban sa mga Scam

Tiwala at seguridad ang aming pangunahing prayoridad sa CommBank. Nakikita namin ang dumaraming kaso kung saan pinipilit o nililinlang ng mga scammer ang mga kostumer na magpadala ng pera sa kanila. Ang mga scam na ito ay maaaring sopistikado at may iba't ibang anyo. Mahalagang bantayan at ipaalam sa amin kung may isang bagay na parang hindi tama. Upang malaman ang higit pa kung paano poprotektahan ang iyong sarili at magre-report ng scam, tingnan ang **commbank.com.au/safe**.

Pagpapatotoo at Pagpapatunay

- Kumpletuhin ang security check-up sa CommBank app.
- Paganahin ang multi-factor authentication, na may karagdagang pagsusuri para mapatunayan ang iyong pagkakakilanlan.
- Gamitin ang **CallerCheck** para patunayan ang pagkakakilanlan ng mga tumatawag na nagsasabing sila ay mula sa bangko.
- Gamitin ang **CustomerCheck** sa sangay para patunayan ang iyong sarili sa aming mga kawani.
- Didiktahan ka ng**NameCheck** kung ang mga detalye ng account sa pangunang pagbabayad ay mukhang hindi tama.

Seguridad ng Device at Pagbabayad

- Panatilihing napapanahon ang anti-virus software at protektahan ang iyong computer laban sa mga karaniwang banta.
- Gumamit ng mga ligtas na paraan ng pagbabayad tulad ng pag-tap o pagpasok ng iyong card.
- Huwag magpahiram ng mga device na may access sa iyong digital wallet.

Password at Personal na Impormasyon

- Huwag kailanman magbahagi ng mga password o PIN, at mag-ingat kapag nagbabahagi ng personal na impormasyon.
- Huwag kailanman ibigay ang iyong NetCode kaninuman, maging sa mga kawani ng CommBank.
- Maaari mong baguhin ang iyong password sa NetBank at sa CommBank app anumang oras.
- Lumikha ng malakas na password at regular itong palitan Para sa aming mga tip sa paglikha ng password, bisitahin ang commbank.com.au/password-security.

Email, SMS at Online

- Huwag mag-click ng mga link sa kahina-hinalang mga email o SMS.
- Kung hindi ka sigurado tungkol sa isang mensahe, kausapin ang taong pinagkakatiwalaan mo o direktang makipag-ugnayan sa organisasyon sa pamamagitan ng mga opisyal na detalye ng kontak.
- Mag-hang up sa mga awtomatiko, kahina-hinala o nagbabantang tawag sa telepono mula sa mga third party.
- Maging maingat sa mga hindi kilalang contact sa social media at online na mga platform.

Huminto. Suriin. Tanggihan.

Huminto. Mukha bang may hindi tama? Kung may pagdududa, ang pinakamagandang gawin ay huminto. Huminga ka.
Suriin. Magtanong sa isang taong pinagkakatiwalaan mo o direktang makipag-ugnayan sa organisasyon, gamit ang kanilang mga opisyal na detalye.
Tanggihan. Babaan ng telepono ang tumatawag, i-delete ang email, i-block ang numero ng telepono. Palitan ang iyong mga password

Kung naniniwala ka na biktima ka ng isang scam, makipag-ugnayan kaagad sa CommBank sa **13 22 21**, o **+61 2 9999 3283** mula sa ibang bansa.

Kung hindi Ingles ang iyong unang wika, ang libreng Serbisyo sa Pagsasalinwika at Interpreter ng pamahalaan ay makakatulong sa iyo na makipag-ugnayan sa amin. Ang serbisyong ito ay magagamit sa mahigit 150 na mga wika. Maaari naming ayusin ang serbisyong ito kapag tinawagan mo kami o binisita kami sa sangay.

Mga bagay na dapat mong malaman: Hindi kami kailanman magpapadala sa iyo ng email o SMS na humihingi ng impormasyon sa pagbabangko tulad ng iyong NetBank Client ID, password, o NetCode; o maglagay ng link para mag-log on nang direkta mula sa isang email o SMS. Palaging i-type ang commbank.com.au sa isang browser o gamitin ang CommBank app upang ligtas na magawa ang iyong pagbabangko. Kung may mukhang kahina-hinala mula sa CommBank, i-forward ito sa hoax@cba.com.au at i-delete ito. Commonwealth Bank of Australia ABN 48 123 123 124 AFSL at Australian credit licence 234945.

Mahalagang impormasyon tungkol sa mga karaniwang scam

Pamumuhunan (Kasama dito ang Crypto)

Inaakit ng mga scammer ang mga indibidwal sa pangako ng mataas na kita, kadalasang kinasasangkutan ng crypto o iba pang mga oportunidad sa pamumuhunan. Maaaring subukan ng mga scammer na makipag-ugnayan sa iyo sa pamamagitan ng telepono, email, o sa mga social media platform.

Mga tip para protektahan ang iyong sarili:

- Kung parang napakaganda para maging totoo, malamang hindi nga ito totoo.
- Maging maingat sa mga hindi mo naman hinihinging mga alok (offers) at pamimilit sa iyong mamuhunan o kaya umaksyon kaagad.
- Hilingin na patunayan ang pagiging lehitimo ng kumpanya o broker sa ASIC website.

Malayuang Pag-access (Remote Access)

Kung saan tinatawagan ka ng isang scammer at sinusubukang makakuha ng access sa iyong mga account o device, habang nagpapanggap na mula sa isang pinagkakatiwalaang kumpanya o organisasyon.

Mga tip para protektahan ang iyong sarili:

- Huwag kailanman mag-download ng remote access software dahil hinilingan ka o pinipilit ng isang third-party na tumatawag.
- Maaari mong tawagan ang isang organisasyon anumang oras sa kanilang mga lehitimong detalye ng kontak, na makikita sa kanilang opisyal na website.
- Kung nakatanggap ka ng tawag na nagsasabing siya ay mula sa CommBank, maaari mong hilingin sa amin anumang oras na patunayan ang tawag sa pamamagitan ng in-app na CallerCheck.

Nakompromisong Business Email

Maaaring targetin ng mga scammer ang mga negosyo na may mga email mula sa isang nakompromisong address, o mga email na pinagmukhang parang nagmula sa isang pinagkakatiwalaang contact gaya ng: iyong assistant, kostumer, abogado, manager o supplier.

Mga tip para protektahan ang iyong sarili:

- Bago gumawa ng mga pangunang pagbabayad o magpalit ng mga detalye ng pagbabayad (payment details), tawagan ang organisasyon sa kanilang opisyal na contact number upang kumpirmahin muna ang mga detalye.
- Gamitin ang NameCheck kapag nagbabayad, para makita kung tumutugma ang pangalan ng account sa BSB at account number na ibinigay.
- Sanayin ang mga empleyado na kilalanin at iulat ang mga sumusubok mag-phishing.

Phishing at Smishing

Gumagamit ang mga scammer ng mga mapanlinlang na email o text message na maaaring may kasamang link na nagdidirekta sa iyo sa isang mapanlinlang na website o humingi ng sensitibong personal na impormasyon.

Mga tip para protektahan ang iyong sarili:

- Huwag mag-click ng mga link sa kahina-hinalang mga email o SMS.
- Maaari mong kumpirmahin ang pagiging tunay ng isang mensahe sa pamamagitan ng direktang pakikipag-ugnayan sa organisasyon, gamit ang kanilang mga opisyal na paraan ng pakikipag-ugnayan.
- Iulat ang anumang kahina-hinalang mensahe mula sa CommBank sa hoax@cba.com.au

Mahalagang impormasyon tungkol sa mga karaniwang scam

Ugnayan

Ang mga scammer ay gumagawa ng mga pekeng profile upang bumuo ng mga relasyon at manipulahin ang mga biktima na magpadala ng pera o personal na impormasyon.

Mga tip para protektahan ang iyong sarili:

- Huwag magpadala ng pera, o magbahagi ng mga password, credit card o mga detalye ng account sa sinumang hindi mo pinagkakatiwalaan.
- Magsaliksik tungkol sa iyong potensyal na kasosyo sa online sa pamamagitan ng Google o mga social media app. Subukan ang reverse image search para matukoy kung may ibang nagmamay-ari ng mga larawang ipinadala sa iyo.
- Makipag-usap sa iyong pamilya at mga kaibigan tungkol sa iyong online na ugnayan. Maaaring magbigay sila ng kanilang pananaw at matukoy ang mga palatandaan ng babala (warning signs) na maaaring hindi mo napansin.

Online Shopping

Gumagawa ang mga scammer ng mga online store o mga ad para akitin ang mga mamimili na bumili ng mga hindi totoo o pekeng produkto.

Mga tip para protektahan ang iyong sarili:

- Mag-shop lamang sa mga napatunayan na at ligtas na mga website at mag-ingat sa anumang alok na mukhang napakaganda para maging totoo.
- Gumamit ng mga ligtas na paraan ng pagbabayad at iwasan ang mga direct transfer sa mga nagbebenta.
- Huwag magmadali o ma-pressure ng 'mga limited offer' o 'mga end of sale countdown'.

Oportunidad sa Pagtatrabaho

Kung ang alok na trabaho ay nangangailangan lamang ng kaunti o halos walang kahirap-hirap para kumita ng malaki, o nangangako na kikita kaagad ng pera.

Mga tip para protektahan ang iyong sarili:

- Patunayan na totoo ang kumpanya at ang inaalok sa pamamagitan ng mga opisyal na channel, at magsaliksik tungkol sa kumpanya upang matiyak na sila ay lehitimo at kasalukuyang nakikipagkalakalan.
- Mag-ingat sa mga alok ng trabaho sa pamamagitan ng social media, naka-encrypt na chat, email, telepono o sulat mula sa mga taong hindi mo pa nakikilala o mga kumpanyang hindi mo kilala.
- Hindi kailanman hihilingin sa iyo ng isang lehitimong kumpanya na magbigay ng paunang bayad o gamitin ang iyong personal na impormasyon sa pagbabangko (personal banking information) upang mapadali ang mga pondo o kalakalan ng kumpanya.

Banta at Multa

Ang mga scammer ay nagpapanggap bilang mga awtoridad o pinagkakatiwalaang organisasyon upang mangikil ng pera sa pamamagitan ng mga banta ng multa o ligal na aksyon.

Mga tip para protektahan ang iyong sarili:

- I-hang up ang tawag sa nagbabantang mga tumatawag at direktang makipag-ugnayan sa organisasyon.
- Ang isang lehitimong organisasyon ay hindi kailanman hihilingin sa iyo na magbayad sa pamamagitan ng mga hindi pangkaraniwang paraan gaya ng mga gift o store card, iTunes voucher, wire transfer o Bitcoin.
- Kung nag-aalala ka para sa iyong kaligtasan, makipag-ugnayan sa linya ng tulong ng pulisya.