Panatilihing ligtas ang sarili:
alamin ang mga scam at panloloko

Maaaring dumami ang mga scam at panloloko na may kinalaman sa COVID-19 sa mga darating na buwan.

Gumagamit ng mga pekeng email, mga tawag sa telepono o mga text message ang mga scammer para subukan at kumuha ng personal na impormasyon. Nagkukunwari silang mula sa iyong bangko, World Health Organization, gobyerno, mga charity o mga lehitimong negosyo tulad ng mga travel agent, elektrisidad, provider ng telepono o internet, o sa inyong lokal na supermarket.

Protektahan ang Sarili

HINDI KAILANMAN magpapadala ng email o text message ang bangko mo para humingi ng mga detalye ng anumang account o pananalapi, kabilang dito ang pag-update ng address o mga detalye ng pag-log in mo sa Telepono, Mobile o Internet Banking.

HINDI KAILANMAN hihilingin sa iyo ng gobyerno at iba pang lehitimong organisasyon na i-update ang mga detalye mo sa pamamagitan ng pag-click sa isang link. Kung nagdududa, makipag-usap sa isang kaibigan o miyembro ng pamilya, o makipag-ugnayan at direktang magtanong sa organisasyon.

Kung nakatanggap ka ng tawag mula sa isang tao na hindi mo kilala na nagtatanong ng personal na impormasyon, IBABA ITO. Direktang tumawag sa kumpanya at tanungin kung tumawag sila.

HUWAG magbukas ng mga attachment mula sa mga tao o organisasyon na hindi mo kilala. Mag-ingat sa mga alok na masyadong hindi kapani-paniwala o nagtatanong ng sobrang impormasyon.

Makakatulong ang bangko mo, makipag-ugnayan kaagad sa kanila kapag:

- naibahagi mo ang iyong mga detalye sa bangko bilang tugon sa isang mapanlinlang na tawag sa telepono, email o text
- aksidente mong na-click ang anumang link o na-download ang anumang attachment
- napansin mo ang anumang hindi pangkaraniwang transaksyon sa iyong account.

Paano matutukoy ang isang scam

- Sinabihan ka na i-update o kumpirmahin ang mga personal na detalye, kabilang ang address, petsa ng kapanganakan, mga detalye ng bank account, numero ng tax file, o anumang PIN o password.
- Naglalaman ang email o text message ng mga kahina-hinalang link. Kung hindi ka sigurado, humingi ng tulong sa isang kaibigan o miyembro ng pamilya.
- Hiningan ka ng agarang pagbabayad o gumawa ng paunang pagdeposito.
- Kung sobra-sobra ang iniaalok, maaaring isa itong scam.
- Hindi tugma ang email address sa kumpanya.
- Humihiling ang tumatawag ng isang remote na pag-access sa computer mo.

Australian Banking Association

www.ausbanking.org.au

Mga nangungunang tip para protektahan ang iyong impormasyon sa pananalapi mula sa mga scam at panloloko

- Ibaba ang mga kahina-hinalang tawag, at sa halip ay pumunta sa website ng mga kumpanya o hanapin ang kanilang numero at direkta silang tawagan.
- Huwag kailanman ibahagi ang mga password o PINs. Protektahan ng password ang mga device mo. Kung may kahati ka sa paggamit ng computer, huwag kailanman i-save ang mga password at palaging i-log out ang account mo.
- Palaging tingnan ang mga bank account mo para malaman mo kaagad kung may mga kahina-hinalang transaksyon.
- Iwasang magpa-swipe ng mga card mo kapag namimili. Ang pag-tap at pagpasok ay kadalasang mas ligtas.
- I-block ang mga cash advance sa mga credit card.
- Kausapin ang bangko mo tungkol sa pinakamagandang paraan para protektahan ang account mo.
- Kung sa tingin mo ay na-scam ka, i-ulat ito kaagad sa bangko mo.

Maraming paraan na susubukan kang nakawan ng mga manloloko, narito ang mga pangunahing paraan.

Phishing – Isang email o text ang ginagamit para makakuha ng personal na impormasyon mo sa pamamagitan ng pagkukunwari na galing ito sa isang mapagkakatiwalaang mapagkukunan tulad ng bangko, charity, o gobyerno. Mukhang totoo ang mensahe at kadalasang magtatanong sa iyo ng personal na impormasyon gamit ang mga pekeng website o sasabihan ka na i-click ang isang link-papahintulutan nito ang manloloko na ma-access ang iyong computer at personal na impormasyon.

Mga Online shopping scam – nagkukunwari ang mga scammer bilang mga totoong tindahan online, maaaring gamit ang isang pekeng website o pekeng ad mula sa isang totoong retail site. Ang mga pekeng online shopping site ay madalas na humihiling ng mga hindi karaniwang paraan ng pagbabayad tulad ng paunang pagbabayad sa pamamagitan ng money order, wire transfer, international funds transfer o mga gift card.

Mga Investment scam – nagkukunwari ang scammer na mga stockbroker o portfolio manager na nag-aalok ng financial o investment advice. Sasabihan ka nilang magbigay ng pera para sa isang oportunidad na investment na maaaring totoo o maaaring hindi, at pagkatapos ay kukunin nila ang pera mo.

Mga Remote access scam – nagkukunwari ang scammer na mayroong problema sa computer o koneksyon ng internet mo, o na-infect ito ng malware. Susubukan ka nilang kumbinsihin na mag-install ng isang application o bigyan mo sila ng access sa computer mo. Gagamitin nila ito para maaccess ang iyong personal na impormasyon o hihingi ng "bayad" para sa pag-aayos ng problema.

Mga Relationship at dating scam – makikipagrelasyon sa iyo ang scammer para makahingi ng pera o mga regalo. Makikipagrelasyon sila sa pagdaan ng panahon at hihilingin sa iyo na mag-transfer ng mga ari-arian sa kanilang pangalan o hihilingin na maging benepisyaryo ng kayamanan mo. Kadalasan, hihingi sila ng pera para sa kalusugan, pagbibiyahe o problema sa pamilya.

MGA KAPAKI-PAKINABANG NA LINK:

www.ausbanking.org.au/safe-savvy-a-guide-to-help-older-people-avoid-abuse-scams-and-fraud

www.esafety.gov.au/seniors/staying-safer-online

www.scamwatch.gov.au/

Mahalagang paalala: Ang fact sheet na ito ay nagbibigay ng pangkalahatang kaalaman at hindi ito inilaan para asahan mo bilang payo sa anumang partikular na bagay. Dapat kang makipag-ugnayan sa bangko mo kung paano magiging angkop ang impormasyong ito sa mga sitwasyon mo.