ISUMBONG ANG MGA CYBER-ATTACK AT INSIDENTE UPANG MAPANATILI ANG SEGURIDAD SA AUSTRALYA.

MAGPALISTA

Sa aming libreng serbisyo ng alerto
cyber.gov.au

ISUMBONG

Ang cybercrime sa REPORTCYBER:
cyber.gov.au/report

MAKIPAG-UGNAY

Tumawag sa 1300 CYBER1 o bisitahin ang cyber.gov.au

Itong numero ay magagamit lamang sa loob ng Australya.

SUNDAN KAMI

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5. MAG-INGAT SA MGA SCAM

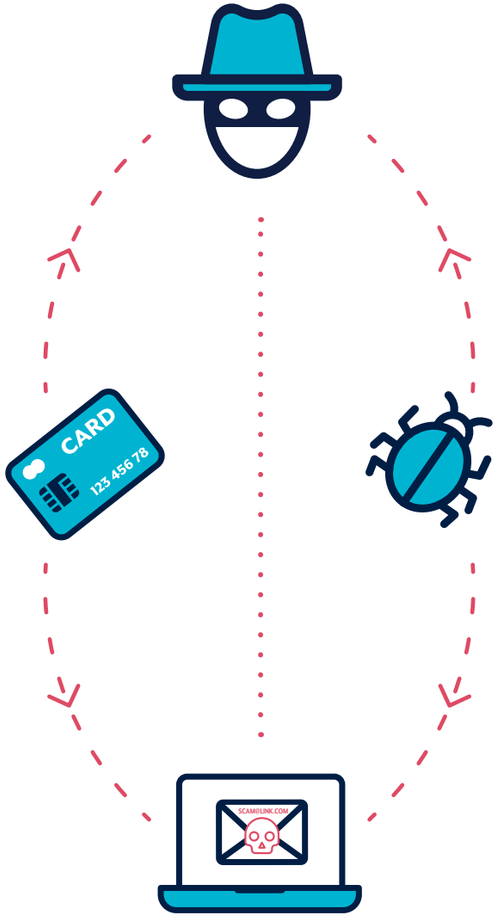
Ang mga cybercriminal ay gumagamit ng email, SMS, mga tawag sa telepono at social media upang linlangin ka na buksan ang isang attachment, bisitahin ang isang website, ibunyag ng mga detalye ng account login, isiwalat ang sensitibong impormasyon o ilipat ang pera o mga gift card. Ang mga mensaheng to ay ginawa na parang ipinadala mula sa mga indibidwal o organisasyon na sa tingin mo ay kilala mo, o sa tingin mo ay dapat paniwalaan.

Upang makilala ang mga mensaheng scam, huminto at mag-isip:

- **Awtoridad:** Ang mensahe ba ay nagpapanggap na mula sa taong opisyal?
- **Pagmamadali:** Sinabi ba sa iyo na mayroon kang limitadong panahon na magresponde?
- **Emosyon:** Ang mensahe ba ay ginagawa kang natataranta, natatakot, umaasa o nagtataka?
- **Kakulangan:** Ang mensahe ba ay nag-aalok ng isang bagay na nakakapus?
- **Kasalukuyang mga pangyayari:** Ang mensahe ba ay nauugnay sa mga kasalukuyang balita, malalaking mga kaganapan o partikular na mga panahon ng taon (tulad ng pag-uulat ng buwis)?

Upang masuri kung ang isang mensahe ay lehitimo:

- Bumalik sa isang bagay na mapagkakatiwalaan mo. Bisitahin ang opisyal na website, mag-log in sa iyong account, o tawagan ang kanilang inanunsiyong numero ng telepono. Huwag gamitin ang mga link o mga detalye ng pakikipag-ugnay sa mensaheng ipinadala sa iyo o ibinigay sa telepono.
- Tingnan kung ang opisyal na pinagmulan ay nagsabi na sa iyo kung ano ang hindi nila kailanman itatanong sa iyo. Halimbawa, maaaring sinabi na sa iyo ng iyong banko na hindi nila kailanman tatanungin ang iyong password.



Para sa karagdagang impormasyon sa pagkilala ng mga mensaheng scam, tingnan ang paglalathalang Detecting Socially Engineered Messages ng Australian Cyber Security Centre (ACSC), at magkaroon ng kamalayan sa pamamagitan ng pagpalista sa Alert Service (Serbisyong Pag-alerto) ng ACSC sa **cyber.gov.au.**

MADALING MGA HAKBANG

UPANG BIGYAN NG SEGURIDAD ANG IYONG MGA GADYET AT MGA ACCOUNT

BAWASAN ANG PANGANIB NA MAGING TARGET NG MGA CYBERCRIMINAL SA PAMAMAGITAN NG PAGSUNOD SA MGA SUMUSUNOD NA MGA HAKBANG

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1. GAWING NAPAPANAHON (UPDATED) ANG IYONG MGA GADYET

Ang mga cybercriminal ay nagha-hack ng mga gadyet gamit ang mga kilalang kahinaan ng mga sistema o mga app. Ang mga update ay may mga pag-upgrade sa seguridad upang ayusin ang mga kahinaan na ito. Paganahin ang automatic updates upang mangyayari ito nang walang aksyon mula sa iyo.

Paganahin ang automatic updates sa lahat ng iyong mga gadyet:

- Teleponong mobile
- Laptop
- Desktop

Palaging tingnan kung may mga update para sa iyong:

- Mga app
- Mga programa
- Mga smart na gadyet

2. PAGANAHIN ANG MULTI-FACTOR AUTHENTICATION (MFA)

Pinapabuti ng MFA ang iyong seguridad sa pamamagitan ng pagdaragdag sa kahirapan ng mga cybercriminal na ma-access ang iyong mga file o account.

Paganahin ang MFA, mag-umpisa sa iyong pinakamahalagang mga account:

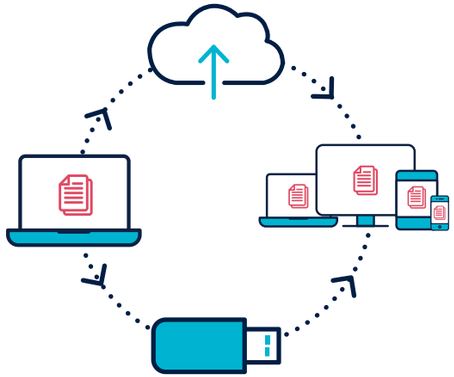
- Mga account ng email
- Mga pagbabangko sa online at mga account na may nakalagay na detalye ng pagbabayad
- Social media

3. I-BACK UP ANG IYONG MGA GADYET

Ang backup ay isang kopyang digital ng impormasyon na nakalagay sa iyong gadyet, tulad ng mga larawan, dokumento, video, at datos mula sa mga application. Maaari itong i-save sa isang external storage device o sa cloud. Ang pagba-back up ay nangangahulugan na maaari mong ibalik ang iyong mga files kung sakaling ang gadyet ay nawala, ninakaw, o nasira.

Palaging i-back up ang iyong mga gadyet:

- Teleponong mobile
- Laptop
- Desktop
- Tablet



4. MAGLAGAY NG MGA SECURE NA PASSPHRASE

Sa mga kaso kung saan walang magagamit na MFA, ang isang may seguridad na passphrase ay kadalasang ang tanging bagay na magpoprotekta sa iyong impormasyon at mga account laban sa mga kriminal.

Ang isang passphrase ay gumagamit ng apat o higit pang mga random na salita bilang iyong password. Palitan ang iyong mga password ng mga passphrase, sinisigurado na ang mga ito ay:

- Mahaba: Kung mas mahaba ang iyong passphrase, mas mabuti. Gawin itong hindi bababa sa 14 letra ng haba
- Hindi mahuhulaan: Gumamit ng isang random na halo ng hindi magkakaugnay na mga salita
- Kakaiba: Huwag muling gamitin ang mga passphrase sa iba't-ibang mga account