Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

PANSARILING SEGURIDAD SA CYBER

MGA UNANG HAKBANG

cyber.gov.au

Serye ng Pansariling Seguridad sa Cyber

Ang ***Personal Cyber Security: First Steps Guide*** ay una sa serye ng tatlong mga patnubay na dinisenyo upang makatulong sa mga ordinaryong Australyano na maintindihan ang mga mahalagang bagay tungkol sa seguridad ng cyber. Pag-aralan kung paano kumilos upang maprotektahan ang sarili laban sa mga kadalasang banta sa cyber.

Mga Unang Hakbang

Mga Susunod na Hakbang

Mga Mas Mataas na Hakbang

Talaan ng mga Nilalaman

Panimula

Ano ang pansariling seguridad sa cyber?

Sa isang mundong mas lalong pinapaandar ng teknolohiya, tayo ay araw-araw gumagamit ng mga gadyet at mga account na nanganganib sa mga banta sa cyber:

- Maaaring kabilang sa mga gadyet mo ang mga computer, teleponong mobile, tablet at iba pang mga gadyet na konektado sa internet.
- Maaari ka ring gumagamit ng mga online account para sa email, pagbabangko, pamimili, social media, paglalaro at iba pa.

Ang pansariling seguridad sa cyber ang nagpapatuloy na mga hakbang na maaari mong gawin upang protektahan ang iyong mga account at mga gadyet mula sa mga banta sa cyber.

Paano makakatulong ang gabay na ito na protektahan ako mula sa mga banta sa cyber?

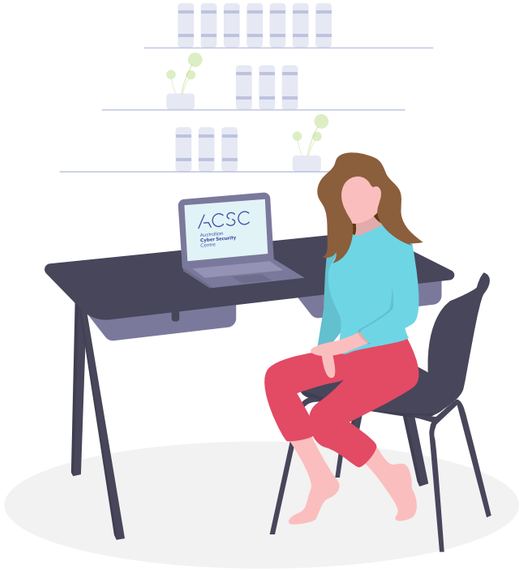
Kung ikaw ay nagsisimula pa lang na matuto tungkol sa seguridad sa cyber, o pinapanatiling napapanahon ang iyong sarili, ang gabay na ito ay isang napakagaling na pagsimulan. Ang Gabay sa Pansariling Seguridad sa Cyber: Mga Unang Hakbang ang una sa serye ng tatlong mga gabay na dinisenyo upang tulungan kang maunawaan ang mga pangunahing kaalaman sa\ seguridad sa cyber.

Ano ang mga banta sa cyber?

Ang pangunahing mga banta sa cyber na nakakaapekto sa mga pang-araw-araw na mga Australyano ay ang mga **scam at malware**.

- **Malware ang pangkalahatang pantawag na ginagamit upang ilarawan ang malicious software** na dinisenyo upang magdulot ng pinsala. Maaaring kabilang dito ang mga virus, worm, spyware, trojan at ransomware. Ginagamit ng mga cybercriminal ang malware upang nakawin ang iyong impormasyon at pera, at kontrolin ang iyong mga gadyet at mga account.
- **Ang mga scam ay mga mensaheng ipinadadala ng mga cybercriminal** na dinisenyo upang manipulahin ka na magbigay ng sensitibong impormasyon, o kaya ay mag-activate ng malware sa iyong gadyet.

Ang mga pag-atakeng ito ay maaaring may malubhang epektong personal o pinansyal sa mga biktima. Ang mga ito ay lumalago rin sa pagkasopistikado at pagkadalas.



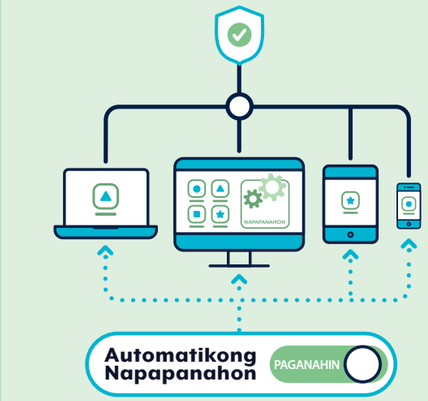
Pansariling Seguridad sa Cyber: Mga Unang Hakbang

Paganahin ang mga automatic update

Ano ang mga update?

Ang update ay isang pinabuting bersyon ng software (mga program, apps at mga operating system) na iyong na-install sa iyong computer at mga mobile na gadyet.

- **Ang mga software update ay tumutulong na maprotektahan ang iyong mga gadyet** sa pamamagitan ng pagkukumpuni sa mga software ‘bugs’ (mga pagkakamali sa coding o mga kahinaan). Ang mga cybercriminal at malware ay maaaring gumamit ng mga ‘bugs’ na ito upang ma-access ang iyong gadyet at nakawin ang iyong personal na datos, mga account,pampinansyal na impormasyon at pagkakakilanlan.
- **Ang mga bagong software ‘bugs’ ay patuloy na nahahanap** at pinagsasamantalahan ng mga cybercriminal. Ang pag-update ng software sa iyong mga gadyet ay nakakatulong na maprotektahan ka mula sa mga pag-atakeng cyber.



Paano ako mag-set up ng mga awtomatikong update?

Ang mga awtomatikong pag-update ay isang nakatakda o ‘i-set at kalimutan na’ na setting na nag-i-install ng mga bagong update sa sandaling ang mga ito ay makukuha na.

- **Paganahin at kumpirmahin ang mga automatic update sa lahat ng mga software at mga gadyet.**
- **Kung paano paganahin ang mga automatic update ay maaaring magkakaiba depende sa software at sa gadyet.**
- **Magtakda ng isang nababagay na oras para sa awtomatikong pag-update kung posible, tulad halimbawa, kung ikaw ay natutulog o hindi karaniwang ginagamit ang iyong gadyet.**

Dapat naka-on ang iyong gadyet, nakasaksak sa kuryente at may hindi pa gamit na storage space.

Paalala: Kapag nakatanggap ka ng isang prompt na i-update ang software ng iyong gadyet, dapat mong gawin ito sa lalong madaling panahon.

Ang karagdagang detalyadong impormasyon kung paano paandarin ang awtomatikong pag-update ay makikita sa pamamagitan ng paghanap ng ‘Updates’ sa cyber.gov.au

Paano kung walang setting ng awtomatikong update?

Kung ang setting ng awtomatikong pag-update ay hindi naroon, dapat mong palaging tingnan at mag-install ng bagong mga update sa pamamagitan ng iyong software o sa settings menu ng iyong gadyet.

Paano kung ang aking mas lumang gadyet at software ay hindi nakakatanggap ng anumang mga update?

Kung ang iyong gadyet, operating system o software ay napakaluma na, maaaring hindi na ito sinusuportahan ng tagagawa o developer.

Kung ang mga produkto ay makarating sa 'end of support' (pagtatapos ng suporta) na yugtong ito, hindi na makakatanggap ang mga ito ng mga update. Maaari kang nanganganib sa mga pag-atakeng cyber dahil dito. Kabilang sa mga halimbawa ng mga produktong tapos na ang suporta ang Windows 7 operating system at ang iPhone 7.

Kapag ang iyong gadyet, operating system o software ay nakaabot na sa end of support, inirerekomenda ng ACSC na mag-upgrade sa lalong madaling panahon upang manatili ang seguridad.

Para sa karagdagang impormasyon, hanapin ang 'End of support' sa cyber.gov.au

Pansariling Seguridad sa Cyber: Mga Unang Hakbang

Paganahin ang multi-factor authentication (MFA)

Ano ang MFA?

Maaari mong gamitin ang multi-factor authentication (MFA) upang mapabuti ang seguridad ng iyong pinakamahalagang mga account. Ang MFA ay nagngangailangan sa iyo na magpakita ng isang kombinasyon ng dalawa o mahigit pang mga uri ng pagpapatunay bago ibigay ang access sa isang account.

- **Isang bagay na alam mo** (hal. PIN, password o passphrase)
- **Isang bagay na mayroon ka** (hal. smartcard, pisikal na token, authenticator app, SMS o email)
- **Ang bagay na pagkakakilanlan mo** (hal. fingerprint, facial recognition o iris scan)

Ginagawang mas mahirap ng MFA para sa mga cybercriminal na makakuha ng paunang pag-access sa iyong account. Nagdaragdag ito ng higit pang mga patong ng pagpapatunay, na nangangailangan ng karagdagang oras, pagsisikap at mga mapagkukunan upang makapasok.

Paano ko pagaganahin ang MFA upang protektahan ang aking pinakamahalagang mga account?

Magkakaiba ang mga hakbang para sa pag-activate ng MFA depende sa account, gadyet o software application. Dapat mong i-activate ang MFA ngayon, sa pagsisimula sa iyong mga mahahalagang account:

- Lahat ng mga pagbabangko sa online at mga account na pinansyal (hal. ang iyong bangko, PayPal)
- Lahat ng mga account ng email (hal. Gmail, Outlook, Hotmail, Yahoo!)

Kung mayroon kang maraming mga account ng email, bigyan ng priyoridad ang mga naka-link sa iyong pagbabangko sa online o ibang mga mahahalagang serbisyo.

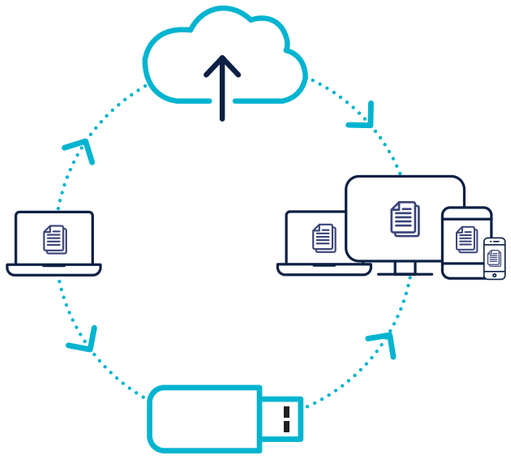
Maaari kang magbasa ng karagdagang impormasyon kung paano pagaganahin ang multi-factor authentication sa pamamagitan ng pag-search sa 'Multi-factorauthentication' o 'MFA' sa cyber.gov.au

Palaging naka-back up ang iyong mga gadyet

Ano ang back up?

Ang back up ay isang digital na kopya ng iyong impormasyon. Maaaring kabilang dito ang mga bagay na tulad ng mga larawan, impormasyong pinansiyal o mga rekord na na-save mo sa isang panlabas na storage device, o sa cloud.

Ang pag-back up ng iyong impormasyon ay isang hakbang sa pag-iingat upang maaari itong mabawi kung sakaling ito ay mawala, manakaw o masira.

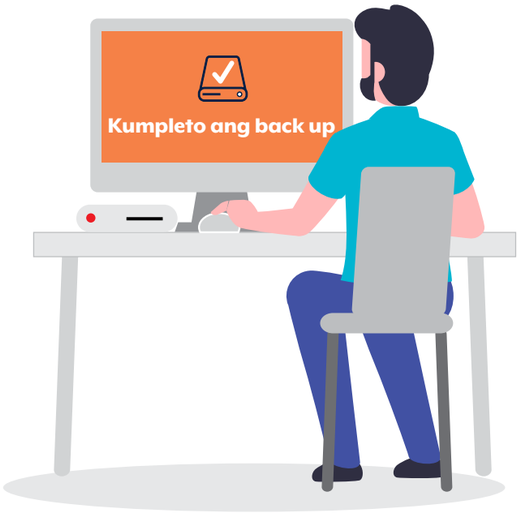


Paano ko iba-back up ang aking mga gadyet at files?

Dapat mong palaging i-back up ang iyong mga files at gadyet. Ang anyo niyan, kung ito ay araw-araw, lingguhan o buwanan ay nasa sa iyo. Kung ilang beses kang mag-back up ay maaaring depende sa bilang ng:

- mga bagong files na ilalagay mo sa iyong gadyet,
- mga pagbabagong gagawin mo sa mga files.

Paalala: Palaging tingnan ang iyong mga back up upang ikaw ay pamilyar sa proseso ng recovery (pagbabawi). Laging siguraduhin na gumaganang maayos ang iyong mga back up.



Ang karagdagang detalyadong impormasyon kung paano i-back up ang iyong impormasyon ay maaaring makita sa pamamagitan ng pag-search sa 'Back ups' sa cyber.gov.au

Pansariling Seguridad sa Cyber: Mga Unang Hakbang

Gumamit ng mga passphrase upang bigyan ng seguridad ang iyong mga mahalagang account

Ang multi-factor authentication (MFA) ay isa sa mga pinaka-epektibong paraan upang maprotektahan ang iyong mga account mula sa mga cybercriminal. **Kung walang magagamit na MFA**, ang isang natatanging malakas na passphrase ay mas mabuting magprotekta sa iyong account kumpara sa isang simpleng password.

Ano ang isang passphrase?

Ang isang passphrase ay gumagamit ng apat o higit pang random na salita bilang iyong password.

Halimbawa: 'crystal onion clay pretzel'.

- **Ang mga passphrase ay may mas may seguridad** kaysa sa mga simpleng password.
- Ang mga passphrase ay **mahirap para sa mga cybercriminal** na mahulaan, ngunit **madali para sa iyo na** matandaan.

Paano ako lumikha ng isang passphrase?

Lumikha ng mga passphrase na:

- **Mahaba:** hindi bababa sa 14 titik ang haba, na gamit ng apat o higit pang mga random na salita. Kung mas mahaba ang iyong passphrase, mas mataas ang seguridad nito.
- **Hindi mahuhulaan:** gumamit ng random na halo ng apat o higit pang walang kaugnayang mga salita. Walang tanyag na mga parirala, mga sipi o mga liriko.
- **Kakaiba:** hindi ginamit muli sa iba't-ibang mga account.

Kung ang isang website o sebisyo ay nangangailangan ng isang kumplikadong password kabilang ang mga simbolo, malalaking titik, o numero, maaari mong isama ang mga ito sa iyong passphrase. Ang iyong passphrase ay dapat pa ring mahaba, hindi mahuhulaan at kakaiba para sa pinakamahusay na seguridad.

Alin sa mga account ang dapat kong bigyan ng seguridad gamit ang isang passphrase?

Kung ang iyong pinakamahalagang mga account ay hindi pinuprotektahan ng MFA, palitan ang iyong mga password ng mga kakaibang malakas na mga passphrases, simula sa:

- Mga pagbabangko na nasa online at mga account na pinansiyal
- Mga account ng email

Kung mayroon kang maraming mga account ng email, bigyan ng priyoridad ang mga naka-link sa iyong pagbabangko sa online o ibang mga mahahalagang serbisyo.

Karaniwan mong mapapalitan ang iyong password ng isang kakaibang malakas na passphrase sa pamamagitan ng iyong account settings menu.

Tandaan: Kung nahihirapan kang matandaan ang lahat ng iyong mga passphrase, isaalang-alang ang paggamit ng password manager. Sa pamamagitan ng password manager, kailangan mo lang na tandaan ang isang password, ang password manager na bahala na sa iba. I-search ang 'password manager' sa cyber.gov.au para sa karagdagang payo.

Ang karagdagang detalyadong impomasyon kung paano lilikha ng may seguridad na mga passphrase ay maaaring mahanap sa pamamagitan ng pag-search sa 'Passphrases' sa cyber.gov.au

Bigyan ng seguridad ang iyong mobile na gadyet

Sa kasalukuyan, ang mga smartphone at tablet ay ginagamit sa pang-araw-araw na buhay. Ginagamit natin ang mga ito upang kumonekta, bumili, magtrabaho, magbangko, manmanan ang kalakasan ng ating katawan at tapusin ang daan-daang gawain sa anumang oras, at mula sa anumang lokasyon.

Ano ang mangyayari kung ang aking mobile gadyet ay nakompromiso, nawala o ninakaw?

- Maaari itong gamitin ng mga cybercriminal upang nakawin ang iyong salapi o pagkakakilanlan. Ginagawa nila ito sa pamamagitan ng paggamit sa iyong impormasyon na nakalagay sa iyong gadyet, kabilang ang social media at mga account ng email.
- Maaari kang mawalan ng hindi mapapalitang datos tulad ng mga larawan, mga sulat o mensahe (kung hindi ito na-back up).
- Maaaring gamitin ng isang cybercriminal ang iyong numero ng telepono upang lokohin ang ibang tao.

Paano ko bibigyan ng seguridad ang aking mobile na gadyet?

Seguridad ng gadyet:

- **Sarhan** (lock) ang iyong gadyet gamit ang isang passphrase, password, PIN o passcode. Gawin itong mahirap hulaan – ang iyong petsa ng kapanganakan at mga pattern lock ay madaling hulaan ng mga cybercriminals. Gumamit ng isang passphrase para sa pinakamainam na seguridad (tingnan ang pahina 6). Maaari mo ring isaalang-alang ang paggamit ng facial recognition o isang fingerprint upang i-unlock ang iyong gadyet.
- **Tiyakin** na ang iyong gadyet ay nakatakda na awtomatikong mag-lock pagkaraan ng ilang sandali ng kawalan ng aktibidad.
- **Huwag** isaksak ang iyong gadyet sa isang pampublikong charging station at iwasan ang mga charger mula sa mga pangatlong partido.
- **Tratuhin** ang iyong telepono gaya ng iyong pitaka. Panatilihing nasa iyo ito sa lahat ng oras.

Software at seguridad ng app:

- **Gamitin** ang automatic update feature ng iyong gadyet para mag-install ng bagong programa at mga pag-update ng operating system sa saglit na ang mga ito ay makukuha na.
- **I-set** ang gadyet upang mangailangan ng isang passphrase/password bago ma-install ang mga application. Ang mga kontrol para sa mga magulang ay maaari ring magamit para sa layuning ito.
- **Suriing** mabuti ang mga pahintulot sa pagkapribado (privacy permission) kapag nag-install ng bagong mga app sa iyong gadyet, lalo na ang para sa mga libreng app. Mag-install lamang ng mga app na galing sa mga mapagkakatiwalaang nagtitinda.

Seguridad ng datos:

- **Paganahin** ang remote locking and wiping functions, kung ang mga ito ay suportado ng iyong gadyet.
- **Siguraduhin** na lubusan mong alisin ang iyong personal na datos mula sa iyong gadyet bago mo ibenta o itapon ito.

Seguridad ng pagkakakonekta:

- **Isara** ang Bluetooth at Wi-Fi kapag hindi mo ginagamit ang mga ito.
- **Siguraduhin** na ang iyong gadyet ay hindi awtomatikong komukonekta sa mga bagong Wi-Fi network.

Karagdagang detalyadong impormasyon kung paano gawing may seguridad ang iyong mobile ay maaaring makita sa pamamagitan ng paghahanap ng 'Secure your mobile phone' sa cyber.gov.au

Paunlarin ang iyong pag-iisip sa seguridad ng cyber

Ang pansariling seguridad sa cyber ay hindi lamang tungkol sa pagbabago ng settings, tungkol din ito sa pagbabago ng iyong pag-iisip at kilos.

Mag-ingat sa mga cyber scam

Ang mga cybercriminal ay kilala na gumagamit ng email, messages, social media o mga tawag sa telepono upang subukang lokohin ang mga Australyano. Maaari silang magpanggap na isang indibidwal o organisasyon na sa tingin mo ay kilala mo, o sa tingin mo ay mapagtitiwalaan mo.

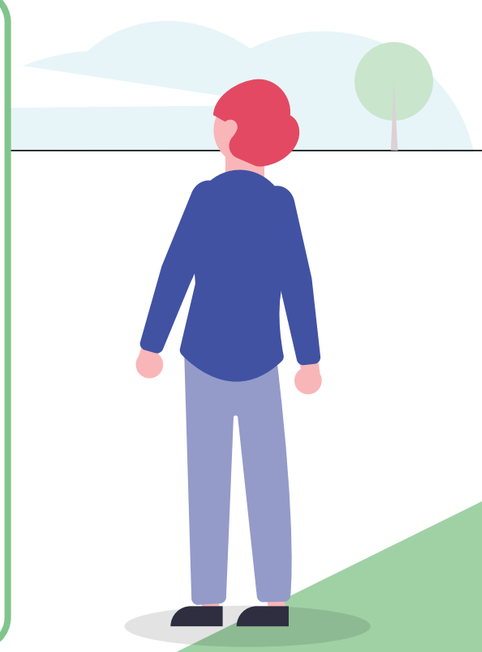
Ang kanilang mga mensahe at mga tawag ay magtatangka na linlangin kang magsagawa ng partikular na mga aksyon, tulad ng:

- Pagsisiwalat ng mga detalye ng bank account, mga password, at numero ng credit card,
- Pagbibigay ng remote access sa iyong computer,
- Pagbubukas ng isang attachment, na maaaring may laman na malware,
- Pagpapadala ng salapi o mga gift card.

Paano ko makikilala ang mga scam message?

Maaaring mahirap na kilalanin ang mga scam message. Ang mga cybercriminal ay madalas na gumagamit ng mga partikular na paraan upang linlangin ka. Ang kanilang mga mensahe ay maaaring kabilang ang:

- **Awtoridad:** ang mensahe ba ay nagpapanggap na mula sa taong opisyal, tulad ng iyong banko?
- **Pagmamadali:** sinabi ba sa iyo na mayroong problema, o na limitado ang iyong oras na magresponde o magbayad?
- **Emosyon:** ang mensahe ba ay ginagawa kang natataranta, umaasa o nagtataka?
- **Kakulangan:** ang mensahe ba ay nag-aalok ng isang bagay na nakakapos, o nangangako ng isang magandang presyo?
- **Kasalukuyang mga pangyayari:** ang mensahe ba ay tungkol sa isang kasalukuyang balita o malaking kaganapan?



Alamin kung paano makilala ang mga phishing o scam message sa pamamagitan ng pagbisita sa 'Learn the basics' sa cyber.gov.au

Ano ang dapat kong gawin kapag nakatanggap ako ng isang scam message?

Kung nakatanggap ka ng isang mensaheng scam o tawag sa telepono, dapat mong huwag pansinin, tanggalin o iulat ito sa Scamwatch ng ACCC sa scamwatch.gov.au

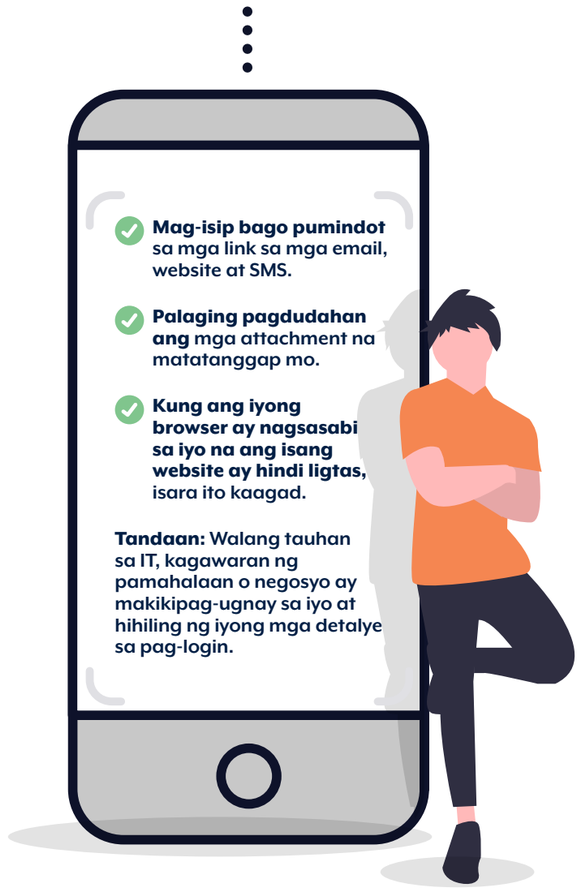
Maaari ka ring makipag-ugnay sa Cyber Security Hotline ng ACSC sa **1300 CYBER1** (1300 292 371) kung nababahala ka tungkol sa iyong seguridad sa cyber.

Kapag nakisali ka na sa isang scam at sa tingin mo ay maaaring nanganganib ang iyong mga bank account, credit o debit card, makipag-ugnayan kaagad sa iyong institusyong pinansyal. Baka kaya nilang isara ang iyong account o ihinto ang isang transaksyon.

Paano kung hindi ako sigurado kung scam ang isang mensahe?

Kung sa tingin mo ay ang mensahe o tawag ay talagang nagmumula sa isang organisasyon na pinagkakatiwalaan mo (tulad ng iyong bangko), maghanap ng isang paraan ng pakikipag-ugnay na puwede mong pagkatiwalaan. Hanapin ang opisyal na website, tawagan ang kanilang naka-anunsiyong numero ng telepono, o bisitahin ang isang pisikal na tindahan o sangay. Huwag gamitin ang mga link o detalye ng pakikipag-ugnay sa mensahe na ipinadala sa iyo o ibinigay sa telepono dahil ang mga ito ay maaaring nanlilinlang.

Tandaan:
Mag-isip Bago Pumindot



Kung sa tingin mo ay isa kang biktima ng cybercrime, iulat ito sa pamamagitan ng ReportCyber ng ACSC sa cyber.gov.au/report o tumawag sa aming Cyber Security Hotline sa 1300 CYBER1 (1300 292 371).

Maaari ka ring panatilihing napapanahon sa mga pinakabagong banta sa pamamagitan ng pag-subscribe sa libreng serbisyo ng alerto ng ACSC. Mag-search sa 'Subscribe to the ACSC alert service' sa cyber.gov.au
Padadalhan ka namin ng alerto kapay may matukoy kaming bagong banta sa cyber.

Pansariling Seguridad sa Cyber: Mga Unang Hakbang

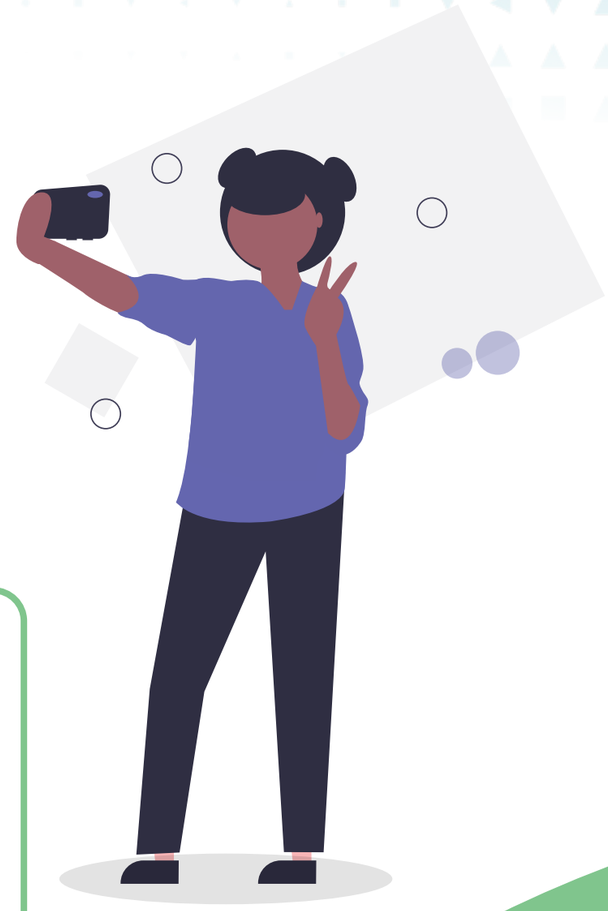
Huminto at mag-isip bago ka mag-share sa social media

Maaaring gamitin ng mga cybercriminal ang impormasyon na pinost mo para sa publiko sa iyong (mga) social media account sa kanilang mga scam at mga pag-atakeng cyber.

Tandaan na ang impormasyon sa internet ay permanente ay hindi mo maaaring lubos na maaalis ang ipinost.

Paano ako hihinto at mag-iisip bago mag-post?

- **Mag-isip:** Paano gagamitin ng isang cybercriminal itong impormasyon upang puntiryahin ako o ang aking mga account?
- **Mag-isip:** Komportable ba akong ipakita itong impormasyon o larawan sa isang estranghero sa online?



Anong impormasyon ang dapat kong iwasang ibahagi?

Iwasan ang pagbabahagi ng impormasyon (kabilang ang mga larawan) sa online na maaaring gamitin ng mga cybercriminal upang makilala ka, manipulahin ka sa pamamagitan ng isang scam o hulaan ang iyong mga tanong sa account recovery. Maaaring kasama dito ang iyong:

- Lugar ng kapanganakan at petsa ng kapanganakan.
- Address at numero ng telepono.
- Employer at kasaysayan ng trabaho.
- Kung saan ka nag-aral.
- Anumang ibang mga personal na impormasyon na maaaring magamit upang i-target ka.

Kabuuan ng Listahan

Nakumpleto mo na ba ang lahat sa gabay na ito?

Gamiting itong madaling-gamitin na listahan ng buod upang manmanan ang iyong pagsulong:

- **Pinagana ko ang awtomatikong pag-update para sa lahat ng aking mga gadyet:**
  - Computer (desktop at laptop).
  - Teleponong mobile.
  - Tablet.
- **Pinaandar ko ang multi-factor authentication sa aking mga pinakamahalagang account:**
  - Lahat ng aking pagbabangko sa online at mga account na pinansiyal (hal. iyong bangko, PayPal).
  - Lahat ng aking mga account ng email (hal. Gmail, Outlook, Hotmail, Yahoo!).
- **Palagi akong nagba-back up ng aking mga gadyet:**
  - Computer (desktop at laptop).
  - Teleponong mobile.
  - Tablet.
- **Gumagamit ako ng mga kakaibang malakas na passphrase sa karamihan ng aking mga pinakamahalagang account na hindi protektado ng MFA:**
  - Pagbabangko sa online at nga account na pinansiyal.
  - Mga account ng email.
- **Nilagyan ng seguridad ang aking mga mobile na gadyet:**
  - Laptop.
  - Teleponong mobile.
  - Tablet.
- **Ginagamit ko ang pag-iisip sa seguridad ng cyber araw-araw:**
  - Nakikilala ko ang mga mensaheng scam.
  - Alam ko kung ano ang gagawin kung makatanggap ako ng isang mensaheng scam.
  - Alam kong suriin kung ang isang mensahe ay isang scam kung hindi ako sigurado.
  - Nag-iisip ako bago ko i-click ang mga link at mga attachement.
  - Nag-iisip ako bago ko ibahagi ang anuman sa social media.
- **Alam ko kung saan makakakuha ng tulong kung ako ay isang biktima ng cybercrime o isang scam.**

Talasalitaan

App
Kinikilala rin bilang isang mobile application, ang app ay isang tawag para sa software na karaniwang ginagamit para sa isang smartphone o tablet.

Authenticator app
Isang app na ginagamit upang kumpirmahin ang pagkakakilanlan ng isang gumagamit ng computer upang payagan ang pag-access sa pamamagitan ng multi-factor authentication (MFA).

Cloud
Isang istraktura ng mga magkakalayong server na nagbibigay ng napakalaki, pinaghahati-hating imbakan ng datos at lakas na magproseso.

Cybercriminal
Sinumang indibidwal na labag sa batas na nag-a-access ng isang computer system o account upang sirain o magnakaw ng impormasyon.

Device (Gadyet)
Isang gadyet sa computing o komunikasyon. Halimbawa, isang computer, laptop, teleponong mobile o tablet.

Kalakip (Attachment)
Isang file na ipinapadala kasama ng isang mensaheng email.

Malware
Malicious software na ginagamit upang makakuha ng hindi awtorisadong pag-access at pagkontrol sa kompyuter ng isang gumagamit, magnakaw ng impormasyon at guluhin o salantain ang mga network.

Operating system
Ang software na naka-install sa hard drive ng isang computer na nagpapagana sa hardware ng computer na makipag-ugnay at magpatakbo sa mga programa ng computer. Mga halimbawa: Microsoft Windows, Apple macOS, iOS, Android.

Paghinto ng suporta (End of support)
Ang end of support (pagtatapos ng suporta) ay tumutukoy sa isang sitwasyon kung saan ang isang kompanya ay maghihinto ng pagsuporta para sa isang produkto o serbisyo. Ito ay karaniwang nalalapat sa mga produktong hardware at software kapag ang kompanya ay maglalabas ng isang bagong bersyon at ihihinto ang suporta para sa nakaraang mga bersyon.

Pagpapanumbalik ng Account (recovery)
Isang proseso kung saan isang pangkat ng mga tanong o iba pang mga paraan ng pagpapatunay ay gagamitin upang panumbalikin o mabawi ang pag-access sa isang account o upang baguhin ang isang account passphrase/password.

Physical token
Isang pisikal na gadyet na karaniwang kumakasya sa isang keyring, na lumilikha ng isang security code na ginagamit parakumpirmahin ang pagkakakilanlan ng gumagamit ng computer gamit ang MFA.

Remote access
Pagkuha ng pag-access at pagkontrol sa mga gadyet at mga imprastraktura mula sa isang malayong lokasyon.

Software
Karaniwang kinikilala na mga programa, koleksyon ng mga instruksiyon na nagbibigay-daan sa gumagamit na makipag-ugnayan sa computer, ang hardware nito o magsagawa ng mga gawain.

Pagtatatwa

Ang materyal sa gabay na ito ay may pangkalahatang katangian at hindi dapat itinuturing bilang legal na payo o aasahan para sa tulong sa anumang partikular na pangyayari o pang-emerhensyang sitwasyon. Sa anumang mahalagang bagay, dapat kang humingi ng nararapat na independiyenteng propesyonal na payo na kaugnay sa iyong sariling mga kalagayan.

Ang Komonwelt ay hindi tumatanggap ng responsibilidad o pananagutan para sa anumang pinsala, pagkawala o gastos na natamo bilang resulta sa pagsalalay sa impormasyon na nakalagay sa gabay na ito.

Para sa karagdagang impormasyon, o upang mag-ulat ng isang insidente ng seguridad sa cyber, makipag-ugnayan sa amin:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Itong numero ay magagamit lamang sa loob ng Australya.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre