Australian Government

Kumilos Ngayon.
Manatiling Ligtas.

Paano ka manatiling ligtas sa online

Madaling Basahin na Bersyon

Easy Read

Paano ang paggamit nitong gabay

Tayo ang Pamahalaang Australya.

Tayo ang nagsulat nitong gabay.

Isinulat namin ang ilang mga salita na naka-**bold**.

Ipaliwanag namin kung ano ang kahulugan ng mga salitang ito.

May listahan din ng mga salitang ito sa pahina 28.

Maaari kang humiling ng isang tao na pinagkakatiwalaan mo para sa suporta na:

- basahin itong gabay
- humanap ng dagdag na impormasyon.

Ito ay isang buod ng Madaling Basahin na ibang gabay.

Isinasama lang dito ang mga pinakamahalagang ideya.

Matatagpuan mo yong isa pang gabay sa aming website.

www.actnowstaysecure.gov.au

Ano ang napapaloob sa gabay na ito?

Tungkol sa gabay na ito 4

Ipanatiling ligtas ang iyong mga account 6

I-tsek ang iyong settings upang maproteksyunan ang iyong impormasyon 10

Proteksyunan ang iyong mga device 16

Mga Panlilinlang 20

Magsalita ka 25

Listahan ng salita 28

Tawagan kami 30

Tungkol sa gabay na ito

Lahat tayo ay kailangang mag-isip tungkol sa kung paano tayo manatiling ligtas sa online.

Tawag natin dito ay ligtas sa **cyber**.

Ang Cyber ay nangangahulugang may kinalaman sa internet.

Itong gabay ay nagpapaliwanag ng mga ilang bagay na magagawa mo upang maprotektahan ang iyong sarili sa online.

Halimbawa, laban sa **cyber crime**.

Ang Cyber crime ay kapag ginamit ng mga kriminal ang internet para sa krimen.

Halimbawa, gagamitin nila ang internet para:

- nakawin ang iyong personal na impormasyon
- kamkamin ang iyong mga account o profile sa online.

Ang Cyber crime ay nangyayari sa kahit anumang elektronikong gamit (device).

Kabilang dito ang iyong:

- computer
- smartphone
- smart watch.

May mga bagay na magagawa mo upang manatiling ligtas laban sa cyber crime.

Pinapaliwanag namin sa kasunod na mga pahina kung ano ang magagawa mo.

Ipanatiling ligtas ang iyong mga account

Dapat kang mag-isip tungkol sa kung paano mo mapapanatiling ligtas ang iyong mga account sa online.

Gumamit ng malakas at iba't-ibang mga passphrase

Ang **passphrase** (binuong mga salita at numero) ay mas malakas na klase ng password.

Mahirap itong mahulaan ng ibang tao.

Ang paggamit ng malakas at iba't-ibang mga passphrase ay isa sa mga pinakamabisang paraan para protektahan ang iyong mga account.

Dapat kang gumamit ng magkakaibang mga passphrase sa bawa't isang account sa online.

Kabilang sa malakas na mga passphrase ay:

- 4 o mahigit pa na mga salitang pasumala
- 15 o mahigit pa na mga letra at numero.

Maaari mong isama ang ilang mga letrang malalaking titik.

Maaari mo ding gamitin ang mga simbolo kagaya ng:

- isang gitling (dash)
- senyal ng dolyar (dollar sign)
- isang email @ na sign.

Hindi ka dapat gumagamit ng anumang personal na impormasyon sa iyong mga passphrase.

Halimbawa:

- iyong birthday
- mga pangalan ng kapamilya o mga alagang hayop.

Magdagdag ng mga hakbang sa paglog-in sa iyong mga account

Mapoproteksyunan mo ang iyong mga account sa online sa pamamagitan ng **multi factor authentication (MFA)**.

Ang MFA ay kapag gumamit ka ng 2 o mahigit pa na mga paraan sa paglog-in sa iyong account sa tuwina.

Halimbawa, kailangan mong i-entra muna ang iyong passphrase.

Pagkatapos ay i-entra naman ang code na natanggap mo sa iyong cellphone.

Maaaring may pagpipilian ka na:

- kunin ang isang app sa iyong cellphone para magbigay ng code

- kunin ang code sa email

- kunin ang code sa isang text message.

Sa MFA ay mas mahihirapan ang ibang tao na makapasok sa iyong mga account sa online.

Kahit na natuklasan nila ang iyong passphrase.

I-tsek ang iyong settings upang maproteksyunan ang iyong impormasyon

Matse-tsek mo na pinoprotektahan ng iyong settings ang iyong impormasyon sa online.

Kabilang nito ang iyong mga setting sa:

- mga online account
- mga elektronikong device
- mga apps.

Maaari mong:

- baguhin ang iyong mga setting
- piliin kung anong apps ang pwedeng gumamit ng iyong impormasyon.

Makikita mo ang settings sa iyong device sa pamamagitan ng:

- tingnan ang ‘gear’ na icon

  o kaya

- i-type ang ‘settings’ sa search bar ng iyong device.

Maaaring makita mo ang settings ng isang app o account sa online sa pagbubukas ng menu.

Ang hitsura ng menu ay parang 3 mga paderetsong guhit.

Ang ilan sa mga settings na ito ay maaaring magbahagi ng impormasyon tungkol sa:

- kung sino ka
- kung nasaan ka
- kung saan ka nakatira

Ang pagbabahagi nitong impormasyon sa online ay maaaring maglagay sa iyo sa panganib ng mga cyber crime.

Ang mga kriminal sa Cyber ay maaaring gamitin ang iyong impormasyon sa pagpapanggap bilang ikaw.

Halimbawa, maaaring gumamit sila ng impormasyon tulad ng:

- kung saan ka nakatira

- ang mga pangalan ng iyong kapamilya

- mga pangalan ng iyong alagang hayop.

Maaari mong i-set ang iyong mga account na ang mga taong kilala mo lamang ang makakakita ng iyong mga profile sa social media.

Halimbawa, ang profile mo sa Facebook.

Itong mga settings ay kalimitang tinatawag na privacy settings.

Mako-kontrol mo rin ang iyong **location settings**.

Ipinapakita ng location settings kung saan nararoooon ang iyong device.

Maaari mong ilagay ang location settings sa ‘on’ o sa ‘off’.

Maaari mo ring piliin kung alin sa mga apps ang pwedeng gumamit ng iyong location settings.

Magagawa mo ito para sa iyong:

- online na mga account
- mga device
- mga apps.

Ang ilan sa mga apps ay maaaring magtanong sa iyo kung pwede sila na:

- gamitin ang iyong kamera

- tingnan ang iyong mga larawan.

Pumayag ka lamang sa mga apps na pamilyar ka na gamitin ang iyong kamera at mga larawan.

Proteksyunan ang iyong mga device

Dapat kang mag-isip tungkol sa kung paano mo poproteksyunan ang iyong mga device upang mapanatiling ligtas ka sa online.

Halimbawa, ang iyong cellphone o smart watch.

Ito ay mahalaga para sa mga device na kumukonekta sa internet.

I-update ang iyong mga device

Maaari mong i-update ang iyong mga device para mapanatiling ligtas sila sa online.

Halimbawa, ang iyong cellphone at laptop.

Maaaring tawagin ito ng iyong device na software update.

Ang mga update ay tumutulong sa device na protektahan ang sarili nito laban sa krimeng cyber.

Maaari mong i-set ang device na mag-update ng kanyang sarili.

Maaaring dagdagan ang iyong kaalaman tungkol sa pag-update ng iyong mga device sa aming website.

www.actnowstaysecure.gov.au/cyber-safe-actions

Mga Pampublikong Wi-Fi na network

Kailangang maging maingat ka kung gumagamit ng **pampublikong Wi-Fi**.

Ang pampublikong Wi-Fi ay libreng gamit ng internet na hindi kailangan ang kable sa mga pampublikong lugar.

Halimbawa, sa isang:

- cafe
- paliparan
- hotel.

Kailangan maingat ka tungkol sa kung anong impormasyon ang iyong ikinakarga sa website gamit ang pampublikong Wi-Fi.

Halimbawa, ang iyong:

- mga detalye ng bangko
- mga account sa email
- mga profile sa social media.

Ang ilang mga kriminal ng cyber ay nakakagamit ng pampublikong Wi-Fi para:

- makita kung ano ang ginagawa mo sa online
- nakawin ang iyong impormasyon.

Ito ay dahil sa:

- kahit sino ay makakagamit

- mas mahirap proteksyunan ang iyong mga device.

Malalaman mo sa aming website kung paano manatiling ligtas sa paggamitt ng pampublikong Wi-Fi.

www.actnowstaysecure.gov.au/cyber-safe-actions

Mga Panlilinlang

Ang tawag natin ay isang **scam (panlilinlang)** kapag sinubukan ng isang tao na:

- lokohin ka
- kunin ang iyong pera.

Ang **manlilinlang (scammer)** ay isang tao na gumagawa ng mga panlilinlang.

Ang mga scammer ay maaaring lokohin ka sa pamamagitan ng:

- isang text na mensahe o tawag sa telepono
- isang email
- social media
- isang website.

Mukha silang mapagkaibigan.

Ngunit maaari kang lokohin na magbigay sa kanila ng iyong impormasyon.

Magagamit nila ang mga iyon para:

- makapasok sa iyong mga account sa online

- magpanggap bilang ikaw

- nakawin ang iyong pera.

Maaari ding gawin ng mga scammer na:

- maglikha ng mga pekeng account para lokohin ka

- magbahagi ng mga ugnay at paanunsyo para i-klik mo.

Paano mo matutunugan ang isang scam

Maaaring scam iyan kung ito ay:

- magsasabi sa iyong madaliang gawin ang isang bagay

- mag-aalok sa iyo ng maraming pera

- humihingi sa iyo ng pera

- sabihin sa iyo na i-klik mo ang isang link (ugnay).

Ang mga scammer ay maaari ding magpanggap na isang organisasyon na kilala mo at pinagkakatiwalaan.

Halimbawa, ang iyong bangko.

Ginagawa ito ng mga scammer para ibahagi mo ang iyong personal na impormasyon sa kanila.

Dapat tumigil ka sa pakikipag-usap sa tao kung palagay mo ay isang scammer ito.

Dapat mong i-tsek kung ang tao nga ay siya talaga ayon sa sabi niya.

Maaari mong tawagan ang tao o organisasyon na gagamitin ang mga detalyeng pinagtitiwalaan mo at ikaw mismo ang nakadiskubre.

Kumilos kaagad para protektahan ang iyong sarili kung may naramdaman kang tila hindi tama.

Pagsusumbong ng isang scam

Ang Scamwatch ay tumutulong sa mga Australyano na:

- maintindihan ang mga scam
- isumbong ang mga scam.

Ang Scamwatch ay tumutulong din sa mga Australyano na nakaranas ng mga scam.

Makakapagsumbong ka ng scam sa website ng Scamwatch.

www.scamwatch.gov.au/report-a-scam

Magsalita ka

Dapat kang magsalita tungkol sa kung paano mapoproteksyunan ng ibang tao ang kanilang mga sarili sa online.

Kabilang dito ang:

- pagsusumbong ng krimen na cyber

- pagbabahagi ng nalalaman mo sa pamilya at mga kaibigan.

Ipapaliwanag namin sa susunod na mga pahina kung paano ka magsasalita.

Isumbong ang krimen na cyber

Ang pagsusumbong ng cyber crime ay nakakatulong sa pamahalaan:

- alamin kung paano ginagawa ng mga kriminal sa cyber ang pang-aatake sa tao

- protektahan ang mas maraming tao.

Makapagsusumbong ka ng cyber crime sa website na ReportCyber.

www.cyber.gov.au/report

Pag-usapan sa pamilya at mga kaibigan ang tungkol sa kung paano ang pagpapanatiling ligtas sa online

Dapat mong ibahagi sa iyong pamilya at mga kaibigan ang iyong mga tip tungkol sa pagpanatiling ligtas sa online.

May matututunan ka rin sa kanila.

Mapoprotektahan mo ang iyong sarili at mga taong nasa paligid mo sa pagbabahagi ng iyong nalalaman tungkol sa pagpapanatiling ligtas sa online.

Ito ay mahalaga rin kapag nakikigamit ka ng mga device sa ibang tao.

Listahan ng salita

Ipinapaliwanag ng listahang ito kung ano ang kahulugan ng mga salitang naka-**bold** sa gabay na ito.

Cyber

Ibig sabihin ng Cyber ay may kinalaman tungkol sa internet.

Krimen na Cyber (Cyber crime)

Ang Cyber crime ay kapag ginamit ng mga kriminal ang internet sa krimen.

Halimbawa, maaaring gamitin nila ang internet para:

- nakawin ang iyong personal na impormasyon
- kamkamin ang iyong mga account sa online.

Mga setting ng lokasyon

Ipinapakita ng location settings kung nasaan ang iyong device.

Multi-factor na pagpapatunay (MFA)

Ang MFA ay kapag gumamit ka ng 2 o mahigit pa na kaibang paraan sa paglog-in sa iyong account sa tuwina.

Passphrase

Ang isang passphrase ay mas malakas na klase ng password.

Mahirap itong mahulaan ng ibang tao.

Pampublikong Wi-Fi

Ang pampublikong Wi-Fi ay isang libreng paggamit ng internet na walang gamit na kable sa mga pampublikong lugar.

Mga panloloko

Ang tawag namin ay isang panlilinlang (scam) kapag sinubukan ng isang tao na:

- lokohin ka
- kunin ang iyong pera.

Mga scammer

Ang manlilinlang (scammer) ay isang tao na gumagawa ng mga panlilinlang.

Tawagan kami

Maaari mong tawagan ang Australian Cyber Security Hotline.

1300 292 371

Makakabisita ka sa aming website.

www.actnowstaysecure.gov.au

Makapagsusumbong ka ng cyber crime sa website ng ReportCyber.

www.cyber.gov.au/report

Ang Information Access Group ang lumikha nitong Easy Read na dokumento na gamit ang dating-yari-ng-mga-larawan at video (stock photography) at pasadyang mga larawan (custom images). Ang mga larawan ay bawal gamitin nang walang pahintulot. Para sa anumang pagtatanong tungkol sa mga larawan, mangyaring bisitahin ang www.informationaccessgroup.com. I-quote ang job number 6342.