Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

PAANO GAMITIN ANG INTERNET NA MAY SEGURIDAD

ISANG GABAY PARA SA MGA NAKATATANDA

cyber.gov.au

Panimula

Ang pagpupunta sa online ay nagbibigay-daan sa iyo na makipag-ugnayan sa mga kaibigan at pamilya, matuto tungkol sa mga paksa at pati na rin ang maglaro ng mga games.

Tulad ng pagkabit ng iyong seatbelt bago magmaneho, dapat kang magsagawa ng mga hakbang bago gamitin ang internet upang maging mas ligtas.

Nais ng Australian Cyber Security Centre (ACSC) na masigurong lahat ay may seguridad kapag sila ay nasa online. Ang dokumentong ito ay sumasaklaw sa ilang mga simpleng kagawian sa seguridad sa cyber na maaari mong gamitin upang protektahan ang iyong sarili kapag nag-a-access ng internet.

Ang Australian Cyber Security Centre (ACSC), ay bahagi ng Australian Signals Directorate (ASD), na nagbibigay ng payo, tulong at mga tugon sa pagpapatakbo upang maiwasan, makita at mabigyan ng lunas ang mga panganib na cyber sa Australya. Nandito ang ACSC upang tumulong na gawing pinakamabuting lugar ang Australya na komunekta sa online.

Para sa karagdagang impormasyon ng seguridad sa cyber, mga gabay at payo, bisitahin ang cyber.gov.au

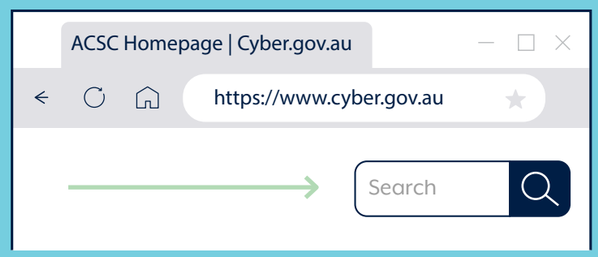
Seguridad sa cyber ng mga matatanda

Payo 1: I-update ang iyong gadyet

Ang pag-update sa iyong software ay katulad ng pagpapaserbis sa iyong sasakyan. Pinapabuti nito ang takbo ng iyong gadyet at ginagawa itong may mas mataas ang seguridad.

Ang mga cybercriminal ay palaging humahanap ng mga bagong paraan upang mag-hack sa mga gadyet. Ang pag-set up sa iyong gadyet na awtomatikong mag-install ng mga update ay maaring ayusin ang anumang mga kahinaan sa iyong software at panatilihing ligtas sa mga hacker.

Upang makahanap ng karagdagang impormasyon, i-search ang 'Updates' sa cyber.gov.au



ALAM MO BA:

Ang mga update ay maaari ring magdagdag ng mga bagong katangian (features) sa iyong gadyet at gawin itong mas mabilis ang pagtakbo.

Payo 2: I-on ang multi-factor authentication

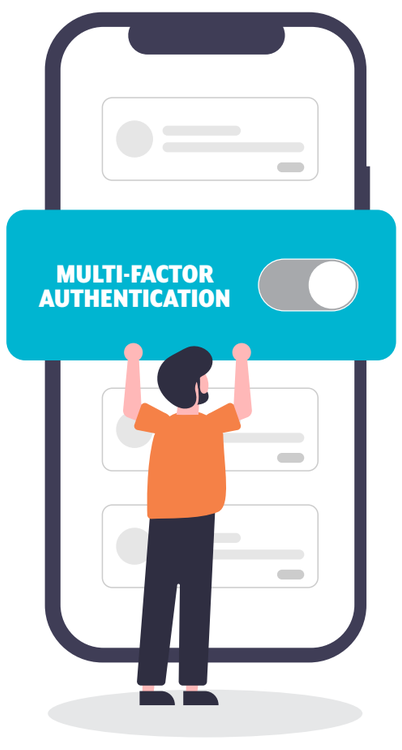
Ang multi-factor authentication sa iyong account ay katulad ng security screen sa iyong bahay.

Pinoprotektahan ka nito mula sa mga kriminal na sinusubukang makapasok.

Sa pag-activate sa multi-factor authentication, kailangan mong magbigay ng maramihang piraso ng impormasyon upang mabigyan ng pag-access sa iyong account. Halimbawa, maaaring kakailanganin mong i-enter ang iyong password at isang text message code upang mag-log in sa iyong social media profile.

Ang maramihang patong ay ginagawang mas mahirap para sa mga cybercriminal na mag-hack upang makapasok. Posibleng maaari nilang malutas ang isang bahagi, tulad ng iyong password, ngunit kailangan pa rin nilang makuha ang iba pang mga piraso ng puzzle upang ma-access ang iyong account.

Upang makahanap ng karagdagang impormasyon, i-search ang 'Multi-factor authentication' o 'MFA' sa cyber.gov.au



TANDAAN:

Kung kinakailangan mo ng tulong na i-on ang multi-factor authentication, humingi ng tulong mula sa isang kaibigan o miyembro ng pamilya.

Payo 3: I-back up ang iyong gadyet

Ang pagsasagawa ng isang 'backup' ay kung gumagawa ka ng isang kopya ng iyong mga mahalagang file at itinatabi ang mga ito sa isang lugar na may seguridad.

Kapag nai-back up mo ang iyong computer, telepono o tablet, ang mga kopya ng iyong mga file ay naka-save sa online o sa isang nakahiwalay na gadyet. Ang pagkakaroon ng backup ng iyong mga mahalagang file at mga pinahahalagahang larawan ay magbibigay sa iyo ng kapayapaan ng isip.

Kung may masamang mangyari sa iyong gadyet o ma-hack ka ng mga cybercriminal, madali mong ibalik ang iyong mga file mula sa iyong mga backup.

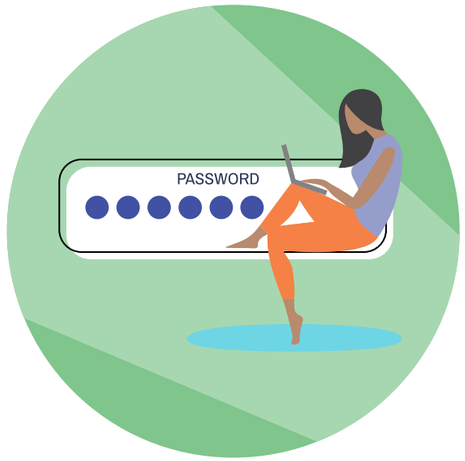
Upang makahanap ng karagdagang impormasyon, i-search ang 'Backups' sa cyber.gov.au

ALAM MO BA:

Ang regular na pag-back up ng iyong gadget ay nangangahulugan na palagi kang may access sa iyong pinakabagong mga file.

Payo 4: Gumamit ng passphrase

Kung ang password ay naglalagay ng isang kandado sa iyong account, ang passphrase ay nagbibigay ng sarili nitong security system! Ang mga ito ay mas malakas at mas mataas ang seguridad na bersyon ng mga password.



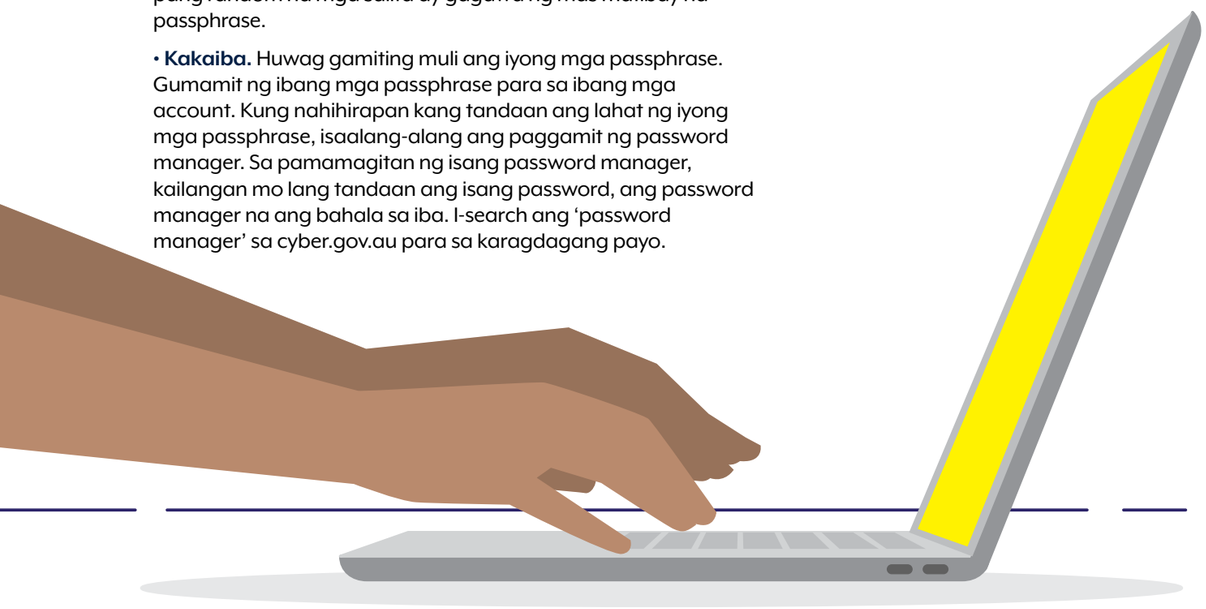
Kung hindi mo ma-on ang MFA, gumamit ng passphrase upang bigyan ng seguridad ang iyong account. Ang mga passphrase ay gumagamit ng apat o mahigit pang mga random na salita bilang iyong password. Ito ay ginagawang mahirap para sa mga cybercriminal na mahulaan ngunit madali para sa iyo na matandaan.

Kung gagawa ka ng passphrase, gawin itong:

• **Mahaba.** Kung mas mahaba, mas mabuti. Magsikap na gawing hindi bababa sa 14 letra ng haba. Ang apat o higit pang random na mga salita na matatandaan mo ay maganda. Halimbawa, 'kulay-lilang pato patatas bangka'.

• **Hindi mahuhulaan.** Kung hindi masyadong mahuhulaan ang iyong passphrase, mas mabuti. Ang mga pangungusap ay maaaring magandang mga passphrase, ngunit ang mga ito ay mas madaling hulaan. Ang kumbinasyon ng apat o higit pang random na mga salita ay gagawa ng mas matibay na passphrase.

• **Kakaiba.** Huwag gamiting muli ang iyong mga passphrase. Gumamit ng ibang mga passphrase para sa ibang mga account. Kung nahihirapan kang tandaan ang lahat ng iyong mga passphrase, isaalang-alang ang paggamit ng password manager. Sa pamamagitan ng isang password manager, kailangan mo lang tandaan ang isang password, ang password manager na ang bahala sa iba. I-search ang 'password manager' sa cyber.gov.au para sa karagdagang payo.



Dagdagan ang kaalaman tungkol sa paglikha ng mga may seguridad na passphrase sa pamamagitan ng pag-search ng 'Passphrases' sa cyber.gov.au

Payo 5: Kilalanin at isumbong ang mga scam

Kung mas mabilis mong isumbong ang scam, mas mabilis kaming kikilos.

Kung sa tingin mo ay may nagtatangkang gumamit ng internet upang lokohin ka, mas mabuting maging maagap at maingat kaysa sa magbakasakali at mapagsamantalahan.

Kung ang isang bagay ay sobrang napakabuti na hindi na kapani-paniwala, malamang na ito ay hindi tunay. Habang ang isang mensahe ay maaaring nagpapahayag na nanalo ka ng isang gantimpala o naglalaman ng isang virus ang iyong computer, ang mensaheng iyan ay hindi natatanging sa iyo lamang.

Maaaring nanggagaling ito sa isang scammer at nais ka nilang samantalahin.

Tandaan, ang mga scammer ay kadalasang nagpapanggap na isang tao o organisasyon na pinagkakatiwalaan mo. Maghinala kung nakatanggap ka ng isang mensahe na parang galing sa isang taong pinagkakatiwalaan mo, ngunit sila ay gumagamit ng bagong numero ng telepono, email address o social media profile. Bago ka sumagot, patunayan na ang tao o organisasyon na nakikipagmensahe sa iyo ay talagang sila nga sa pamamagitan ng pakikipag-ugnay sa kanila sa isang pamamaraan na maaasahan mo. Halimbawa, kung makatanggap ka ng isang text message na sa tingin mo ay parang galing sa isa sa mga anak mo, ngunit ito ay galing sa isang bagong numero, huwag mong sagutin. Padalhan mo muna siya ng mensahe sa social media upang masuri kung talagang pinalitan niya ang kaniyang numero ng telepono.

ALAM MO BA:

Ang mga cybercriminal ay manlilinlang at maaaring gumamit ng isang kilalang pangalan at email address.
Maging maingat kung:
• hinilingan kang magbayad kaagad sa isang bayarin.
• hinilingan kang palitan ang iyong mga detalye o password.
• hinilingan kang i-click ang isang link o buksan ang isang attachment.

Katapusan

Ngayong armado ka na ng kaalaman sa paggamit ng internet nang mas maingat, maaari kang mag-browse nang may pagtitiwala sa sarili at patuloy na ikatuwa ang iyong oras sa online.

Tandaan lamang, ang mga cybercriminal ay palaging lumilikha ng mga bagong paraan upang i-target ang mga tao.

Hindi kailanman nakakapinsala kung paminsan-minsang pagbutihin ang iyong kaalaman sa seguridad sa cyber at matuto ng mga bagong paraan upang manatiling may seguridad.

Bonus na mga payo

Nais mo bang matuto ng mga karagdagang paraan upang mapanatiling may seguridad sa online? Tingnan ang mga sumusunod na tip.

Pag-isipan kung ano ang ipo-post mo.

Isiping mabuti ang impormasyon na ibabahagi mo sa online at sino ang makakakita nito. Tanggapin lamang ang mga friend request na galing sa mga taong kilala mo sa totoong buhay.

Kumuha ng mga alerto ng mga bagong banta.

Magpalista sa aming libreng serbisyo ng alerto. Ipapaalam nito sa iyo kung may makikita kaming bagong banta sa cyber.

Bibigyan ka rin nito ng payo kung ano ang gagawin kung may mangyayaring pag-atake.

Pag-usapan ang tungkol sa seguridad sa cyber kasama ng iyong pamilya at mga kaibigan.

Ngayong tumaas na ang iyong kasanayan sa seguridad ng cyber, ibahagi ang iyong natutunan sa iyong pamilya at mga kaibigan.

Ang iyong kaalaman ay maaaring tumulong sa kanilang harapin ang isang mahirap na problema sa hinaharap!

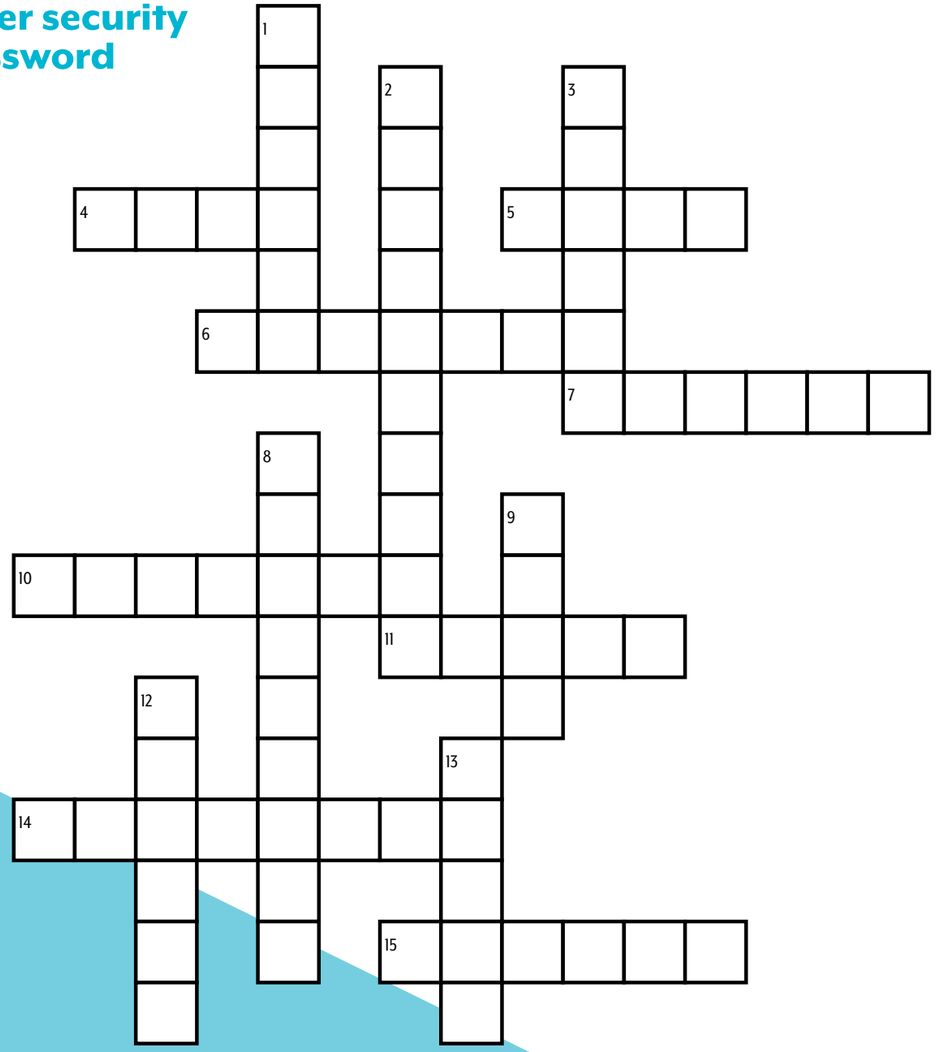
Iwasan ang pampublikong Wi-Fi kapag ikaw ay nagbabangko o bumibili sa online.

Ang pampublikong Wi-Fi ay maganda para sa panunuod ng mga video o pagbabasa ng mga website, ngunit gawin ang anumang aktibidad sa online na may kinalaman sa pera sa iyong koneksyon ng internet sa bahay. Ang pampublikong Wi-Fi ay maaaring mapanganib.

Isumbong ang mga cyber crime at mga insidente upang mapanatiling ligtas ang Australya.

Kung sa tingin mo ay naging biktima ka ng isang cybercrime, kumilos ng mabilis. May karagdagang payo sa cyber.gov.au

Cyber security crossword



PABABA

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

PATAGILID

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

Karagdagang mga gabay

Para sa karagdagang impormasyon, mangyaring tingnan ang aming Serye ng *Pansariling Seguridad sa Cyber*: tatlong mga gabay na dinisenyo upang tulungan ang mga pang-araw-araw na Australyano na maunawaan ang pangunahing kaalaman tungkol sa seguridad sa cyber at kung paano ka maaaring gumawa ng aksyon upang maprotektahan ang iyong sarili mula sa mga karaniwang banta sa cyber.

Maaari mong makuha ang lahat ng tatlong gabay sa **cyber.gov.au**

Mga Sagot sa Crossword:

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

Mga Paalala

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 kaugnay ng iyong sariling mga kalagayan.

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

Para sa karagdagang impormasyon, o upang magsumbong 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