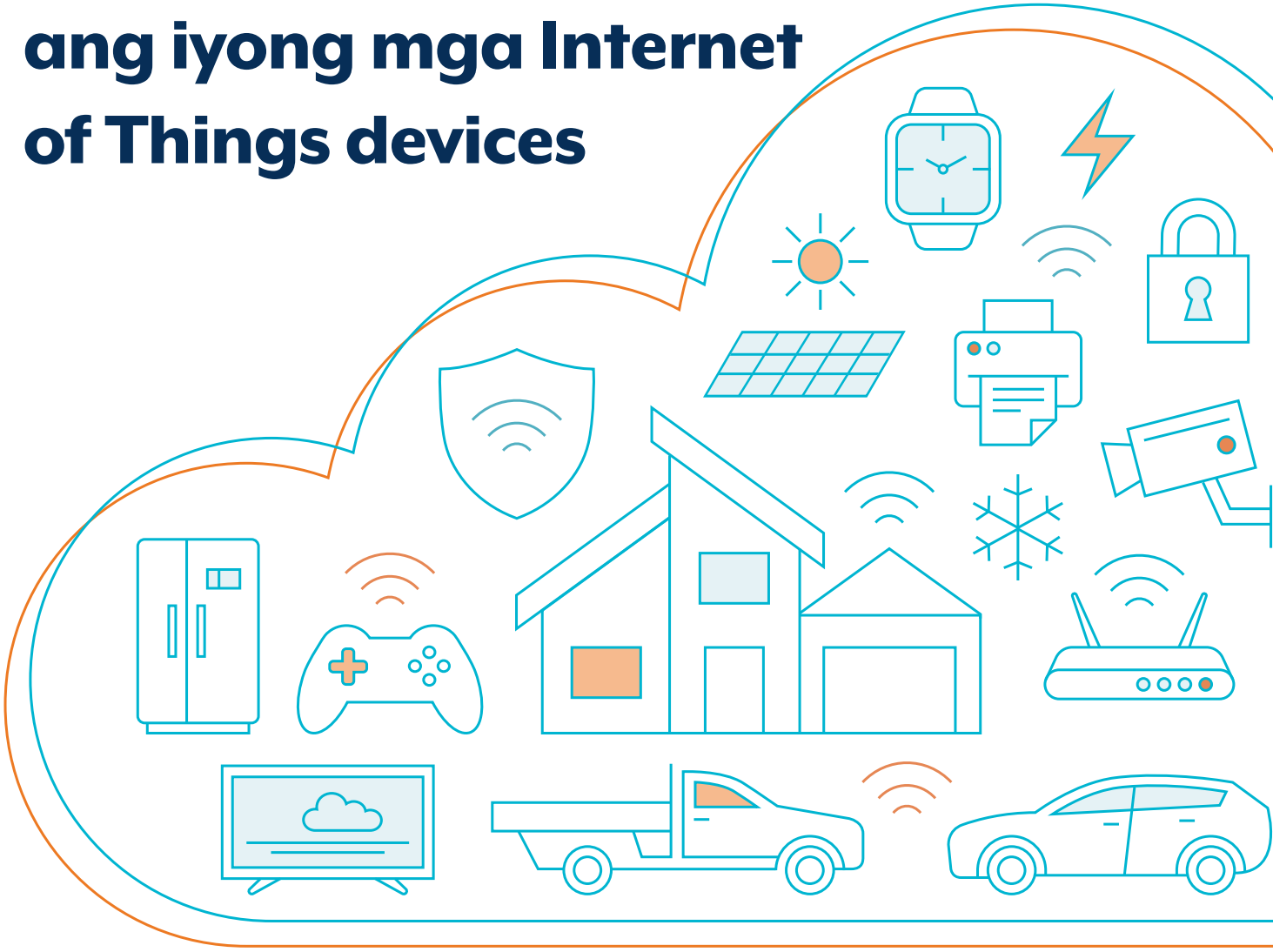
Mga tip para ma-secure ang iyong mga Internet of Things devices



Binuo ng Australian Cyber Security Center ang impormasyong ito upang matulungan ang komunidad na bumili at gumamit ng mga Internet of Things (IoT) device nang ligtas. Ang IoT device ay isang pang-araw-araw na item na may koneksyon sa internet na idinagdag dito. Kabilang sa mga halimbawa ng IoT device ang mga baby monitor, drone, security camera, smart television at solar inverter. Ang mga IoT device sa loob ng mga tahanan at negosyo ay karaniwang gumagamit ng Wi-Fi o mga cellular network, gaya ng 4G o 5G, upang kumonekta sa internet.

Maraming IoT device na karaniwang makikita sa mga tahanan at negosyo sa Australya ay idinisenyo na hindi pinag-isipan ang seguridad. Nagresulta ito sa mga device na madaling makompromiso sa pamamagitan ng internet. Ang ganitong mga insidente ay maaaring magbigay-daan upang ang mga cybercriminal ay maka-access nang hindi mo gusto sa iyong device at personal data para sa mga malicious na layunin.

Bago bumili ng IoT device

Mahalagang magsaliksik ng mga device bago bumili, dahil nagbibigay ang mga tagagawa ng iba't ibang antas ng seguridad. Bago bumili ng device, ihambing ang mga katulad na device na ibinebenta ng iba't ibang tagagawa. Kabilang sa mga dapat isaalang-alang ang:

1. **Ang device ba ay ginawa ng isang kilalang kumpanyang may mabuting reputasyon at ibinebenta ng isang kilalang store na may mabuting reputasyon?** Ang mga kilalang kumpanyang may mabuting reputasyon ay mas malamang na gumawa ng mga device na isinaisip ang seguridad. Ang mga kilalang store na may mabuting reputasyon ay mas malamang na magbenta lamang ng mga device mula sa mga kilalang kumpanya na may mabuting reputasyon, at may mas mahigpit na supply-chain na tinitiyak na ang device ay makakarating sa iyo ayon sa nilalayon ng tagagawa.

2. **Posible bang baguhin ang password?** Magandang laging pinapalitan ang iyong password. Gayunpaman, kung ang device ay ipinadala na may mahinang default password, lalong mahalaga na laging palitan ang password. Ang isang device na may mahusay na seguridad ay dapat may mga password na natatangi, mahirap matukoy, kumplikado at halos imposibleng mahulaan, dahil ang mahihinang default password ang pinakamadaling paraan upang ma-atake ang isang device.

3. **Nagbibigay ba ng mga update ang tagagawa?** Mahalagang mag-alok ang mga kumpanya ng mga update para ayusin ang mga kahinaan ng device kapag natuklasan ang mga ito. Halimbawa, kung ang software sa device ay naglalaman ng mga kilalang kahinaan o ang mga hacker ay bumuo ng mga bagong paraan para makompromiso ang iyong device, ang mga update ay kinakailangan sa pag-ayos nito.

4. **Anong data ang kokolektahin ng device at kanino ibabahagi ang data?** Ang impormasyon kung anong data ang kokolektahin at kung paano ito gagamitin ay dapat na madaling makuha sa website ng tagagawa o sa kanilang patakaran sa pribasya. Mahalagang isaalang-alang lagi ang impormasyong kinokolekta ng online o mobile application.

5. **Ginagawa lang ba ng device ang gusto mong gawin nito?** Ang pagbili ng device na gumagawa ng higit pa sa kailangan mo, kabilang ang pagkonekta sa internet, ay maaaring makabawas sa iyong seguridad. Maaaring dumagdag sa mga kahinaan ng device laban sa mga pag-atake ang mga device capability na hindi mo naman ginagamit at walang anumang benepisyo sa iyo.

Ang IoT device

Tandaan ang ilang simpleng tanong habang sine-set up ang iyong device, para matulungan kang panatilihing mas secure ang iyong network at data.

1. **Kailangan bang nakakonekta ang device sa internet?** Dahil maaari itong konektado ay hindi nangangahulugan na dapat itong gawin. Ang mga device na hindi nakakonekta sa internet ay mas malamang na hindi makokompromiso. Kung hindi mo gagamitin ang mga feature na nangangailangan ng koneksyon sa internet, dapat mong pag-isipan kung dapat itong ikonekta.

2. **Nasa secure na lokasyon ba ang device?** Kung hindi kailangang i-install ang device sa isang hindi secure na lugar, ang pag-install nito sa isang secure na lokasyon ay makakabawas sa panganib na pisikal na makompromiso.

3. **Papalitan ko ba ang default na username at password?** Mahalagang gumamit ka ng malakas na password o passphrase. Kung ang iyong device ay hindi naipadala na may natatangi, mahirap matukoy, kumplikado at halos imposibleng mahulaang password, kailangang baguhin ang password na ito. Ang mga default username at password ay kinokolekta at ipino-post online, na ginagawang mahina ang iyong device.

4. **Ang aking Wi-Fi network ba ay secure na naka-set up, at mayroon ba itong secure na password?** I-secure ang iyong Wi-Fi network at router upang gawing mas mahirap para sa mga umaatake na i-access ang iyong device at network.

Dagdagan pa ang pagsisikap

Mag-set up ng karagdagang Wi-Fi network sa iyong router para sa mga IoT device lang. Ito ay maaaring kilala sa iyong Wi-Fi router bilang 'guest' network. Kung ang iyong mga IoT device ay hindi nangangailangan ng komunikasyon sa pagitan ng isa't isa, paganahin ang feature na 'client isolation'. Ang pagpapanatiling nakahiwalay ang iyong mga IoT device sa iyong sensitibong data ay nagsisiguro na kung makompromiso ng IoT device, hindi makaka-access sa iyong iba pang mga device o data.

5. **Naka-off ba ang mga hindi kinakailangang feature ng device?** Kung ang iyong device ay may mga hindi ginugusto o hindi kinakailangang mga feature (tulad ng mga camera o mikropono), ang mga ito ay dapat i-disable kung posible.

Dagdagan pa ang pagsisikap

Maghanap ng configuration setting na nagbabanggit ng pag-enable ng remote access sa web administration interface ng device mula sa local LAN o WAN/internet. Tiyaking naka-set ito sa local LAN, maliban kung ikaw mismo ang nangangailangan ng reemote pag-access.

Pagpapanatili ng IoT device

Mayroong ilang mahahalagang bagay na dapat tandaan kapag na-set up at ginagamit na ang iyong IoT device. Kabilang dito ang:

1. **I-reboot nang regular ang iyong mga device.** Maaaring may mga virus kung ang IoT device ay magsisimulang maging mabagal o hindi magamit. Karamihan sa malware ay nakaimbak sa memory at madaling maalis sa pamamagitan ng pag-reboot ng device, ibig sabihin, sa pamamagitan ng pag-off at pag-on ng device. Kung ang device ay patuloy na bumabagal o hindi gumagana pagkatapos i-reboot, subukang mag-factory reset; gayunpaman tandaan na maaari nitong mabura ang lahat ng iyong user data at mga personalised setting.

2. **Ilapat ang mga regular na update.** Awtomatikong naglalapat ng mga update ang ilang device. Para sa mga hindi, regular na suriin sa tagagawa at ilapat ang mga update kapag available na ang mga ito. Kapag hindi na available ang mga update para sa iyong device, isaalang-alang ang pag-upgrade sa mas bagong device kung saanavailable ang mga update. Ang mga device na walang access sa mga security update ay hindi mapoprotektahan kung may natuklasang mga bagong kahinaan, at ang mga device na ito ay maaaring maging panganib sa iyong network, sa iyong pribasya at sa iyong data.

3. **I-off ang iyong device kapag hindi ito ginagamit.** Ang pag-iwan sa mga hindi ginagamit at hindi namo-monitor na device na naka-on at nakakonekta sa iyong Wi-Fi network nang matagal ay maaaring magpapataas ng posibilidad na maatake ang iyong mga device. Isang opsyon upang awtomatikong makamit ito ay ang paggamit ng power outlet timer upang magbigay lang ng power sa device sa mga tinukoy na oras.

4. **Bantayan ang malaking pagtaas sa iyong buwanang paggamit sa internet o singil.** Ang mga malaking pagtaas sa paggamit ng internet o mga singil ay maaaring nagpapahiwatig na ang iyong device ay nakompromiso. Maliban na lang kung sisiyasatin ito ng IT department sa loob ng inyong negosyo, dapat ilapat ang factory reset (gayunpaman, tandaan na maaaring mabura nito ang lahat ng iyong user data at mga personalise setting), na susundan ng pagpapalit ng iyong password.

Pagtatapon ng isang IoT device

Ang pagtatapon ng device (sa pamamagitan ng pagtatapon o pagbebenta nito) ay maaaring magbigay sa ibang tao ng madaling access sa iyong personal na impormasyon o data.

Kabilang sa mga paraan upang maiwasan ito:

1. **Burahin lahat ng data at personal na impormasyon.** Dapat magbigay ang tagagawa ng paraan kung paano buburahin ang iyong data at personal na impormasyon mula sa device at sa mga nauugnay na application. Ang pagbubura ng iyong personal na impormasyon ay nagsisiguro na walang sinuman ang makaka-access dito pagkatapos mong itapon ang device. Tanggalin ang iyong online account kung hindi na ito kailangan nang wala ang IoT device.

2. **I-factory reset ang device.** Ang factory reset ay idinisenyo upang burahin ang data na nakatabi sa local storage at i-reset ang mga password, username at mga setting pabalik sa default. Tingnan ang user manual ng device o website ng tagagawa para sa impormasyon kung paano magsagawa ng factory reset.

3. **Idiskonekta ang device sa mga mobile phone at iba pang device.** Ang pagtatapon ng isang device na may access pa rin sa iyong iba pang mga device, network o online account ay posibleng maging daan upang maka-access ang iba. Tiyaking na-check mo ang iba mo pang mga device at natanggal ang anumang koneksyon sa device na iyong itatapon. Alisin ang anumang mga permisong ibinigay sa mobile application na hindi na kailangan.

4. **Alisin ang anumang naaalis na media (hal. mga USB flash drive, memory card atbp.) na naka-attach sa device.** Ang naaalis na media ay maaaring maglaman ng personal data na hindi na-delete sa pag-factory reset at dapat na pisikal na alisin, pisikal na sirain at itapon nang hiwalay sa device.

Tulong

Makipag-ugnayan sa Australian Cyber Security Centre ng Australian Signals Directorate sa pamamagitan ng pag-email sa asd.assist@defence.gov.au o tawagan ang 24/7 Hotline para sa agarang tulong sa **1300 CYBER1** (**1300 292 371**).

Iulat ang cybercrime sa ReportCyber sa www.cyber.gov.au/report

Makipag-ugnayan sa IDCARE sa pamamagitan ng kanilang website na www.idcare.org kung nakaranas ka ng pagnanakaw ng pagkakakilanlan (identity theft).

Bisitahin ang www.cyber.gov.au para sa payo para sa iyo at sa iyong pamilya. Mag-sign up para sa libreng ACSC Alert Service sa mga kamakailang online threat.

Gawin nating pinaka-secure na lugar ang Australya para kumonekta sa online.

Para sa payo sa cyber security, bisitahin ang www.cyber.gov.au

Pagtatatwa

Ang materyal sa gabay na ito ay may pangkalahatang katangian at hindi dapat ituring bilang legal na payo o pagsalalayan para sa tulong sa anumang partikular na pangyayari o emerhensya. Sa anumang mahalagang bagay, dapat kang humingi ng naaangkop na independiyenteng propesyonal na payo kaugnay ng iyong sariling mga kalagayan.

Ang Commonwealth ay hindi tumatanggap ng responsibilidad o pananagutan para sa anumang pinsala, pagkawala o gastos na natamo bilang resulta ng pagsalalay sa impormasyong nakapaloob sa gabay na ito.

Para sa higit pang impormasyon, o para mag-report ng insidente sa cyber security, makipag-ugnayan sa amin:

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

Ang numerong ito ay magagamit lamang sa loob ng Australia.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre