Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Gabay sa seguridad ng cyber para sa maliit na negosyo

cyber.gov.au

Panimula

Para sa isang maliit na negosyo, kahit isang maliit na insidente ng seguridad sa cyber ay maaaring magkaroon ng mapangwasak na epekto.
Kasama sa gabay na ito ang mga pangunahing hakbang sa seguridad upang makatulong na protektahan ang iyong negosyo laban sa mga karaniwang banta sa seguridad sa cyber.
Bilang panimulang punto, inirerekomenda namin ang sumusunod na tatlong hakbang:

- I-on ang multi-factor authentication
- I-update ang iyong software
- I-back up ang iyong impormasyon

Maaaring kasama sa gabay na ito ang mga hakbang na hindi nauugnay sa iyong negosyo, o maaaring may mas kumplikadong mga pangangailangan ang iyong negosyo. Pagkatapos kumpletuhin ang gabay na ito, inirerekomenda namin sa mga maliliit na negosyo na ipatupad ang Maturity Level One ng **Essential Eight**.
Kung mayroon kang mga tanong tungkol sa payong ito o sa mas malawak na seguridad sa cyber, inirerekomenda naming makipag-usap ka sa isang IT professional o isang pinagkakatiwalaang tagapayo.

Bisitahin ang cyber.gov.au upang basahin ang aming buong gabay, kabilang ang payo kung ano ang gagawin para sa bawat hakbang.

Talaan ng mga Nilalaman

Banta sa maliliit na mga negosyo

Mga mensaheng scam

Ang mga scam ay pangkaraniwang paraan upang ma-target ng mga cybercriminal ang maliliit na negosyo. Ang kanilang layunin ay i-scam ka o ang iyong mga kawani upang:

- magpadala ng pera o mga gift card
- mag-click sa mga mapanirang link o attachment
- magbigay ng sensitibong impormasyon, tulad ng mga password.

Maaaring subukang i-scam ng mga cybercriminal ang iyong negosyo sa pamamagitan ng email, text message, tawag sa telepono at social media. Madalas silang magpanggap na isang tao o organisasyong pinagkakatiwalaan mo.

Mga pag-atakeng phishing

Partikular na ipinag-aalala ng mga maliliit na negosyo ang **mga pag-atakeng phishing.** Ang mga scam na ito ay kadalasang naglalaman ng link sa isang pekeng website kung saan hinihikayat kang mag-log in sa isang account o maglagay ng mga kumpidensyal na detalye.

Karaniwang kinokompromiso ng mga pag-atakeng phishing ang mga password ng iyong account. Kadalasang ginagamit ng mga cybercriminal ang paraang ito para makontrol ang mga social media account ng maliliit na negosyo at humingi ng ransom.

Mga paraan upang mapagaan

Kung ang isang mensahe ay mula sa isang kilalang entity na mukhang kahina-hinala, mag-ingat. Makipag-ugnayan sa tao o negosyo sa ibang paraan upang malaman kung lehitimo ang mensahe. Gumamit ng mga detalye sa pakikipag-ugnayan na nahanap mo sa isang lehitimong pinagmulan, halimbawa sa pamamagitan ng pagbisita sa opisyal na website ng negosyo, at hindi iyong nakalagay sa kahina-hinalang mensahe.

Matuto kung paano tumukoy ng mga scam at pag-atakeng phishing gamit ang mga sumusunod na mapagkukunan:

- Kilalanin at iulat ang mga scam
- Alamin kung paano matutukoy ang mga phishing scam
- Pag-tuklas ng mga Socially Engineered na Mensahe.

Pag-aaral ng kaso:

Nakatanggap ang isang empleyado sa isang kumpanya ng courier ng email mula sa isa sa kanilang executive staff, na humihiling na bumili sila ng 6 x $500 MasterCard prepaid credit card. Sinabihan siya ng executive na panatilihin itong kumpidensyal dahil ang mga card ay mga gift voucher para sa mga miyembro ng kawani. Kapag nabili na, ang empleyado ay hihilingan na kunan ng larawan ang magkabilang panig ng mga card at ipadala ang mga ito sa Executive bilang patunay ng pagbili.

Gaya ng tagubilin, nagpunta ang empleyado sa isang post office at ginamit ang kanyang personal na credit card upang bilhin ang mga gift card. Tumugon siya sa email ng executive at ipinadala ang mga larawan ng mga gift card bilang patunay.

Pagbalik mula sa post office, ibinigay ng empleyado ang mga pisikal na card sa executive - na walang nalalaman tungkol dito. Sa pagsusuri, **lahat ng email tungkol sa mga gift card ay nagmula sa isang random na email address at hindi mula sa lehitimong email account ng executive. Ito ay isang scam.**

Mga pag-atake sa email

Bilang karagdagan sa mga scam tulad ng phishing, isang karaniwang pag-atake sa email laban sa maliliit na negosyo ay ang **business email compromise** (BEC). Maaaring magpanggap ang mga kriminal bilang mga kinatawan ng negosyo sa pamamagitan ng paggamit ng mga nakompromisong email account, o sa pamamagitan ng iba pang paraan – tulad ng paggamit ng domain name na mukhang katulad ng isang tunay na negosyo. Bukod sa pagnanakaw ng impormasyon, ang layunin ng mga pag-atakeng ganito ay kadalasang i-scam ang mga biktima sa pagpapadala ng mga pondo sa isang bank account na pinamamahalaan ng scammer.

Mga paraan upang mapagaan

Ang pinakamahusay na depensa laban sa mga pag-atake sa email ay pagsasanay at kaalaman para sa iyong mga empleyado. Tiyaking alam ng iyong mga kawani na lagi silang maging maingat sa mga email na may sumusunod:

- mga kahilingan para sa mga pagbabayad, lalo na kung madalian o overdue
- pagbabago ng mga detalye ng bangko
- isang email address na mukhang hindi tama, tulad ng domain name na hindi eksaktong tumutugma sa pangalan ng kumpanya ng supplier.

Bagama't ang mga pag-atakeng ito ay maaaring mapangwasak, ang mga hakbang sa pagpapagaan ay madali at halos walang bayad. **Kapag nakatanggap ang mga kawani ng mga email na tulad nito, ang pinakamabuting gawin ay tawagan ang nagpadala upang kumpirmahin kung ang mga ito ay lehitimo.**Huwag gamitin ang mga detalye ng contact na ipinadala sa iyo dahil maaaring hindi totoo ang mga ito. Ipatupad ang pormal na proseso na susundin ng mga kawani kapag nakatanggap sila ng mga kahilingan sa pagbabayad o kung nagbago ang mga detalye ng bangko.

Matutunang protektahan ang iyong negosyo laban sa mga BEC scam at nakompromisong email gamit ang mga sumusunod na mapagkukunan:

- Kompromiso sa email ng negosyo
- Protektahan ang iyong negosyo laban sa mapanlinlang at nakompromisong email
- Ano ang dapat gawin kung ang iyong negosyo ay na-target ng mapanlinlang at nakompromisong email.

Pag-aaral ng kaso:

Isang maliit na negosyo ng konstruksiyon ang nakatanggap ng email mula sa kanilang supplier na nagsasabing nagpalit ito ng bangko. Nagbigay ang supplier ng mga bagong detalye ng account para sa mga pagbabayad ng invoice. Dahil parang lehitimo ang email, **hindi tinawagan ng construction business ang supplier para kumpirmahin ang pagbabago ng mga detalye ng bank account.**

Binayaran ng negosyo ang invoice mula sa supplier ng mahigit sa $70,000. Nang sumunod na araw, nagkamaling binayaran ng isa pang empleyado ang parehong invoice para sa karagdagang halaga na mahigit sa $70,000. Sa kabuuan, mahigit $150,000 ang binayaran sa bagong bank account.

Nang tumawag ang negosyo sa kanilang supplier upang hilingin kung puwede nilang i-refund ang nadobleng bayad, sinabi ng supplier na mali ang mga detalye ng bangko na iyon. Agad na inilunsad ang pagsisiyasat, at natuklasan ng supplier na isa sa kanilang mga email account ay na-hack at nagpapadala ng mga mapanlinlang na detalye ng bank account. Walang naibalik na pondo. **Walang naibalik na pondo.**

Mapanirang software

Ang malware ay isang malawak na termino para sa mapanirang software na idinisenyo upang magdulot ng pinsala, gaya ng ransomware, mga virus, spyware at mga trojan. Ang malware ay maaaring:

- nakawin o i-lock ang mga file sa iyong aparato
- nakawin ang iyong mga numero ng bangko o credit card
- nakawin ang iyong mga username at password
- kontrolin o mag espiya sa iyong computer.

Maaaring ihinto ng malware ang iyong aparato sa paggana ng maayos, tanggalin o sirain ang iyong mga file, o payagan ang iba na i-access ang iyong personal na impormasyon o impormasyon ng negosyo. Kung ang iyong device ay nahawaan ng malware, maaari kang maging mahina sa iba pang mga pag-atake. Ang malware ay maaari ring kumalat sa iba pang mga device sa iyong network.

Maaaring mahawaan ng malware ang iyong device sa maraming paraan, kabilang ang:

- pagbisita sa mga website na nahawaan ng malware
- pag-download ng mga nahawaang file o software mula sa internet
- pagbubukas ng mga nahawaang email attachment.

Ransomware

Ang Ransomware ay isang karaniwan at mapanganib na uri ng malware. Gumagana ito sa pamamagitan ng pag-lock o pag-encrypt ng iyong mga file upang hindi mo na ma-access ang mga ito. Ang isang ransom, kadalasan sa anyo ng cryptocurrency, ay hinihingi upang maibalik ang access sa mga file. Maaari ring magbanta ang mga cybercriminal na mag-lathala o magbenta ng mga datos online, maliban kung babayaran ang isang ransom.

Mga paraan upang mapagaan

Bagama't makakatulong ang anti-virus o software na pangseguridad upang protektahan ka laban sa malware, walang software na 100% epektibo. Dapat maging alerto ang mga kawani sa mga email, website at pag-download ng file, at regular na i-update ang kanilang mga aparato upang mapanatili ang seguridad nito.

Tingnan ang mga sumusunod na mapagkukunan para sa higit pang impormasyon sa pagprotekta sa iyong negosyo laban sa ransomware:

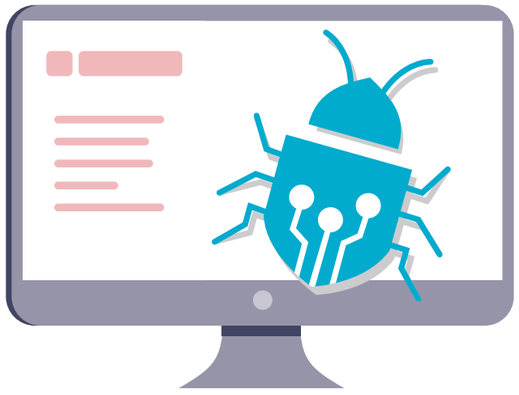
- Ransomware
- Protektahan ang iyong sarili laban sa mga pag-atake ng ransomware
- Ano ang gagawin kung ikaw ay na-ransom

Pag-aaral ng kaso:

Ang mga empleyado ng isang tindahan ng mga piyesa ng sasakyan ay pumasok sa trabaho isang umaga at hindi nagawang i-boot ang kanilang server computer. Nang magkaroon ng access ang kanilang IT provider sa server, nakakita sila ng bukas na window na nagsasabing ang lahat ng mga datos ng computer ay na-encrypt. Hinihiling ng mensahe na magbayad sila ng ransom sa bitcoin upang mabuksan ang mga file.

May backup drive na nakasaksak sa computer, na na-encrypt din. Sinubukan nilang ikonekta ang higit pang mga backup drive, ngunit ang mga file ay awtomatikong na-encrypt sa loob ng ilang segundo. **Nabigo silang alisin ang ransomware bago subukang bawiin ang kanilang mga datos at nawala ang bawat backup file na mayroon sila.**

Ang tanging opsyon na natitira ay i-factory reset ang server at magsimulang muli gamit ang isang bagong sistema. Ang kanilang negosyo ay nawalan ng maraming taong mga datos at kailangang magsimulang muli.



Bigyan ng seguridad ang iyong mga account

I-on ang multi-factor authentication

Ang multi-factor authentication (MFA) ay nagpapahirap sa mga cybercriminal na i-access ang iyong mga account.

Nagdaragdag ang MFA ng isa pang layer ng seguridad sa iyong account. Isa ito sa pinakamabisang paraan para protektahan ang iyong mga account laban sa pagkuha ng access ng ibang tao, kaya dapat mong gamitin ito hangga't maaari. Ang sinumang magla-log in sa iyong account ay kailangang magbigay ng iba pang bagay bilang karagdagan sa iyong username at password. Ito ay maaaring isang natatanging code mula sa isang text message o isang authenticator app. Para sa karagdagang impormasyon, basahin ang aming payo sa MFA, na makukuha sa **cyber.gov.au/mfa**.

✓ **I-on ang MFA hangga't maaari, simula sa iyong pinakamahahalagang account.**

Ipatupad ang mga kontrol sa pag-access

Ang paghihigpit sa pag-access ng user ay maglilimita sa pinsalang dulot ng insidente ng seguridad sa cyber.

Ang kontrol sa pag-access ay isang paraan upang limitahan ang pag-access sa ilang partikular na mga file at sistema. Karaniwan, hindi nangangailangan ng ganap na access ang mga kawani sa lahat ng mga datos, account, at sistema sa isang negosyo. Dapat lamang silang pahintulutan na ma-access ang kailangan nila upang maisagawa ang kanilang mga tungkulin.

Ang paghihigpit sa pag-access ay makakatulong upang limitahan ang pinsalang dulot ng insidente ng seguridad sa cyber. Halimbawa, kung ang computer ng isang kawani ay nahawaan ng ransomware, kung may wastong mga kontrol sa pag-access maaari lamang itong makaapekto sa isang maliit na bilang ng mga file sa halip na sa buong negosyo.

✓ **Tiyaking maa-access lang ng bawat user ang kailangan nila para sa kanilang tungkulin.**

Gumamit ng malalakas na password o passphrase

Protektahan ang iyong mga account laban sa mga cybercriminal gamit ang isang ligtas na password o passphrase.

Maraming maliliit na negosyo ang nahaharap sa mga pag-atake sa cyber bilang resulta ng hindi magandang gawi sa password. Halimbawa, ang paggamit ng parehong password sa maraming account. Maaari mong gamitin ang mga password manager at mga passphrase upang lumikha ng mga malalakas na password.

Ang password manager ay kumikilos bilang isang virtual safe para sa iyong mga password. Magagamit mo ito upang lumikha at mag-imbak ng matibay at **natatanging** mga password para sa bawat isa sa iyong mga account. Kung marami kang account, inaalis nito ang kahirapang matandaan ang mga natatanging password. Hindi mo kailangang tandaan ang mga password o ang mga account para dito, dahil lahat ito ay nakatala sa iyong password manager.

Para sa mga account na regular kang nagsa-sign in, o yaong ayaw mong iimbak sa isang password manager, isaalang-alang ang paggamit ng passphrase bilang iyong password. Ang mga passphrase ay kumbinasyon ng mga random na salita, halimbawa 'crystal onion clay pretzel'. Kapaki-pakinabang ang mga ito kapag gusto mo ng secure na password na madaling matandaan. Gumamit ng random na halo ng apat o higit pang salita at panatilihin itong kakaiba – **huwag muling gamitin ang passphrase** sa maraming account. Para sa karagdagang impormasyon, basahin ang aming payo tungkol sa mga passphrase at password manager, na makukuha sa **cyber.gov.au/passphrases**.

✓ **Gumamit ng password manager para gumawa at mag-imbak ng mga natatanging password para sa bawat isa sa iyong mahahalagang account.**

Pamahalaan ang mga shared account

Ang mga shared account ay maaaring makakompromiso sa seguridad at nagpapahirap sa pagsubaybay sa mapanirang aktibidad.

Sa isang maliit na negosyo, maaaring may mga lehitimong dahilan kung bakit kailangang ng mga kawani ng mga shared account, ngunit dapat itong iwasan hangga't maaari. Kapag maraming kawani ang gumagamit ng parehong account, maaaring mahirap subaybayan ang aktibidad na nagmula sa isang partikular na empleyado at lalong mas mahirap subaybayan ang mga cybercriminal na pumapasok. Maliban kung papalitan mo ang password, maaari ring magpatuloy ang mga empleyado sa pag-access ng mga account kahit na umalis na sila sa negosyo.

✓ **Limitahan ang paggamit ng mga shared account at gawing ligtas ang anumang ginagamit na account sa iyong negosyo.**

Protektahan ang iyong mga aparato at impormasyon

I-update ang iyong software

Ang pag-update ng iyong software ay isa sa pinakamahusay na paraan upang maprotektahan ang iyong negosyo laban sa pag-atake sa cyber.

Maaaring ayusin ng mga pag-update ang mga depekto sa seguridad sa iyong operating system at iba pang software, upang mas mahirap para sa isang cybercriminal na makapasok. Laging may mga bagong depektong natutuklasan, kaya huwag balewalain ang mga prompt para mag-update. Ang regular na pag-update ng iyong software ay magbabawas sa pagkakataong magamit ng isang cybercriminal ang nalamang kahinaan upang patakbuhin ang malware o i-hack ang iyong aparato. Kung kailangan mo ng tulong, ang ACSC ay naglathala ng gabay sa mga update.

Kung masyadong luma ang iyong aparato o software, maaaring hindi available ang mga update. Kung ang manufacturer ay huminto sa pagsuporta sa produkto sa pagbibigay ng mga update, dapat mong isaalang-alang ang pag-upgrade sa isang mas bagong produkto upang manatili ang seguridad nito. Ang mga halimbawa ng mga sistema na hindi na nakakatanggap ng mga pangunahing update ay ang **iPhone 7** at **Microsoft Windows 7.**

Para sa karagdagang impormasyon, basahin ang aming gabay sa mga update, na makukuha sat **cyber.gov.au/updates**.

✓ **I-on ang mga awtomatikong pag-update para sa iyong mga aparato at software.**

Gumamit ng software ng seguridad

Ang software ng seguridad tulad ng proteksyon ng antivirus at ransomware ay makakatulong sa pagprotekta sa iyong mga aparato.

Gumamit ng software ng seguridad upang matukoy at maalis ang malware sa iyong mga aparato. Maaaring i-set up ang antivirus software upang regular na mag-scan para sa mga kahina-hinalang file at programa. Kapag may nakitang banta, makakatanggap ka ng alerto at ang kahina-hinalang file ay makukuwarentina o aalisin.

Maraming maliliit na negosyo ang maaaring **gumamit ng Windows Security** upang protektahan ang kanilang sarili laban sa mga virus at malware. Ang Windows Security ay kasama sa Windows 10 at Windows 11 na mga aparato at may kasamang libreng proteksyon laban sa virus at pagbabanta.

Magagamit mo rin ito para i-on ang mga gamit sa proteksyon ng ransomware sa iyong aparato.

Para sa mga alternatibong produkto at opsyon, basahin ang aming payo tungkol sa antivirus software, sa pamamagitan ng pag-search sa salitang *antivirus* sa cyber.gov.au.

✓ **I-set up ang software ng pang-seguridad upang kumpletuhin ang mga regular na pag-scan sa iyong mga aparato.**

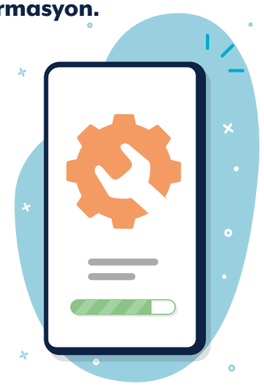
I-back up ang iyong impormasyon

Makakatulong sa iyo ang mga regular na pag-backup upang makuhang-muli ang iyong impormasyon kung ito ay nawala o nakompromiso.

Ang pag-back up ng mahalagang impormasyon ay dapat maging regular o awtomatikong kagawian sa iyong negosyo. Kung walang regular na pag-backup, maaaring imposible na para sa iyo na makuhang-muli ang iyong impormasyon pagkatapos maatake sa cyber.

Maraming mga pamamaraan at produkto na maaari mong gamitin upang i-back up ang iyong impormasyon. Para sa detalyadong payo sa pag-back up ng iyong negosyo, basahin ang aming payo para sa mga pag-backup, na makukuha sa **cyber.gov.au/backups**. Iba-iba ang pinakamabuting opsyon para sa bawat negosyo, kaya makipag-usap sa isang IT professional kung hindi ka sigurado.

✓ **Lumikha at magpatupad ng plano para sa regular na pag-back up ng iyong impormasyon.**



I-secure ang iyong network at mga panlabas na serbisyo

Protektahan ang iyong negosyo laban sa pag atake sa cyber sa pamamagitan ng pagtugon sa mga potensyal na kahinaan sa inyong network.

Ang mga aparato at serbisyo sa inyong network ay maaaring pangunahing target para sa mga cybercriminal. Marami sa mga sistema na ito ay kumplikadong gawing ligtas, kaya talakayin ang mga sumusunod na rekomendasyon sa isang propesyonal sa IT.

- **I-secure ang iyong mga server:** Kung gumagamit ka ng NAS o iba pang server sa iyong tahanan o negosyo, dagdagan ang pag-iingat na i-secure ang mga ito. Ang mga aparato na ito ay karaniwang mga target ng mga cybercriminal dahil madalas nag-iimbak ang mga ito ng mahahalagang file o gumaganap ng mahahalagang gawain. Maraming mga pamamaraan sa pagpapagaan na kinakailangan upang maprotektahan ang mga aparato na ito. Halimbawa, mahalagang tiyaking regular na ina-update ang anumang server o NAS na aparato. Ang mga administratibong account ay dapat i-secure gamit ang malakas na passphrase o multi-factor authentication.

- **Bawasan ang external-facing footprint:** Suriin at gawing ligtas ang anumang mga serbisyong nasa internet sa iyong network. Maaaring kabilang dito ang Remote Desktop, mga File Share, Webmail at mga serbisyo ng malayuang pangangasiwa.

- **Lumipat sa mga serbisyo sa cloud:** Isaalang-alang ang paggamit ng mga serbisyo sa online o cloud na nag-aalok ng built-in na seguridad, sa halip na pamahalaan ito nang mag-isa. Halimbawa, gumamit ng mga online na serbisyo para sa mga bagay tulad ng email o pagho-host ng website sa halip na patakbuhin at i-secure ang mga serbisyong ito.

- **Pahusayin ang seguridad ng iyong router:** Sundin ang aming gabay sa mga paraan upang maging ligtas ang iyong router, kabilang ang pag-update ng mga default na password, pag-on sa “Guest” na Wi-Fi para sa mga customer o bisita, at paggamit ng pinakamalakas na mga protocol sa pag-encrypt. I-search ang salitang *router* sa **cyber.gov.au** para sa higit pang impormasyon.

- **Alamin ang iyong cyber supply chain:** Ang mga modernong negosyo ay kadalasang nag-a-outsource ng maraming serbisyo. Halimbawa, ang paggamit ng Managed Service Provider upang i-maintain ang kanilang IT. Ang mga isyu sa seguridad sa mga serbisyo o provider na ito ay maaaring magkaroon ng malaking epekto sa iyong negosyo. Para sa detalyadong payo sa cyber supply chain risk management, basahin ang aming Cyber Supply Chain Guidance sa **cyber.gov.au**.

✓ **Makipag-usap sa isang propesyonal sa IT tungkol sa mga paraan upang i-secure ang iyong network.**

Patatagin ang iyong website

Ang mga website ay pangunahing target sa mga pag-atake sa cyber.

Protektahan ang iyong website laban sa pag-hijack sa pamamagitan ng pagsunod sa ilang pangunahing hakbang sa seguridad:

- I-secure ang iyong pag-login sa website gamit ang multi-factor authentication o isang malakas na password

- regular na i-update ang mga sistema at plugin ng pamamahala ng nilalaman (content management systems and plugins) ng iyong website

- i-back up nang regular ang iyong website upang maibalik mo ito pagkatapos ng pag-atake sa cyber.

Ang ACSC ay may mga karagdagang mapagkukunan na magagamit ng mga may-ari ng website. Hanapin ang mga mapagkukunang ito sa **cyber.gov.au**:

- Mabilis na Panalo para sa iyong Website
- Pagpapatupad ng mga Certificate, TLS, HTTPS at Opportunistic TLS
- Seguridad sa Sistema ng Pangalan ng Domain para sa mga May-ari ng Domain
- Paghahanda at Pagtugon sa mga Pag-atake na Pagtanggi sa Serbisyo (Denial-of-Service)

✓ **Basahin ang mga mapagkukunan ng ACSC tungkol sa seguridad ng website.**

I-reset ang iyong mga aparato bago ito itapon o ibenta

Ang mga datos sa iyong mga lumang aparato ay maaaring ma-access ng ibang mga tao.

Kung hindi mo ligtas na dinispatsa ang iyong mga aparato, maaaring ma-access ng mga cybercriminal ang impormasyon na naroon. Maaaring kabilang dito ang mga email, file at iba pang mga datos ng negosyo. Alisin ang lahat ng impormasyon mula sa iyong mga aparato sa negosyo bago ibenta, i-trade o itapon ang mga ito. Halimbawa, sa pamamagitan ng pag-factory reset. Makakatulong ito na matanggal ang anumang impormasyon at ibalik ang aparato sa orihinal nitong mga setting.

Para sa payo sa pag-reset ng iyong mga aparato, basahin ang aming gabay tungkol sa ligtas paraan ng pag-dispatsa ng iyong aparato. I-search ang salitang dispose sa **cyber.gov.au**.

✓ **Magsagawa ng factory reset bago ibenta o itapon ng mga aparatong pangnegosyo.**

Panatilihing naka-lock ang iyong mga aparato at pisikal na na-secure

Ang paghihigpit sa pag-access sa iyong mga aparato sa negosyo ay makakabawas sa mga pagkakataong makapasok ang mapanirang aktibidad.

Ang paglilimita sa pisikal na pag-access sa iyong mga aparato sa negosyo ay isang simpleng paraan upang maiwasan ang pagnanakaw ng mga datos o iba pang mapanirang aktibidad. Hindi dapat itago ang mga aparato sa negosyo kung saan maaaring ma-access ang mga ito ng hindi awtorisadong mga kawani o miyembro ng publiko.

Gumamit ng mga kontrol sa seguridad para higit pang maprotektahan ang iyong mga aparato sa negosyo. Dapat man lang na naka-lock ang mga ito gamit ang passphrase, PIN o biometrics. Tiyaking nakatakdang awtomatikong mag-lock ang mga aparato na ito pagkaraan ng sandaling walang aktibidad.

✓ **I-konpigura ang mga aparato upang awtomatikong mag-lock pagkaraan ng sandaling walang aktibidad.**

Protektahan ang mga datos ng iyong negosyo

Ang mga datos na hawak ng iyong negosyo ay nakakaakit na target ng mga cybercriminal.

Dumadalas ang mga panghihimasok (breaches) sa mga mga datos – huwag hayaang mabiktima ang iyong negosyo. Mahalagang malaman kung anong mga datos ang hawak ng iyong negosyo, at saang mga lokasyon. Kapag alam mo na, gamitin ang mga rekomendasyon sa gabay na ito upang makatulong na protektahan ang iyong mga datos laban sa pag-access ng mga cybercriminal. Ang ilang maliliit na negosyo ay maaari ring magkaroon ng mga karagdagang obligasyon sa ilalim ng batas.

- **Pagsama-samahin ang mga datos ng iyong negosyo.** Maaaring mayroon kang mga datos na nakaimbak sa maraming aparato o serbisyo. Kapag ang mga datos ay desentralisado, pinapataas nito ang bilang ng mga sistema na kailangan mong panatilihing ligtas at nai-back up. Ang maraming mga sistema ay maaari ring magbigay ng higit pang mga pagkakataon para sa isang cybercriminal na umatake. Kung posible, iimbak ang mga datos ng iyong negosyo sa isang sentral na lokasyon na ligtas at regular na naka-back up. Ang pagsentro sa iyong mga datos ay maaaring lumikha ng mas malaking panghihimasok (breach) kung ang iyong mga sistema ay nakompromiso, kaya tiyaking ang sentral na lokasyong ito ay sapat na protektado ng mga ligtas na konpigurasyon at hinigpitang pag-access. Makipag-usap sa isang IT o cyber security professional para sa payo.
- **Alamin ang iyong mga obligasyon sa pagprotekta ng mga datos.** Ang ilang maliliit na negosyo ay maaaring may mga legal na obligasyon sa paghawak ng personal na impormasyon na kanilang kinokolekta. Basahin ang gabay para sa maliliit na negosyo ng Office of the Australian Information Commissioner upang malaman ang higit pa, na makukuha sa **oaic.gov.au.** Kumunsulta sa isang legal na propesyonal kung hindi ka sigurado.

✓ **Alamin ang mga datos na hawak ng iyong negosyo at ang iyong mga responsibilidad upang protektahan ito.**

Ihanda ang iyong mga kawani

Turuan ang mga empleyado

Ang mga empleyadong may mahusay na kasanayan sa seguridad sa cyber ang iyong unang linya ng depensa laban sa mga pag-atake sa cyber.

Ang iyong mga empleyado ay dapat magkaroon ng kamalayan sa seguridad sa cyber, kabilang ang mga sumusunod na paksa:

- karaniwang mga banta sa seguridad sa cyber tulad ng kompromiso sa email ng negosyo at ransomware
- mga hakbang sa proteksyon kabilang ang mga malalakas na password o passphrase, MFA at mga update sa software
- paano matutukoy ang mga scam at pag-atakeng phishing
- mga patakarang partikular sa negosyo (halimbawa, mga proseso para sa pag-uulat ng mga kahina-hinalang email o para sa pagpapatunay ng mga invoice bago magbayad)
- ang gagawin sa isang emerhensya.

Ang website ng ACSC ay may mga mapagkukunan para sa karamihan ng mga paksang ganito sa cyber.gov.au/learn. Maaari mong isaalang-alang ang iba pang mga paraan ng pagtuturo sa iyong mga empleyado, halimbawa sa isang pormal na kurso o panloob na pagsasanay. Ano man ang iyong pasya, tandaan na ang pagsasanay sa seguridad sa cyber ay hindi isang beses lamang at dapat itong i-refresh nang pana-panahon.

✓ **Pag-isipan kung paano ituturo sa iyong negosyo ang kaalaman sa seguridad sa cyber.**

Gumawa ng planong pang-emerhensya

Maaaring mabawasan ng isang planong pang-emerhensya ang epekto ng isang pag atake sa cyber sa inyong negosyo.

Kapag tumutugon sa isang insidente ng seguridad sa cyber, bawat minuto ay mahalaga. Ang pagkakaroon ng planong pang-emerhensya ay nangangahulugan na ang iyong mga kawani ay gugugol ng mas kaunting oras sa pag-iisip kung ano ang gagawin at mas maraming oras sa pagkilos.

Isaalang-alang ang mga sumusunod na tanong kapag gumagawa ng iyong planong pang-emerhensya:

- Ano ang proseso sa pag-uulat ng mga potensyal na insidente ng seguridad sa cyber para sa iyong mga kawani?
- Kanino ka nakikipag-ugnayan para sa tulong? Halimbawa, ang mga propesyonal sa IT at sa iyong bangko.
- Paano ipapaalam ang insidente sa iyong mga kawani, stakeholder, o mga customer?
- Paano mo pamamahalaan ang negosyo gaya ng dati, kung offline ang anumang mga kritikal na sistema?

Tiyaking pamilyar ang iyong mga kawani sa planong pang-emerhensiya, kabilang ang anumang mga tungkulin o responsibilidad nila. Panatilihin ang isang hard copy ng plano kung sakaling offline ang iyong mga sistema kapag kailangan mo ito.

✓ **Gumawa ng planong pang-emerhensiya para sa mga insidente ng seguridad sa cyber.**

Manatiling may kaalaman

Maging kasosyo sa ACSC upang makatanggap ng pinakabagong impormasyon mula sa ACSC.

Sa pamamagitan ng pagiging kasosyo sa ACSC, manatiling may alam tungkol sa mga pinakabagong banta at kahinaan sa cyber. Ang serbisyong ito ay magpapadala sa iyo ng buwanang mga newsletter at alerto kapag may natukoy na bagong banta sa cyber.

Ang seguridad sa cyber ay isang mabilis na nagbabagong larangan. Aktibong sinasamantala ng mga cybercriminal ang mga kahinaan sa loob ng ilang minuto ng kanilang pagtuklas. Ang pananatiling may kaalaman tungkol sa seguridad sa cyber ay makakatulong sa iyong negosyo na maunawaan ang mga banta na malamang na kakaharapin nito at kung paano mapoprotektahan laban sa mga ito.

✓ **Irehistro ang iyong negosyo sa ACSC Partnership Program.**

Pagtatatwa

Ang materyal sa gabay na ito ay pangkalahatan lamang at hindi dapat ituring bilang isang legal na payo o hindi dapat sumalalay dito para sa tulong sa anumang partikular na pangyayari o emerhensyang sitwasyon. 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-ulat ng insidente ng seguridad sa cyber, makipag-ugnayan sa amin:

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

Ang numerong ito ay magagamit lamang sa loob ng Australia.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre