Pag-iwas sa Cybercrime

Ang internet ay isang mahusay na paraan upang kumonekta online, ngunit maaari din itong maging mapanganib. Katulad ng kapag naghahanda kang umalis sa iyong bahay, dapat kang mag-ingat bago gumamit ng internet upang matiyak na ikaw at ang iyong impormasyon ay ligtas upang hindi ka maging biktima ng cybercrime.

Pano Maging Ligtas sa Internet

Ano ang Cybercrime?

Ang mga cybercrime ay mga krimen na nangyayari sa mga tao sa internet. Nangyayari ang mga ito kapag ang personal na impormasyon ng isang tao o ang kanilang pera ay ninakaw. Maraming tao ang hindi nakakaalam kung nangyayari ang cybercrime sa kanila, kaya mahalagang malaman kung paano matutukoy ang mga cybercrime para maiwasan ito o makakuha ng tulong at pigilan ang mga ito na mangyaring muli.

Ang Internet ay isang Pampublikong Espasyo

- Nakikita ng mga tao kung anong website ang pinupuntahan mo at, kung minsan, kung anong impormasyon ang itina-type mo.
- Anumang impormasyong ibinabahagi mo sa internet ay maaaring makita ng ibang tao.
- Maging maingat sa pagbabahagi ng iyong personal na impormasyon (tulad ng mga social security number, impormasyon ng bank account, at medikal na impormasyon) sa internet kapag hindi ito para sa tamang dahilan ng negosyo, tulad ng pagbabangko.
- Ang mga pampublikong Wi-Fi network sa mga tindahan at restawran na nagbibigay-daan sa iyong gamitin ito nang libre ay dapat palaging gamitin nang may pag-iingat.
- Bagama't maginhawa ang paggamit ng pampublikong Wi-Fi, madalas itong walang seguridad. Nangangahulugan ito na ang iyong personal na impormasyon (tulad ng username at password sa iyong bank account, halimbawa), ay maaaring makita o manakaw ng ibang tao.

Regular na Suriin ang Mga Setting sa Pagkapribado

- Pinahihintulutan ng setting sa pagkapribado na piliin kung anong impormasyon ang gusto mong ibahagi at kung sino ang makakakita sa iyong impormasyon.
  - Sa social media (tulad ng Facebook o Instagram), maaari mong gamitin ang mga setting sa pagkapribado upang kontrolin kung anong impormasyon ang ibinabahagi sa iba.
- Magtakda ng mga setting sa pagkapribado para sa iba't ibang mga application sa iyong cellphone upang limitahan kung ano ang ibabahagi sa mga application (tulad ng pagbabahagi ng iyong lokasyon o mga pahintulot sa data).
- Siguraduhin na mangangailangan ng password ang mga setting sa pagkapribado sa iyong mga online na account bago i-access ang iyong mga account.
  - Ang Two Factor Authentication ay kapag nakatanggap ka ng text, tawag, o email na may espesyal na code sa tuwing mag-log in ka sa iyong account online (tulad ng bangko o kumpanya ng credit card). Nakakatulong itong matiyak na ikaw talaga ang nagla-log in sa iyong account.
  - Magandang ideya na mag-set up ng Two Factor Authentication para sa mga online na account.

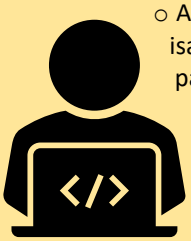
Ang mga Bulletin sa Kagalingan at Kaligtasan ay ginagawa ng Kagawaran ng mga Serbisyo sa Pag-unlad upang alertuhan ang mga indibidwal, pamilya, at iba pa tungkol sa mga partikular na peligrong natukoy sa ating komunidad. Mangyaring magbigay ng feedback tungkol sa bulletin na ito at kung ano ang magagawa namin nang mas mabuti sa pamamagitan ng survey na ito: Survey sa Bulletin

Gumamit ng Mga Malakas na Password para sa Mga Online na Account

- Gawing matibay ang iyong password at tandaan na regular itong palitan. Poprotektahan nito ang iyong mga online na account.
- Ang isang malakas na password ay may hindi bababa sa 8 character, at may kasamang kumbinasyon ng mga upper at lowercase na letra, simbolo, at numero. Kung mas mahaba ang password, mas ligtas ito.
    - **Mga halimbawa ng mahinang password**: password, IyongPangalan, 12345
    - **Mga halimbawa ng mga ligtas na password**: 8blu3Car$dr1vinG, 1&n%00Xb#, Y3!!oWfL0w3rs
- Iwasan ang mga password na madaling hulaan, tulad ng iyong petsa ng kapanganakan o pangalan.
- Ang bawat isa sa iyong mga account ay dapat magkaroon ng sarili nitong natatanging password.
- Huwag maglagay ng listahan ng mga password sa isang papel na nakakalat lang, lalo na malapit sa iyong computer.
- Ang mga password ay dapat lamang ibahagi sa mga taong kilala at pinagkakatiwalaan mo at dapat na itago sa isang ligtas na lugar.

Mag-ingat sa Mga Virus at Malware

- Ang ***Malware*** ay isang uri ng software na nakakapinsala sa iyong computer. Ang ***mga Virus*** ay isang uri ng malware.
    - Ang mga virus at malware ay pumapasok sa isang computer system nang walang pahintulot mo at "ini-infect" ito.
    - Maaaring nakawin ng mga virus at malware ang iyong impormasyon, pabagalin at i-crash ang iyong computer, o ganap na kontrolin ang iyong computer.



- Ang mga virus at malware ay pumapasok sa iyong computer kapag nag-click ka sa isang link o nagbukas ng isang email na nahawaan ng mga ito.
    - Mag-ingat bago mag-click sa isang link na nag-aalok sa iyo ng premyo o isang bagay nang libre.
    - Ang mga ito ay maaaring magmukhang mga laro, screen saver, o pag-download ngunit maaaring malware o mga virus.

Mag-isip Bago Mo I-click

- Bigyang-pansin ang mga nagpapadala ng mga email at mensaheng natatanggap mo online.
    - Tingnan ang kanilang email address upang makita kung tumutugma ito sa address nila na nasa iyo.

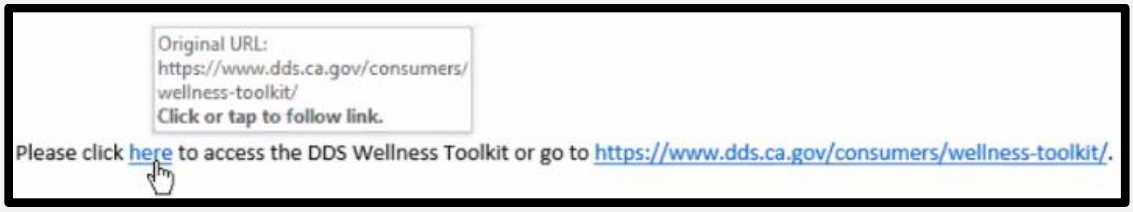
- Lalong mag-ingat kung ang nagpadala sa iyo ay nagmamadaling sumagot kaagad o ginagawang tila may krisis, tulad ng problema sa iyong bank account. Ang mga ganitong uri ng mensahe ay malamang na isang scam.
- Ang phishing ay isang internet scam na nanlilinlang sa mga tao na ibahagi ang kanilang personal na impormasyon sa pamamagitan ng paggamit ng mga pekeng mensahe na mukhang totoo.
    - Bago tumugon sa mga mensahe, tingnan kung may hindi pamilyar na sender o nagpadala, mga pagkakamali sa pagbabaybay o gramatika, mga link na hindi tumutugma sa nilalaman ng mensahe, mga random na attachment, at isang kahilingan sa iyo na kumilos nang mabilis.

- Huwag magbukas ng mga attachment o mag-click sa mga link na hindi mo nakikilala. Ang mga ito ay maaaring peke at humantong sa mga virus na naka-install na maaaring makapinsala sa iyong computer o telepono o magnakaw ng higit pang impormasyon mula sa iyo.
    - Kapag nakatanggap ka ng hindi inaasahang email na may mga link o attachment, palaging tanungin ang nagpadala (sa pamamagitan ng telepono o text) upang matiyak na sila ang nagpadala nito.
- Ang IRS ay magpapadala lamang sa iyo ng mga abiso sa pamamagitan ng U.S. mail. Huwag tumugon sa mga tawag, email o text message na nagsasabing sila ay mula sa IRS.

Ang mga Bulletin sa Kagalingan at Kaligtasan ay ginagawa ng Kagawaran ng mga Serbisyo sa Pag-unlad upang alertuhan ang mga indibidwal, pamilya, at iba pa tungkol sa mga partikular na peligrong natukoy sa ating komunidad. Mangyaring magbigay ng feedback tungkol sa bulletin na ito at kung ano ang magagawa namin nang mas mabuti sa pamamagitan ng survey na ito: Survey sa Bulletin

Alamin Kung Sino ang Iyong Pinapadalhan ng Email o Text

- Tandaan na ang mga taong nasa online ay maaaring hindi sila gaya ng sinasabi nila.
- Huwag kailanman magbahagi ng personal na impormasyon o magpadala ng mga larawan ng iyong sarili sa isang estranghero o isang taong hindi mo pa nakikita nang personal.
- Huwag magpadala ng pera sa isang tao na kamakailan mo lang nakilala o hindi pa nakilala nang personal.
- Bago mo ibigay ang iyong social security number o anumang account number sa isang online na form o website, siguraduhing ang humihingi ng impormasyon ay sila mismo gaya ng sinasabi nila.
    - Suriin ang email address ng nagpadala sa pamamagitan ng paggalaw ng cursor papunta sa kanilang pangalan o sa link upang matiyak na papunta ito sa tamang negosyo.



- Nakokopya ng mga tao ang mga logo at kayang gawing mukhang totoo ang mga email, kaya tingnang mabuti ang mga ito para sa mga maling pagbabaybay, kakaibang nilalaman, o malabong mga larawan.
- Kung hindi ka sigurado kung totoo ang nagpadala, makipag-ugnayan sa kumpanya o organisasyon mula sa iyong online account o direktang tawagan sila.

Ano ang Gagawin kung Naging Biktima Ka ng Cybercrime

- Sabihin kaagad sa isang taong pinagkakatiwalaan mo.
- Kung ang krimen ay may kinalaman sa pag-access sa iyong mga personal na account, tawagan ang iyong bangko o kumpanya ng credit card at ipaalam sa kanila ang tamang paraan. Itigil ang paggamit ng alinman sa mga debit o credit card para sa mga account na na-access na.
- Baguhin ang iyong password sa anumang account o login na naatake na.
- Bantayan ang iyong mga account para sa mga hindi pangkaraniwang aktibidad.

Ang mga Bulletin sa Kagalingan at Kaligtasan ay ginagawa ng Kagawaran ng mga Serbisyo sa Pag-unlad upang alertuhan ang mga indibidwal, pamilya, at iba pa tungkol sa mga partikular na peligrong natukoy sa ating komunidad. Mangyaring magbigay ng feedback tungkol sa bulletin na ito at kung ano ang magagawa namin nang mas mabuti sa pamamagitan ng survey na ito: Survey sa Bulletin