Pag-iwas sa Cybercrime

Ang cybercrime ay isang seryoso at lumalaking isyu para sa mga gumagamit ng internet. Bagama't maganda ang pananatiling konektado online, may mga bagay na dapat malaman tungkol sa ligtas na paggamit ng internet. Tinatarget ng mga cybercriminal ang mga taong pinaniniwalaan nilang mahina, kabilang ang mga taong may mga Kapansanang Intelektwal at/o Kapansanan sa Pag-unlad. Dapat malaman ng lahat ang mga panganib ng cybercrime at kung paano manatiling ligtas habang nagba-browse sa internet.

Ano ang Cybercrime?

Ang mga cybercrime ay mga krimen na ginagawa sa internet gamit ang mga mobile device (tulad ng cellphone), computer, at pampublikong internet Wi-Fi network. Ang mga cybercriminal ay nagnanakaw ng sensitibo o personal na impormasyon para sa pinansyal na kita.

Ang mga indibidwal ay tinatarget sa pamamagitan ng iba't ibang mga diskarte upang palihim na mangalap ng personal na impormasyon. Maraming tao ang nagiging biktima ng mga cybercrime nang hindi nalalaman na kadalasang nagreresulta sa pagkawala ng pananalapi (pagnanakaw), mga paglabag sa personal na data, at pagnanakaw ng pagkakakilanlan ng biktima. Ang pag-alam kung paano maiwasan at humingi ng tulong matapos ng mga cybercrime ay mas mahalaga higit kailanman.

Ang mga cybercriminal ay mga oportunista at naghahanap ng mga mahihinang populasyon upang mabiktima. Sa mga indibidwal na may IDD, maaaring kilala ng mga kriminal ang kanilang biktima o gawing malapit sa kanila ang mga ito bilang isang kakilala o mapagkakatiwalaang tao.

Mga Karaniwang Uri ng Cybercrime

Phishing: Paggamit ng email, mga text message, at mga tawag sa telepono upang maihayag ng mga biktima ang personal o pinansyal na impormasyon, at/o mga kredensyal sa pag-log in.

Hindi Pinadala: Paggamit ng internet upang iligal na humingi ng elektronikong pagbabayad para sa pagbili ng mga bagay at serbisyo na hindi kailanman natatanggap.

Pangingikil: Pagkuha ng pera o mga kalakal sa pamamagitan ng pananakot o pagbabanta mula sa isang taong nagpapanggap na mula sa isang awtoridad (tulad ng IRS). Maaaring kabilang dito ang mga banta ng pisikal na pananakit, kriminal na pag-uusig, o pagkakalantad sa publiko. Maaaring kabilang din dito ang pag-lock ng access sa data ng biktima at paghawak nito para sa ransom.

Paglabag sa Personal na Data: Pagnanakaw at pagbabahagi ng pribadong personal na impormasyon at data ng isang indibidwal sa isang hindi awtorisadong user.

Pagnanakaw ng Pagkakakilanlan: Pagnanakaw at paggamit ng personal na impormasyon ng ibang indibidwal upang makagawa ng panloloko o iba pang krimen.

Ang Bulletin sa Kagalingan at Kaligtasan ay ginawa ng Kagawaran ng mga Serbisyo sa Pag-unlad upang alertuhan ang mga direktang tagapagkaloob ng serbisyo, mga regional center, at iba pa sa mga particular na peligro na 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

Cybercrime sa U.S. noong 2020

- Sa panahon ng pandemya ng COVID, ang mga indibidwal na may IDD ay biktima ng mga cybercriminal na naglihis ng pederal na stimulus money na ipinadala sa kanila sa elektronikong paraan.
- Ang California ang may pinakamataas na bilang ng mga reklamo sa cybercrime sa bansa.
- Nakatanggap ang FBI ng halos 800,000 reklamo sa cybercrime mula sa publiko, isang **69% na pagtaas** kumpara noong nakaraang taon.
- Ang phishing ay ang pinakakaraniwang cyberattack na may higit sa **241,000** na naiulat na mga biktima.
- Lumampas ang naiulat na pagkalugi sa **$4.1 bilyon**.
- Ang mga indibidwal na higit sa edad na 60 ang pinakanabiktima sa anumang grupo ng edad.

Tulungang Protektahan ang Mga Indibidwal na Pinaglilingkuran Mo mula sa Cybercrime

Ang internet ay isang pampublikong espasyo

Paalalahanan ang mga indibidwal na maging maingat bago magbahagi ng personal na impormasyon, tulad ng mga social security number, impormasyon sa bank account, at medikal na impormasyon sa internet.

- **Dapat palaging gamitin nang may pag-iingat ang mga pampublikong Wi-Fi network.**
- Ang mga pampublikong Wi-Fi network ay bukas sa sinuman kung nasa loob sila ng saklaw nito, at hindi karaniwang nangangailangan sa mga user na sumang-ayon sa anumang mga tuntunin o kondisyon bago sumali.
- Bagama't maginhawa ang paggamit ng pampublikong Wi-Fi, madalas itong walang seguridad. Nangangahulugan ito na ang personal na impormasyon (tulad ng username at password), ay maaaring elektronikong matingnan ng ibang tao nang hindi nalalaman ng biktima.
- Ang mga ligtas na Wi-Fi network ay kadalasang nangangailangan ng password ng user at maaaring mangailangan ng bayad o pagbili para magamit.

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

Tulungan ang mga indibidwal na iyong pinaglilingkuran na lumikha ng mga malalakas na password.

- Hikayatin ang mga indibidwal na huwag gumamit ng mga karaniwang password o password na madaling mahulaan.
- 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.
  - **Mahihinang mga password**: “password”, ang iyong pangalan o kaarawan, 12345,
  - **Malakas na mga password**: 8blu3Car$dr1vinG, 1&n%00Xb#, Y3!!oWfL0w3rs

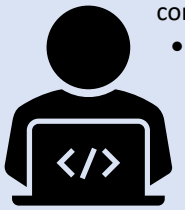
Regular na suriin ang mga setting sa pagkapribado

Tulungan ang mga indibidwal na iyong pinaglilingkuran na suriin ang mga setting sa pagkapribado sa kanilang mga mobile device at computer. Ipaliwanag kung paano mag-set up ng Two Factor Authentication sa pamamagitan ng pagsasaayos ng mga setting sa pagkapribado sa mga online na account. Ang Two Factor Authentication ay kapag pinapadalhan ang user ng text o email na may espesyal na code sa tuwing magla-log ang indibidwal sa kanilang online na account.

Ang Bulletin sa Kagalingan at Kaligtasan ay ginawa ng Kagawaran ng mga Serbisyo sa Pag-unlad upang alertuhan ang mga direktang tagapagkaloob ng serbisyo, mga regional center, at iba pa sa mga particular na peligro na 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

Mga Virus at Malware

- Ang ***Malware*** ay isang uri ng software na idinisenyo upang makapinsala sa isang mobile device o computer system.



  - Ang ***mga Virus*** ay mga computer code na pumapasok sa isang computer system nang walang pahintulot at "ini-infect" ito. Nagtatago sila sa mga file o application na ipinadala sa pamamagitan ng email o text at ini-infect ang isang computer kapag binuksan ang mga ito. Ang mga virus ay isang uri ng malware.
- Ang mga virus ay maaaring magnakaw ng impormasyon ng user, magpabagal at magpa-crash sa computer, o ganap na kontrolin ang isang computer o device.
- Ang mga virus ay hindi maaaring kumalat mag-isa. Kumakalat sila kapag hindi nila namamalayan ng mga tao na ibinabahagi nila ang mga ito. Ito ay karaniwang nangyayari sa pamamagitan ng pagbabahagi ng mga nahawaang file o email.

Ano ang gagawin Pagkatapos Maging Biktima ng Cybercrime

Ipaliwanag ang kahalagahan ng pagtawag sa kanilang bangko at pagkansela ng kanilang mga debit o credit card na ginamit sa cyberattack. Tumulong sa pagbabago ng impormasyon sa pag-log in para sa mga online na account. Alertuhan ang institusyon ng account na na-hack tungkol sa pag-atake at pagtatanong tungkol sa anumang naitalang mapanlokong pagsingil.

Ang DDS Wellness Toolkit ay may higit pang impormasyon tungkol sa kung paano makakatulong na suportahan at protektahan ang mga indibidwal na iyong pinaglilingkuran.

Nakatutulong na Mapagkukunan

Lokal na Tagapagpatupad ng Batas

Internet Crime Complaint Center (IC3)

Federal Trade Commission (FTC)

- I-report ang pandaraya sa ReportFraud.ftc.gov
- Tawagan ang FTC hotline sa1-877-IDTHEFT (1-877-438-4338)
- I-report ang pagnanakaw ng pagkakakilanlan at maghanap ng higit pang impormasyon sa identitytheft.gov

Mag-isip Bago mo I-click

- Pigilan ang mga indibidwal na pinaglilingkuran mo mula sa pagbubukas ng mga hindi hinihinging attachment o pag-click sa mga hindi nakikilalang link. Ang mga ito ay maaaring humantong sa mga virus o malware na maaaring makapinsala sa mga computer.
- Babalaan ang mga indibidwal na maging maingat bago mag-click sa mga link na mukhang mga laro o na nangangakong makakakuha ng isang bagay nang "libre" kung i-click nila ang link.
- Hikayatin ang mga indibidwal na suriin ang address ng mga email na kanilang natatanggap upang kumpirmahin na ang nagpadala ay lehitimo. Kung makatanggap sila ng hindi inaasahang email na may mga link o attachment, iminumungkahi na makipag-ugnayan sila sa nagpadala sa pamamagitan ng telepono o text upang kumpirmahin na ipinadala nila ang email.
- 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 sumagot sa anumang mga mensahe, magkaroon ng kamalayan sa mga palatandaan ng isang phishing scam: isang hindi pamilyar na nagpadala, mga pagkakamali sa pagbabaybay at gramatika, mga kahina-hinalang link na hindi tumutugma sa nilalaman ng mensahe, mga random na attachment, nilalaman ng email na humihingi ng agarang pagkilos.

Bago Sumagot o Mag-click sa isang Email

Hikayatin ang mga konsumidor na beripikahin kung sino ang nagpapadala sa kanila ng mga email.

- 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.

Ang Bulletin sa Kagalingan at Kaligtasan ay ginawa ng Kagawaran ng mga Serbisyo sa Pag-unlad upang alertuhan ang mga direktang tagapagkaloob ng serbisyo, mga regional center, at iba pa sa mga particular na peligro na 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