

Cybersecurity, Phishing, at Spam

Malalaman ng mga kalahok ang tungkol sa mga mapanirang user sa online na maaaring sumubok na gamitin ang mga kahinaan ng seguridad para kumuha ng impormasyon tungkol sa kanila. Mailalarawan ng mga kalahok ang mga panganib ng pagiging online, gumawa ng mga istratehiya para sumali sa mas ligtas na mga gawi, kilalanin ang mga message na spam, at ipaliwanag kung sino ang dapat humingi ng kanilang password.

Mga Material

Spam Handout

Mga Panganib sa Online

Part One

Sabihin sa Iyong Mga Estudyante

Kapag ginagamit mo ang Internet, maaaring mong malantad ang iyong sarili sa mga panganib sa pamamagitan ng pag-access ng web page, pakikipag-ugnayan sa online, pag-download ng data. Minsan posible para sa mga website na ina-access mo, mga taong nasa parehong network, o kahit mga third party na malaman ang iyong lokasyon o iba pang impormasyon tungkol sa iyo kapag nagba-browse ka.

Tanungin ang Iyong Mga Estudyante

Sino ang maaaring samantalahin ang mga kahinaan ng seguridad sa online para makita ang iyong personal na impormasyon?

1. Ang mga posibleng sagot kasama ang mga mapanirang hacker, pagbabantay ng pamahalaan, atbp.

Sabihin sa Iyong Mga Estudyante

Kapag nagba-browse ka sa web, posibleng ito para sa mga mapanirang hacker na kumuha ng data sa iyo sa parehong ginagawa ng mga Internet provider. Upang bawasan ang panganib na ito, dapat mong i-secure ang koneksyon sa pagitan mo at (mga) website na sinusubukan mong i-access. Anuman ang iyong koneksyon, sinusubukan ng maraming website na subaybayan ang iyong mga pattern ng paggamit sa maraming platform. Maaari nilang bantayan ang iyong browser lokasyon, at iba pang mga patter ng paggamit para malaman kung sino ka.

Tanungin ang Iyong Mga Estudyante

Bakit maaaring subukang ma-access ng mga mapanirang hacker ang iyong impormasyon sa online? Anong impormasyon ang hinahanap ng mga tao? Bakit gustong subaybayan kung sino ka ng isang website na hindi ka naka-log in.

1. Ang anumang impormasyon na personal na kumikilala at anumang impormasyon na maaaring ibenta o gamitin para kumita ng pera.

Mayroon bang may alam kung ano ang malware? Ano ang magagawa nito?

Sabihin sa Iyong Mga Estudyante

Ang malware ay isang nakakapinsalang code na sikretong tumatakbo sa iyong

computer. Maaaring kumuha ng data ang ilang malware mula sa anumang bahagi ng iyong lokal na computer, mula sa iyong hard drive papunta sa iyong browser data. Maaari rin nitong pahintulutan ang mga hacker na kontrolin ang iyong computer at gamitin ito sa anumang paraan na gusto nila. Karamihan sa malware ay mas simple, tulad ng mga website na nanggagaya ng mga secure na portal katulad ng bangko o mga extension na naglalagay ng mga advertisement sa iyong browser para kumita ng pera.

Tanungin ang Iyong Mga Estudyante

Ano ang maaari mong gawin para protektahan ang iyong sarili laban sa malware, pag-iispiya o pagsubaybay?

Sabihin sa Iyong Mga Estudyante

Mag-ingat kapag nagkli-click ng mga link, ad, o mga post sa social media. Tumutugma ba ang URL na inaasahan mo? Nakukuha mo ba ang parehong page kapag tina-type muli ito o naghahanap ng website? Ang isang magandang tuntunin ay dapat protektahan ng SSL/TLS ang anumang pag-log in sa page para sa mahalagang account (katulad ng Google, Facebook, Twitter, o mga bank account). Ginagawang mahirap ng SSL/TLS para sa hacker sa parehong network para padalhan ka ng hindi totoong website kung magta-type ka sa tamang URL, na maaaring napakasimple.

Makakapagpatakbo ng code ang ilang website para ma-access ang iyong personal na impormasyon o mga online na account kung gumagawa ng pagkakamali sa pag-code ang mga platform na iyon. Maaari nilang gamitin ang iyong mga account para i-spam ang iba.

I-download o i-install lang ang software mula sa pinagkakatiwalaang pinagmulan at isipin kapag nagda-download ka ng mga executable (.exe, .pkg, .sh, .dll, o .dmg extension). Ang mga executable ay anumang na magsasagawa ng aksyon. Minsan, maaaring hindi magandang aksyon ang mga ito. Halimbawa, maaaring sumulat ang isang tao ng executable text para burahin ang hard drive ng isang tao o mag-install na hindi totoong browser. Ito ay kung bakit dapat mo lang i-install ang nilalaman mula sa mga pinagkakatiwalaang pinagmulan.

Maaari kang gumamit ng anti-virus software para pigilan ka mula sa pagpapatakbo ng malware. Kasama sa iyong computer ang ilang anti-virus software (hal., Microsoft Security Essentials para sa Windows); habang ang ilang operating system, katulad ng mga nasa mga Apple computer, ay mayroong mga setting ng seguridad na nagba-block sa software na ma-install mula sa mga hindi pinagkakatiwalaang pinagmulan. Maingat mag-isip bago mag-override sa mga setting na ito.

Maaari mo ring isaalang-alang ang mga browser extension na maaaring, halimbawa, i-block ang mga plug-in na ginagawang mas mahirap para sa mga website na malaman kung sino ka o subaybayan ka. Ang parehong plug-in, gayunpanman, ay

maaaring i-block ang functionality ng mga website, tulad ng kakayahang manood ng mga video. Magdedesisyon ka man na i-install o hindi ang mga browser extension na humahantong sa iyong mga pagpipiliin at kompromiso na handa mong gawin pagdating sa online na seguridad. Maaari mong isaalang-alang ang mga tanong tulad ng, Gaano hindi kumbinyente para sa akin ang masubaybayan? Gaano kahalaga ang aking privacy? Gaano ko gustong panoorin ang bahagi ng nilalaman na ito (kung halimbawa, kung i-block ng browser extension ang isang plug-in na nagbibigay ng video)?

Mga Tool para sa Seguridad

Part One

Pakikipag-ugnayan Ng Klase:

Pakitandaan: Bahagi ng nilalaman ng aktibidad ay natalakay sa “Aktibidad#1: Mga Panganib sa Online.” Tinatanggap anmin ang iyong pagpapasiya tungkol sa kung gusto mo o hindi tignan muli ang material na ito kung sumali ka na sa Aktibidad#1, o laktawan ito.

Tanungin ang Iyong Mga Estudyante

Alam mo ba kung secure ka kapag ginagamit mo ang Internet?

Sabihin sa Iyong Mga Estudyante

Nang hindi ginagamit ang mga tamang pag-iingat, mahirap ito, kung hindi maaari, para matagumpay na protektahan ang iyong sarili laban sa mga panganib sa online na mga ito [Ang mga inilarawan sa dating sekyon.]

Lumalabas sa lahat ng oras ang hindi inaasahang mga bagong panganib sa online, kaya mahalagang manatiling alerto.

Tanungin ang Iyong Mga Estudyante

Ano ang maaaring gawin ng isang tao kung kumbinsihin ka na ang kanilang website ay talagang mahalagang website?

Mayroong mga tool na maaari mong gamitin para iwasan o bawasan ang mga panganib na ito. Mayroon bang may alam nang ganito?

Sabihin sa Iyong Mga Estudyante

Ang HTTPS ay karaniwang ginagamit ng mga website para i-encrypt ang data na ipinapadala sa Internet. Maaaring pigilan ng pag-encrypt ang alinmang third party sa madaling pagtingin ng data mula sa iyong koneksyon. Nagbibigay ito ng dagdag na seguridad at maaaring gamitin sa alinmang browser sa pamamagitan ng pagdagdag ng “https://” sa unahan ng URL na ginagamit mo (hal., <https://www.mysite.com>). Gayunpaman, hindi lahat ng website ay sinusuportahan ang HTTPS.

1. Dapat ilagay mo lang ang sensitibong impormasyon (hal., mga password, impormasyon ng credit card) sa mga web page na may HTTPS:// na prefix.
2. Maaari kang gumamit ng mga tool ng software para tiyakin na palaging kang gumagamit ng HTTPS kung kailan maaari.

3. Karamihan ng browser ay mayroong palatandaan ng seguridad na mukhang mga kandado malapit sa address bar para ipakita ang mga HTTPS na koneksyon.
4. Sa kasamaang-palad, hindi ginagarantiya ng HTTPS na ligtas ka habang ang ilang mapanirang website ay maaari ring suportahan ang HTTPS. Sini-secure ng HTTPS ang koneksyon ngunit hindi tinitiyak na isang magandang actor ang website.

Ang Secure Sockets Layer (SSL)/Transport Layer Security (TLS) ay ang mga pangalan para sa teknolohiya na pinapanatiling secure ang HTTPS. Gumagamit ang SSL/TLS ng mga digital na key sa pag-encrypt, na gumagana na katulad ng mga tunay key. Kung sumulat ng isang sikreto sa isang pirasong papel para sa iyong kaibigan, kung sinuman ang makakita ng papel ay maaaring makita ang iyong sikreto. Sa halip, isipin na binigyan mo sila ng kopya ng key nang personal, at pagkatapos ipinadala ang iyong mga sikreto sa mga magkakatatugmang naka-lock na kahon. Kung mayroong humarang sa kahon, mahihirapan sila makita ang iyong sikreto nang walang key. Kung mayroong sumubok na palitan ang kahon na kapareho, mapapansin mo na hindi gagana ang iyong key. Gumagana ang SSL/TLS sa parehong paraan, ngunit may website.

Ang mga indicator ng seguridad ng Browser ay sasabihin rin ang impormasyon ng Extended Validation (EV). Ang mga EV na certificate ay ibinibigay sa mga website na bini-verify ang kanilang pagkakakilanlan sa may awtoridad sa certificate. Sa mga browser, minsan kinukuha ng EV indicator ang form ng pangalan ng site o nagpaparehistrong entidad kasunod ng address bar. Ang mga EV na certificate ay ibinibigay sa mga website na bini-verify ang kanilang pagkakakilanlan sa may awtoridad sa certificate. Sa mga browser, minsan pinapalitan ng EV indicator ang pangalan ng site o ang nagrerehistrong entity sa tabi ng address bar. Kung naghihinala ka sa nilalaman ng partikular na website, maaari mong tignan para makitang tumutugma ang URL sa certificate sa browser sa pamamagitan ng pag-click sa “Tignan ang Certificate.” [Maaaring makatulong, sa projection screen, para ipakita sa mga kalahok kung paano hanpin ang “Tignan ang Certificate.” Paano ka mag-navigate sa mga ito ay iba-iba ayon sa browser. Halimbawa, sa Chrome, sa ilalim ng “Tignan,” i-click ang “Developer” at pagkatapos “Mga Tool ng Developer.” Mula sa “Mga Tool ng Developer” i-click ang tab ng “Seguridad”, pagkakatapos “Tignan ang Certificate.”

Maliban sa hindi pagpapatakbo ng software mula sa hindi pinagkakatiwalaang pinagmulan, maaaring pigilan ka ng mga anti-virus software sa pagbisita sa mga hindi pinagkakatiwalaang page at pag-download ng malware.

Karaniwang lumalabas ang “phishing” sa email mula sa spammer na nagkukunwaring isang lehitimong party. Pagkatapos hihingiin ang iyong password, na inaasahan nilang ipapadala sa email o ilalagay sa isang hindi tunay na website.

Maaring pigilan ng mga filter para sa spam ang ilan sa mga email na ito mula sa paglabas sa iyong inbox. Para gawin mas maganda ang mga filter para sa spam, tiyakin na markahan ang anumang mga kahina-hinalang email na napupunta sa iyong inbox bilang spam.

Tanungin ang Iyong Mga Estudyante

Anong mga aksyon an magagawa mo para pigilan ang iyong sarili mula sa hindi sinasadyang pag-download ng mga file na nakakapinsala sa iyong computer?

Sabihin sa Iyong Mga Estudyante

Palaging mo tignan muli na ini-access mo ang download mula sa mga mapagkakatiwalaang website. Labis na maging maingat sa pagbubukas ng mga email attachment na hindi kilala at pag-click sa mga pop-up window at mga mensahe ng error. Maaaring isaalang-alang mo rin ang pag-install ng reputable na anti-malware na mga programa sa iyong computer.

Pagbabahagi ng Mga Password

Part One

Tanungin ang Iyong Mga Estudyante

Sa tingin mo kailan okay na ibahagi ang iyong password?

1. Mga posibleng sagot kasama ang mga ibinahaging account (hal., Netflix).

Anong mga panganib ang maaaring may kaugnayan sa pagbabahagi ng iyong password?

1. Kung makuha ang iyong password ng isang mapanirang tao, maaaring na-hack ang iyong account. Ang pagbabahagi ng iyong password ay mas malamang na magkaroon ng access ang isang tao. Kung ginagamit ang parehong password sa iba pang mga website, maaaring ma-access din nila ang mga ito.

Sabihin sa Iyong Mga Estudyante

Karaniwang kasanayan na hindi mo dapat ibahagi ang mga sa sinuman maliban na hinihingi ito ng application para mag-log in. Gaya nang unang inilarawan, ang phishing ay ang gawaing dayain ang isang tao sa pagbabahagi ng kanilang password.

Gayunpaman, maaaring tahasang hilingin ng ilang tao ang iyong password upang ma-access ang iyong mga account, kini-claim na maaaring nasa panganib ang iyong account. Habang ang ilang tao ay mayroon mga magandang intensyon, katulad ng kaibigan na gusto tulungan kang na tumingin sa iyong account na nakakalito sa iyo, hindi mabuting ibahagi ang iyong password, lalo na kung ginagamit mo ang password na iyon para sa maraming account. Kung plano mong ibahagi ang password, siguruhing hindi ito gagamitin kahit saan at gumamit ng password manager para ibahagi ang access.

Minsan, ang mga taong humihingi sa iyo ng iyong mga password ay maaaring mga nasa hustong gulang na kilala at pinagkakatiwalaan mo, katulad ng mga magulang, guro, o employer. Kahit na kilala at pinagkakatiwalaan mo ang mga nasa hustong na ito, karaniwan positibong karanasan ito para sa lahat (sa iyo at sa kanila) na magkaroon ng pag-uusap tungkol sa kung bakit hinihiling nila ang request na ito at paano nila pangangasiwaan ang iyong mga password. Lalo na sa mga nasa hustong gulang na wala sa iyong pamilya, mabuting ideya na tanungin ang mga ito nang direkta kung mayroong batas o iba pang uri ng tuntunin na pinaniniwalaan nila na kinakailangan ibigay mo sa mga ito ang iyong mga password.

Ang magalang at malinaw na mga pagtanong tungkol sa mga batas at tuntunin ay

lalo nang mahalaga kapag ang request ng password ay nagmumula sa isang nasa hustong gulang na wala sa iyong pamilya na hindi mo personal na kilala, katulad ng opsiyal na nagpapatupad ng batas. Kung hihingian ka ng isang pulis o iba pang opsiyal ng pamahalaan para sa iyong mga password sa social media, manatiling kalmado at maging magalang. Tanungin kung bakit ginagawa ang request na ito at aling (mga) batas o (mga) tuntunin pinaniniwalaan nila na nagbibigay sa kanila ng karapatang magkaroon ng impormasyon mula sa iyo.

Depende sa mga pangyayari ng request ng isang magulang / tagapag-alaga, guro, employer, opsiyal ng nagpapatupad ng batas, opsiyal ng pamahalaan, o isa pang nasa hustong gulang, maaaring kailanganin mong ibigay sa kanila ang iyong mga password. Ang mga pangyayari na kakailanganin mong ibigay ang igyong mga password kabilang na mayroong ginagamit na batas o tuntunin na kinakailangang gawin mo o ang iyong pagpapasya na makikinabang ka mula sa kanilang tulong na mas mahalaga sa mga panganib ng pagbabahagi ng password.

Kung makakuha ng request mula sa isang nasa hustong gulang para sa iyong mga password, at ang request na iyon ay ginagawang hindi ka komportable sa anumang paraan, hanapin kaagad ang magulang / tagapag-alaga o ibang pinagkakatiwalaang nasa hustong gulang, sa posibleng paraan bago mo kailangang tumugon sa request.

Tanungin ang Iyong Mga Estudyante

Sa anong pangyayari dapat mong ibahagi ang iyong password sa online?

1. Kapag na-prompt ka lang para sa iyong password sa website na sinusubukang mong i-access. Kailanman huwag ibahagi ang iyong password saanman, kasama ang email, na karaniwan hindi naka-encrypt o secure.

Takdang Aralin

Handout

Assignment

Hatiin ang mga kalahok sa grupo ng 2-3. Ipamahagi ang Handout tungkol sa Spam ng Kalahok. Pagkatapos, sabihin sa bawat kalahok na gumawa ng isang flowchart para ipakita sa iba kung paano nilang makikilala ang spam at kung dapat nilang ibahagi ang partikular na impormasyon sa mga ilang indibidwal/grupo ng mga tao.

Sabihin sa Iyong Mga Estudyante

Basahin ang bawat mga sitwasyon at talakayin kung spam ang message at kung dagap mong ibahagi ang impormasyon sa tao o grupo ng mga tao na nasa sitwasyon.

Pakikipag-ugnayan Ng Klase:

Bigyan ng 10 minuto ang mga kalahok para gawing ito. Pagkatapos, hilingin sa mga grupo na ibahagi ang kanilang mga tugon.

Tanungin ang Iyong Mga Estudyante

Kailan mo dapat ibahagi ang iyong password sa email?

Sabihin sa Iyong Mga Estudyante

Karaniwang kasanayan para sa mga website at kumpanya na huwag kailanman hingiin ang iyong password sa email. Hindi mo dapat kailanman ipadala ang iyong password sa sinuman sa paraang ito, kahit kung mukhang lehitimo ang pinagmulan. Hindi halos kailanman secure ang email.

Part Two

Assignment

Sabihin sa mga kalahok bumalik sa kanilang mga grupo dahil ang sumusunod na pagsasanay ay para sa mga indibidwal na kalahok.

Bigyan ang mga kalahok ng 15 minuto para gawin ang kanilang mga flowchart.

Sabihin sa Iyong Mga Estudyante

Ngayon, sa isang papel, gumawa ng flowchart para ipakita sa mga indibidwal kung paano nilang makikilala ang spam at kung dapat nilang ibahagi ang ilang

impormasyon sa online sa iba. Maaaring nakakatulong ito para gumamit ng partikular na sitwasyon para ibatay ang iyong flowchart; alinman sa isa sa mga sitwasyong ipinapakita sa handout (kung pipiliin mong gawin, pakisulat ang bilang ng sitwasyon sa itaas ng iyong flowchart), o isang bagobase Kung pipiliin mong gawin ang iyong sariling sitwasyon, pakilarawan ito sa isang maikling talata sa itaas ng iyong flowchart.

Bigyan ang mga kalahok ng 15 minuto para gawin ang kanilang mga flowchart.