EFF'S SURVEILLANCE SELF-DEFENSE

JINSI YA: EPUKA MASHAMBULIZI YA PHISHING

https://ssd.eff.org/en/about-surveillance-self-defense

ELECTRONIC FRONTIER FOUNDATION

LOCALIZATION LAB

https://ssd.eff.org/en/module/how-avoid-phishing-attacks
Mara ya mwisho kuhariri: 9-6-2017

Kwa njia yako ya kuboresha usalama wako wa digiti, unaweza kukutana na watendaji wabaya ambao wanajaribu kudhoofisha malengo yako ya usalama. Tunawaita waasi wambaya hawa wasiofaa, au washambuliaji. Wakati mshambulizi anatuma barua pepe au kiungo ambacho kinaonekana kuwa na hatia, lakini kwa kweli ni mbaya zaidi kinachoitwa phishing.

Mashambulizi ya phishing kawaida huja kwa namna ya ujumbe uliotaka kukushawishi:

- Bonyeza kiungo
- Fungua hati;
- Weka programu kwenye kifaa chako; au
- ingiza jina lako la mtumiaji na nenosiri katika tovuti ambayo imefanywa ili kuonekana halali.

Mashambulizi ya phishing yanaweza kukudanganya kuacha nywila zako au kukudanganya katika kufunga programu zisizo kwenye kifaa chako. Washambuliaji wanaweza kutumia zisizo ili kudhibiti kifaa chako, kuiba habari, au kukupeleleza.

Mwongozo huu utakusaidia kutambua mashambulizi ya uwongo wakati unapowaona na kuelezea njia za vitendo za kusaidia kulinda dhidi yao.

Aina za mashambulizi ya Phishing

Phishing kwa nywila (pia hujulikana kama uvunjaji wa uwezeshaji)

weka jina lako la mtumiaji na Phishers inaweza kukudanganya katika kuwapa nywila zako kwa kukupeleka kiungo cha udanganyifu. Anwani za wavuti katika ujumbe zinaweza kuonekana kuwa na marudio moja, lakini uongoze mwingine. Kwenye kompyuta yako, unaweza kuona URL ya marudio kwa kurudi juu ya kiungo. Lakini viungo vinaweza kujificha zaidi kwa barua za kutazama, au kwa kutumia majina ya kikoa ambayo ni barua moja kutoka kwa majina ya kikoa halali na inaweza kukuelekeza kwenye ukurasa wa wavuti ambao unaonekana kwenda kwenye huduma unayoyotumia, kama vile Gmail au Dropbox. Hizi skrini za kuingia za kujiandikisha bandia mara nyingi zinaonekana hivyo halali kuwa ni zinajaribunenosiri. Ikiwa utafanya, utatuma maelezo yako ya kuingia kwa washambuliaji.

Kwa hiyo kabla ya kuandika nywila yoyote, angalia bar ya anwani ya kivinjari chako cha wavuti. Itaonyesha jina la kikoa halisi la ukurasa. Ikiwa hailingani na tovuti unayofikiri unakoingia, usiendelee! Kumbuka kuwa kuona alama ya ushirika kwenye ukurasa hakuthibitishi kuwa ni halisi. Mtu yeyote anaweza kuiga alama au kubuni kwenye ukurasa wao mwenyewe ili kujaribu na kukudanganya.

Baadhi ya wavuvi hutumia tovuti ambazo zinaonekana kama anwani za Mtandao maarufu kukupumbaza: https://wwwpaypal.com/ ni tofauti na https://www.paypal.com/ . Vile vile https://www.paypaI.com/ (na barua kuu "i" badala ya chini "L") ni tofauti na https://www.paypal.com/ . Watu wengi hutumia shorteners URL kufanya URL za muda mrefu rahisi kusoma au kuandika, lakini hizi zinaweza kutumiwa kufikia maeneo mabaya. Ikiwa unapokea URL iliyofupishwa kama kiunganishi cha t.co kutoka Twitter, jaribu kuiingiza kwenye https://www.checkshorturl.com/ ili uone mahali ambapo inakwenda.

Kumbuka, ni rahisi kuunda barua pepe ili waweze kuonyesha anwani ya uongo. Hii ina maana kwamba kuangalia anwani ya barua pepe inayoonekana ya mtumaji haitoshi kuthibitisha kuwa barua pepe imetumwa kwa mtu anayeonekana anapo.

Tambua phishing

Ushambuliaji mwingi wa phishing umesambaa kwenye mtandao. Mshambuliaji anatuma barua pepe kwa watu mamia au maelfu akidai kuwa na video ya kuvutia, taarifa muhimu au bili yenye mgogoro

Ila wakati mwingine mashambulizi ya phishing yanalenga wakati mwingine mshambuliaji anakuwa anamjua anayemshambulia. Hii inaitwa “spear Phishing”

Fikiri umepoke barua pepe kutoka kwa mjomba wako Boris inayosema kuna picha za watoto wake. Kwa kawaida Boris and watoto na inaonekana kama imetoka kwenye anuani yake, unafungua. Unapofungua barua pepe kuna faili limeambatanishwa.

Unapofungua barua pepe kuna faili la PDF limeambatanishwa, Hata linaweza kufungua picha za watoto wa Boris, ila kwa siri imeambatanishwa na programu yenye virusi kwenye mashine yako inaweza kutumika kukuchunguza. Mjomba Boris hakutuma yeye hiyo barua pepe, ila mtu mwingine anayekufahamu (na anazo picha za watoto wake) akufanya. Faili la PDF ambalo ulifungua kwa programu yako ya kusoma faili la PDF, Ila ametumia na kuweka programu na kutengeneza namba zake. Kwa kuongezea kukuonyesha PDF, pia kupakuliwa zisizo kwenye kompyuta yako. Vile zisizo vinaweza kupata anwani zako na kurekodi kile kamera na kipaza sauti ya kifaa chako vinavyoona na kusikia.

Njia bora ya kujilinda kutokana na mashambulizi ya harufu ni kamwe kubonyeza viungo au kufungua viambatisho vyovyote. Lakini ushauri huu ni wa kweli kwa watu wengi. Chini ni baadhi ya njia za kutetea dhidi ya uwongo.

Jinsi ya kusaidia kuzuia mashambulizi ya Phishing

Weka Sasisha programu yako

Mashambulizi ya uchukizo ambayo hutumia zisisho mara nyingi hutegemea mende za programu ili kupata zisizo kwenye mashine yako. Kawaida mara moja mdudu hujulikana, mtengenezaji wa

programu atatoa toleo la kurekebisha. Hii ina maana kuwa programu ya zamani ina zaidi ya vijiti vinavyojulikana hadharani vinavyoweza kutumiwa kusaidia kufunga zisizo. Kuweka programu yako hadi sasa inapunguza hatari zisizo za kinga.

Tumia Meneja ya Nywila moja kwa moja

Meneja Nywila kwamba nywila za kujaza auto zinaweka wimbo wa maeneo ambayo nywila hizo ni za. Ingawa ni rahisi kwa mtu kudanganywa na kurasa za uingizaji wa bandia, passwordmanagers haidanganyi kwa njia ile ile. Ikiwa unatumia meneja wa nenosiri (ikiwa ni pamoja na meneja wa nenosiri uliojenga katika kivinjari chako), na anakataa kujijaza nenosiri, unapaswa kusita na mara mbili uangalie tovuti uliyo nayo. Bora bado, matumizi ya nasibu yanayotokana nywila ili uweze kulazimishwa kutegemea kujitegemea, na uwezekano mdogo kuandika nenosiri lako kwenye ukurasa wa kuingia bandia.

Thibitisha mtumaji wa barua pepe

Njia moja ya kuamua kama barua pepe ni shambulio la uharibifu wa uwongo ni kuangalia kupitia njia tofauti na mtu ambaye amesema aliituma. Ikiwa barua pepe ilitumwa kutoka benki yako, usibofye viungo kwenye barua pepe. Badala yake, piga benki yako au ufungua kivinjari chako na ukipakue kwenye URL ya tovuti ya benki yako. Vivyo hivyo, ikiwa Mjomba wako Boris atakutumia kiambatisho cha barua pepe, kumwita simu na uulize kama alikutumia picha za watoto wake kabla ya kufungua.

Fungua Faili iliyokosewa Google Drive

Baadhi ya watu wanatarajia kupokea faili zilizoambatanishwa
Kutoka wa watu wasiojulikana. Kwa mfano waandishi wa habari kwa kawaida hupokeafaili kutoka kwenye chanzo. Ila ni vigumu kuthibitisha kuwa ni faili la maneno, excel spread sheet, au Faili la PDF sio malicious.

Katika hali hizi, usifungue mara mbili faili iliyopakuliwa. Badala yake, uipakishe kwenye Hifadhi ya Google au msomaji mwingine wa waraka wa mtandaoni. Hii itawageuza waraka katika picha au HTML, ambayo kwa hakika itauzuia kuanzisha zisizo kwenye kifaa chako. Ikiwa unafurahia kujifunza programu mpya na ukitumia muda wa kuanzisha mazingira mapya ya kusoma barua au nyaraka za kigeni, kuna mifumo ya uendeshaji iliyojitolea ili kupunguza kikomo cha athari za zisizo. TAILS ni mfumo wa uendeshaji wa Linux ambao unafuta baada ya kuitumia. Qubes ni mfumo mwingine wa Linux kofia hutenganisha kwa makini maombi ili wasiweze kuingilia kati, na kuzuia athari za zisizo zisizo. Wote ni iliyoundwa kufanya kazi kwenye kompyuta za kompyuta au kompyuta.

Unaweza pia kuwasilisha viungo na faili zisizo na kifungo kwenye VirusTotal, huduma ya mtandaoni inayoangalia faili na viungo dhidi ya injini mbalimbali za antivirus tofauti na inaripoti matokeo. Hii sio ya siri-antivirus mara nyingi hushindwa kugundua zisizo mpya au mashambulizi yaliyolengwa-lakini ni bora kuliko kitu.

Unaweza pia kuwasilisha viungo na faili zisizo na kifungo kwenye VirusTotal, huduma ya mtandaoni inayoangalia faili na viungo dhidi ya injini mbalimbali za antivirus tofauti na inaripoti matokeo. Hii sio ya siri-antivirus mara nyingi hushindwa kugundua zisizo mpya au mashambulizi yaliyolengwa-lakini ni bora kuliko kitu. Faili yoyote au kiungo ambacho unachopakia kwenye tovuti ya umma, kama vile VirusTotal au Google Drive, inaweza kutazamwa na mtu yeyote anayefanya kazi kwa kampuni hiyo, au labda mtu yeyote anayeweza kufikia tovuti hiyo. Ikiwa habari zilizomo katika faili ni nyeti au mawasiliano ya kibinafsi, unaweza kufikiria njia mbadala.

Kuwa Makini kwa maelekezo ya barua pepe

Maandishi mengine ya uwongo yanadai kuwa kutoka idara ya msaada wa kompyuta au kampuni ya teknolojia na kuuliza kujibu kwa nywila zako, au kuruhusu "mtu wa kurekebisha kompyuta" upatikanaji wa kijijini kwenye kompyuta yako, au kuzima kipengele fulani cha usalama kwenye kifaa chako. Barua pepe inaweza kutoa ufafanuzi uliotakiwa wa kwa nini hii ni muhimu, kwa kudai, kwa mfano, kwamba sanduku lako la barua pepe limejaa au kwamba kompyuta yako imetumwa. Kwa bahati mbaya, kutii maelekezo haya ya ulaghai inaweza kuwa mabaya kwako kweli.security. Kuwa makini kabla ya kutoa yeyote data ya kiufundi au kufuata maelekezo ya kiufundi isipokuwa unaweza kuwa na hakika kwamba chanzo cha ombi ni.

Ikiwa wewe ni sawa na barua pepe au kuunganisha mtu amekupeleka, usifungue au ukifungue mpaka umepunguza hali na vidokezo hapo juu na unaweza kuwa na uhakika sio madhara.