Kiberdrošība, pikšķerēšana un surogātpasts

Dalībnieki uzzinās par ļaunprātīgiem lietotājiem tiešsaistē, kuri var izmantot drošības nepilnības, lai iegūtu citu personu datus. Dalībnieki varēs raksturot tiešsaistes riskus, izveidot stratēģijas drošības uzlabošanai, identificēt surogātpastu un paskaidrot, kam ir tiesības pieprasīt viņu paroles.

Materiāli

- Izdales materiāls par surogātpastu

Riski tiešsaistē

Pirmā daļa

Informācijas sniegšana skolēniem

Izmantojot internetu, tu vari pakļaut sevi riskam, vienkārši piekļūstot kādai tīmekļa lapai, sazinoties tiešsaistē vai lejupielādējot datus. Kamēr tu pārlūko internetu, tevis apmeklētās vietnes, tīklā esošās personas un pat trešās puses var izsecināt tavu atrašanās vietu un citu informāciju.

Jautājumi skolēniem

Kas varētu izmantot tiešsaistes drošības nepilnības, lai piekļūtu tavai personiskajai informācijai?

1. Iespējamās atbildes: ļaunprātīgi hakeri, valdības pilnvaroti novērotāji utt.

Informācijas sniegšana skolēniem

Kamēr tu pārlūko tīmekli, ļaunprātīgi hakeri var apkopot tavus datus gluži tāpat kā interneta pakalpojumu sniedzēji. Lai samazinātu šo risku, izmanto drošu savienojumu, lai piekļūtu vietnei(-ēm). Tomēr neatkarīgi no tava savienojuma, daudzas vietnes mēģina izsekot tavas darbības dažādās platformās. Šīs vietnes var iegūt datus par tavu pārlūku, atrašanās vietu un citām darbībām, lai saprastu, kas tu esi.

Jautājumi skolēniem

Kāpēc lai ļaunprātīgi hakeri gribētu piekļūt tavai informācijai tiešsaistē? Kādu informāciju cilvēki meklē? Kāpēc lai vietne, kurā vairs neesi pieteicies, gribētu izsekot tavas darbības?

1. Jebkāda personu identificējoša informācija un informācija, kuru var pārdot vai izmantot, lai gūtu finansiālu labumu.

Vai kāds zina, kas ir ļaunprogrammatūra? Ko tā var darīt?

Informācijas sniegšana skolēniem

Ļaunprogrammatūra ir kaitīgs kods, kas slepeni darbojas tavā datorā. Dažas ļaunprogrammatūras var apkopot datus no tava datora, tostarp cietā diska datus un pārlūka datus. Tā var arī palīdzēt hakeriem pārņemt kontroli pār tavu datoru un izmantot to pēc saviem ieskatiem. Lielākā daļa ļaunprogrammatūru ir vienkāršākas,

piemēram, vietnes, kas imitē drošus portālus (piemēram, banku portālus), vai paplašinājumi, kas tavā pārlūkā rāda reklāmas, lai pelnītu.

Jautājumi skolēniem

Kā vari sevi pasargāt pret ļaunprogrammatūru, spiegošanu vai izsekošanu?

Informācijas sniegšana skolēniem

Esi piesardzīgs, klikšķinot uz saitēm, reklāmām vai ierakstiem sociālajos tīklos. Vai URL atbilst tam, ko gaidīji? Vai tu nonāc tajā pašā lapā, ja ieraksti šo URL manuāli vai meklē attiecīgo vietni? Svarīgu kontu (Google, Facebook, Twitter vai bankas kontu) pieteikšanās lapām ir jābūt aizsargātām ar SSL/TLS. Ja tiek izmantots SSL/TLS, hakerim, kurš atrodas tajā pašā tīklā, ir ļoti grūti nosūtīt tev viltotu vietni, kad tu ieraksti pareizo URL.

Dažas vietnes var izpildīt kodu, lai piekļūtu tavai personiskajai informācijai vai tiešsaistes kontiem, ja šajās platformās ir koda kļūda. Šādā gadījumā tavi konti var tikt izmantoti, lai sūtītu surogātpastu citām personām.

Lejupielādē un instalē programmatūru tikai no uzticamiem avotiem un rūpīgi apdomā, vai lejupielādēt izpildāmos failus (ar paplašinājumiem .exe, .pkg, .sh, .dll vai .dmg). Izpildāmie faili veic noteiktu darbību. Dažkārt tās var būt ļaunprātīgas darbības. Piemēram, kāds var izveidot izpildāmo failu, kas liktu izdzēst datora cietā diska datus vai instalēt viltotu pārlūku. Tieši tāpēc instalē saturu tikai no uzticamiem avotiem.

Vari izmantot antivīrusu programmatūru, kas tevi pasargās no ļaunprogrammatūras. Dažas antivīrusu programmatūras ir jau iebūvētas datorā (piemēram, Microsoft Security Essentials operētājsistēmai Windows), un dažām operētājsistēmām, piemēram, Apple datoros, ir drošības iestatījumi, kas bloķē programmatūru no neuzticamiem avotiem. Esi piesardzīgs, mainot šos iestatījumus.

Vari apsvērt arī pārlūka paplašinājumus, kas, piemēram, bloķē spraudņus, kas neļauj vietnēm tevi izsekot. Tomēr šie spraudņi var arī bloķēt noteiktas vietņu funkcijas, piemēram, video skatīšanās iespēju. Lai izlemtu, vai instalēt pārlūka paplašinājumus, tev ir jāizvērtē, cik tev svarīga sava drošība tiešsaistē un ar ko esi gatavs riskēt. Vari sev uzdot tālāk minētos jautājumus. “Cik ļoti mani apgrūtina izsekošana? Cik svarīgs ir mans privātums? Cik ļoti vēlos skatīties šo saturu (ja, piemēram, pārlūka paplašinājums bloķē video atveides spraudni)?”

Drošības rīki

Pirmā daļa

Sadarbība grupā

Lūdzu, ņem vērā tālāk minēto. Daļa no šīs aktivitātes satura ir ietverta 1. aktivitātē “Riski tiešsaistē”. Vari izvēlēties, vai vēlreiz izskatīt šo materiālu (ja jau esi veicis 1. aktivitāti) vai to izlaist.

Jautājumi skolēniem

Vai esi drošībā, izmantojot internetu?

Informācijas sniegšana skolēniem

Neveicot preventīvus pasākumus, ir grūti (pat neiespējami) efektīvi pasargāt sevi no apdraudējuma tiešsaistē (raksturots iepriekšējā sadaļā).

Ir svarīgi būt modram, jo tiešsaistē rodas arvien jauni riski.

Jautājumi skolēniem

Ko cita persona varētu izdarīt, ja viņa tevi pārliecinātu, ka viņas vietne ir īsta?

Ir pieejami dažādi rīki šo risku novēršanai vai mazināšanai. Vai kāds var nosaukt kādu rīku?

Informācijas sniegšana skolēniem

HTTPS ir standarts, kas tiek izmantots vietnēs, lai šifrētu internetā pārsūtītos datus. Šifrēšana traucē trešajām pusēm skatīt savienojuma laikā pārsūtītos datus. Tā uzlabo drošību un var tikt izmantota ikvienā pārlūkā, pievienojot “https:/” pirms attiecīgā URL (piemēram, https://www.manavietne.com). Tomēr ne visas vietnes atbalsta protokolu HTTPS.

1. Sensitīvu informāciju (piemēram, paroles, kredītkartes informāciju) ieteicams ievadīt tikai tādās tīmekļa lapās, kuru tīmekļa adrese sākas ar prefiksu HTTPS://.

2. Vari izmantot programmatūras rīkus, lai HTTPS tiktu lietots, kad vien tas iespējams.

3. Lielākajai daļai pārlūku HTTPS savienojumi tiek norādīti ar slēdzenes ikonu, kas atrodas blakus adreses joslai.

4. Tomēr HTTPS negarantē drošību, jo arī ļaunprātīgas vietnes var izmantot

HTTPS. HTTPS aizsargā savienojumu, bet negarantē, ka pati vietne nav ļaunprātīga.

Drošligzdu slānis (Secure Sockets Layer — SSL)/Transporta slāņa drošība (Transport Layer Security — TLS) ir HTTPS drošības tehnoloģijas nosaukumi. SSL/TLS izmanto digitālās šifrēšanas atslēgas, kas darbojas līdzīgi tradicionālajām atslēgām. Ja tu uz papīra lapiņas uzrakstītu kādu draugam paredzētu noslēpumu, ikviens, kurš atrastu šo lapiņu, uzzinātu tavu noslēpumu. Tā vietā iedomājies, ka tu iedotu savam draugam atslēgas kopiju un pēc tam sūtītu savus noslēpumus slēgtā kastē. Ja kāds pārtvertu šo kasti, viņam būtu jānopūlas, lai apskatītu tavu noslēpumu bez atslēgas. Ja kāds mēģinātu aizstāt kasti ar līdzīgu kasti, tu to pamanītu, jo tava atslēga nedarbotos. SSL/TLS darbojas gluži tāpat — tikai vietnē.

Pārlūka drošības indikatori norāda arī paplašinātās validācijas (Extended Validation — EV) sertifikāta informāciju. EV sertifikāti tiek piešķirti vietnēm, kas ir verificētas noteiktā sertificēšanas iestādē. Dažkārt pārlūkos EV indikators ir kā vietnes nosaukums vai reģistrācijas iestāde blakus adreses joslai. EV sertifikāti tiek piešķirti vietnēm, kas ir verificētas noteiktā sertificēšanas iestādē. Dažkārt pārlūkos EV indikators ir kā vietnes nosaukums vai reģistrācijas iestāde blakus adreses joslai. Ja kādas vietnes saturs tev šķiet aizdomīgs, vari pārbaudīt, vai sertifikātā minētais URL atbilst pārlūkā redzamajam URL. Lai to izdarītu, noklikšķini uz “Skatīt sertifikātu”. (Būtu noderīgi projektora ekrānā parādīt, kā atrast vienumu “Skatīt sertifikātu”.) Katrā pārlūkā tas ir atrodams citādi. Piemēram, pārlūkā Chrome atver sadaļu “Skatīt”, noklikšķini uz “Izstrādātājs” un pēc tam — uz “Izstrādātāja rīki”. Sadaļā “Izstrādātāja rīki” noklikšķini uz cilnes “Drošība” un pēc tam — uz “Skatīt sertifikātu”.

Antivīrusu programmatūra ne tikai neļauj palaist programmatūru no neuzticamiem avotiem, bet arī brīdina par neuzticamām vietnēm un ļaunprogrammatūru.

Pikšķerēšana parasti notiek e-pastā, kad kāds uzdodas par uzticamu personu. Šī persona mēģina iegūt paroli, cerot, ka to nosūtīsi e-pastā vai ievadīsi viltotā vietnē. Surogātpasta filtri var neļaut šādiem e-pasta ziņojumiem nonākt tavā iesūtnē. Lai uzlabotu surogātpasta filtru darbību, atzīmē jebkādus aizdomīgus e-pasta ziņojumus, kuri ir nonākuši tavā iesūtnē kā surogātpasts.

Jautājumi skolēniem

Kādas darbības būtu jāveic, lai nejauši nelejupielādētu kaitīgus failus savā datorā?

Informācijas sniegšana skolēniem

Vienmēr pārbaudi, vai lejupielādē failus no uzticamām vietnēm. Esi īpaši piesardzīgs, atverot e-pasta ziņojumu pielikumus, kurus neatpazīsti, kā arī noklikšķinot uz uznirstošajiem logiem un kļūdu ziņojumiem. Vari arī savā datorā instalēt atzītas programmas, kas aizsargā pret ļaunprogrammatūru.

Paroļu izpaušana

Pirmā daļa

Jautājumi skolēniem

Kādos gadījumos ir pieņemami izpaust savu paroli?

1. Iespējamā atbilde: koplietojamie konti, piemēram, Netflix.

Kādi ir paroles izpaušanas riski?

1. Ja ļaunprātīga persona iegūst tavu paroli, viņa var uzlauzt tavu kontu. Paroles izpaušana palielina risku, ka kāds iegūs piekļuvi tavam kontam. Ja tā pati parole tiek izmantota citām vietnēm, šī persona var piekļūt arī šīm vietnēm.

Informācijas sniegšana skolēniem

Nav ieteicams norādīt savu paroli nevienam citam kā tikai lietojumprogrammai, kurai tā nepieciešama, lai tu varētu tajā pieteikties. Kā tika minēts iepriekš, pikšķerēšana ir process, kad kāds maldina lietotāju, lai tas izpaustu savu paroli.

Dažkārt cilvēki var tieši pieprasīt piekļuvi tavam kontam, apgalvojot, ka tas ir apdraudēts. Šiem cilvēkiem var būt labi nodomi, piemēram, draugs var tev palīdzēt izpētīt nesaprotamu informāciju tavā kontā, tomēr izpaust savu paroli nav droši, it īpaši, ja tu lieto šo paroli vairākiem kontiem. Ja tu plāno izpaust savu paroli, gādā par to, lai tā netiktu lietota nekur citur, un izmanto paroļu pārvaldnieku, lai koplietotu piekļuvi.

Dažkārt tavu paroli vēlas uzzināt cilvēki, ko tu pazīsti un kuriem uzticies, piemēram, vecāki, pasniedzēji, darba devēji. Kaut arī tu pazīsti šos cilvēkus un uzticies viņiem, ir ieteicams vispirms apspriest, kāpēc viņi vēlas uzzināt tavu paroli un kā viņi to izmantos. Ja tie ir pieaugušie ārpus tavas ģimenes, ir vērts viņiem pajautāt, vai pastāv kāds likums vai cita veida noteikums, kas, viņuprāt, pieprasa, lai tu viņiem izpaustu savas paroles.

Ir īpaši svarīgi uzdot pieklājīgus un skaidrus jautājumus, ja tavu paroli pieprasa kāds personiski nepazīstams pieaugušais ārpus tavas ģimenes, piemēram, tiesībaizsardzības amatpersona. Ja policists vai ierēdnis vēlas uzzināt tavas sociālo tīklu paroles, saglabā mieru un esi pieklājīgs. Jautā šai personai, kāpēc viņa to pieprasa un kurš likums vai noteikums (vai vairāki) atļauj šai personai iegūt no tevis šo informāciju.

Atkarībā no apstākļiem, kuros vecāki/aprūpētāji, pasniedzējs, darba devējs,

tiesībaizsardzības amatpersona, ierēdnis vai kāds cits pieaugušais pieprasa tavas paroles, tev var nākties izpaust savas paroles. Apstākļi, kuros tev būtu jāizpauž savas paroles: likums vai noteikums, kas to pieprasa; tavs lēmums izpaust paroles, pamatojoties uz to, ka tev šo personu palīdzība būtu svarīgāka par risku, ko rada paroļu izpaušana.

Ja tu no kāda pieaugušā saņem pieprasījumu izpaust savas paroles un šis pieprasījums tev liek justies neērti, nekavējoties vērsies pēc palīdzības pie vecākiem/aprūpētājiem vai cita uzticama pieaugušā, pirms atbildi uz pieprasījumu.

Jautājumi skolēniem

Kādos apstākļos tev būtu jāizpauž sava parole tiešsaistē?

1. Tikai tad, ja paroli pieprasa vietne, kurai mēģini piekļūt. Nekad neizpaud savas paroles citur, arī ne e-pastā, kas parasti netiek šifrēts un nav drošs.

Uzdevums

Izdales materiāls

Uzdevums

Sadali dalībniekus grupās pa 2–3. Izdali dalībniekiem materiālu par surogātpastu. Pēc tam lūdz katram dalībniekam izveidot blokshēmu, lai demonstrētu citiem, kā identificēt surogātpastu un izvērtēt, vai atklāt informāciju noteiktām personām/grupām.

Informācijas sniegšana skolēniem

Nolasi katru scenāriju un apspried ar dalībniekiem, vai ziņojumi ir surogātpasts un vai būtu jāatklāj informācija scenārijā minētajām personām vai grupām.

Sadarbība grupā

Atvēli dalībniekiem 10 minūtes uzdevumam. Pēc tam lūdz grupām dalīties ar savām atbildēm.

Jautājumi skolēniem

Kādos gadījumos tev būtu jāatklāj sava parole e-pastā?

Informācijas sniegšana skolēniem

Vietnes un uzņēmumi parasti nepieprasa atklāt paroles e-pastā. Nekad neatklāj savas paroles šādā veidā, pat ja tev šķiet, ka sūtītājs ir uzticams. E-pasts gandrīz nekad nav drošs.

Otrā daļa

Uzdevums

Lūdz dalībniekus atgriezties savās vietās, jo nākamais uzdevums būs jāveic individuāli.

Atvēli dalībniekiem 15 minūtes blokshēmu izveidei.

Informācijas sniegšana skolēniem

Uz papīra lapas izveido blokshēmu, lai parādītu, kā identificēt surogātpastu un izvērtēt, vai atklāt citiem noteiktu informāciju tiešsaistē. Ieteicams blokshēmai izmantot konkrētu scenāriju — vienu no izdales materiālā minētajiem (tādā gadījumā virs blokshēmas norādi scenārija numuru) vai pilnīgi jaunu scenāriju. Ja vēlies

izveidot savu scenāriju, uzraksti to īsā rindkopā virs blokshēmas.

Atvēli dalībniekiem 15 minūtes blokshēmu izveidei.