

Kibernetinis saugumas, duomenų vagystė ir šlamštas

Dalyviai sužinos apie kenkėjiškus interneto vartotojus, kurie naudodamiesi saugumo spragomis gali mėginti rinkti informaciją apie juos. Dalyviai taip pat galės apibūdinti naudojimosi internetu pavojus, sukurti saugesnio elgesio strategijas, atpažinti šlamšto pranešimus ir paaiškinti, kas turėtų prašyti jų slaptažodžio.

Medžiaga

Su šlamštu susijusi padalomoji medžiaga

Pavojai internete

Pirma dalis

Papasakokite mokiniams

Naudodamiesi internetu galite sukelti sau pavojų vos atsidarę interneto puslapį, susirašinėdami internetu ar atsisiųsdami duomenis. Jums naršant, interneto svetainės, kuriose lankotės, tame pačiame tinkle esantys žmonės ar net trečiosios šalys gali sužinoti jūsų buvimo vietą ir kitą informaciją apie jus.

Paklauskite mokinių

Kas gali pasinaudoti internetinio saugumo spragomis norėdami sužinoti jūsų asmens informaciją?

1. Galimi atsakymai yra kenkėjiški įsilaužėliai, valdžios vykdomas stebėjimas ir pan.

Papasakokite mokiniams

Jums naršant internete, kenkėjiški įsilaužėliai gali rinkti duomenis apie jus taip pat, kaip tai atlieka interneto paslaugų teikėjai. Norėdami sumažinti šią riziką, turite naudoti saugų ryšį tarp jūsų ir norimos pasiekti interneto svetainės (-ių). Nepriklausomai nuo jūsų ryšio, dauguma interneto svetainių mėgina stebėti jūsų naudojimo modelius keliose platformose. Jos gali stebėti jūsų naršyklę, buvimo vietą ir kitus naudojimo modelius norėdamos sužinoti, kas jūs esate.

Paklauskite mokinių

Kodėl kenkėjiški įsilaužėliai mėgina pasiekti jūsų informaciją internete? Kokios informacijos žmonės ieško? Kodėl interneto svetainė, prie kurios nesate prisijungę, nori žinoti, kas jūs esate?

1. Bet kokia asmenį identifikuojanti informacija arba bet kokia informacija, kurią galima parduoti arba naudoti pinigams uždirbti.

Ar kas nors žino, kas yra kenkėjiškos programos? Ką jos gali padaryti?

Papasakokite mokiniams

Kenkėjiškos programos – tai kenkėjiškas kodas, kuris slapta veikia jūsų kompiuteryje. Kai kurios kenkėjiškos programos gali rinkti bet kokius jūsų kompiuteryje esančius duomenis, nuo kietajame diske iki naršyklėje esančių

duomenų. Jos taip pat gali leisti įsilaužėliams užvaldyti jūsų kompiuterį ir naudoti jį bet kokiais tikslais. Tačiau dauguma kenkėjiškų programų yra paprastesnės, pvz., interneto svetainės, kurios imituoja saugius portalus, pvz., banką, arba plėtiniai, kurie pateikia reklamas jūsų naršyklėje siekiant užsidirbti pinigų.

Paklauskite mokinių

Ką galite padaryti norėdami apsisaugoti nuo kenkėjiškų programų, šnipinėjimo arba stebėjimo?

Papasakokite mokiniams

Elkitės atsargiai spustelėdami nuorodas, reklamas arba socialinių tinklų įrašus. Ar URL atitinka tą, kurio tikėtės? Ar patenkate į tą patį puslapį dar kartą patys įrašę jo adresą arba ieškodami interneto svetainės? Reikėtų vadovautis principu, kad SSL / TLS turėtų apsaugoti bet kokią svarbios paskyros (pvz., „Google“, „Facebook“, „Twitter“ arba banko paskyrų) prisijungimo puslapį. Naudojant SSL / TLS tame pačiame tinkle esančiam įsilaužėliui yra daug sunkiau jums atsiųsti netikrą interneto puslapį, jei įvedate tinkamą URL, kas kitu atveju būtų labai paprasta.

Kai kuriose interneto svetainėse, kur buvo atlikta kodavimo klaida, gali veikti kodas, mėginantis pasiekti jūsų asmens informaciją arba internetines paskyras. Tada šios paskyros gali būti naudojamos šlamštui siųsti kitiems žmonėms.

Programinę įrangą atsisiųskite ir diekite tik iš patikimų šaltinių ir gerai pagalvokite prieš atsisiųsdami diegimo failus (.exe, .pkg, .sh, .dll arba .dmg plėtiniai). Diegimo failai yra bet kokie failai, kurie paleis veiksmą. Kartais tai gali būti blogi veiksmai. Pavyzdžiui, kitas asmuo gali sukurti vykdomąjį tekstą, kuris ištrins kietąjį diską arba įdiegs netikrą naršyklę. Todėl turinį diegti turite tik iš patikimų šaltinių.

Galite naudoti antivirusinę programinę įrangą norėdami apsisaugoti nuo kenkėjiškų programų paleidimo. Kai kurios antivirusinės programos pateikiamos su jūsų kompiuteriu (pvz., „Windows“ skirta „Microsoft Security Essentials“), o kitose operacinėse sistemose, pvz., „Apple“ kompiuteriuose, yra saugos nuostatos, blokuojančios programinės įrangos iš nepatikimų šaltinių diegimą. Atidžiai pagalvokite prieš nepaisydami šių nuostatų.

Taip pat pagalvokite apie naršyklės plėtinių, galinčių, pvz., blokuoti įskiepius, diegimą, nes jie apsunkina jūsų identifikavimą ir stebėjimą. Tačiau tas pats įskiepis gali blokuoti interneto svetainių funkcijas, pvz., galimybę žiūrėti vaizdo įrašus. Naršyklės plėtinių diegimas priklauso nuo jūsų nuostatų ir kompromisų, kuriuos esate pasiruošę priimti norėdami didesnio saugumo internete. Turėtumėte atsakyti sau į klausimus: kiek man nepatogu, kad esu stebimas? Kiek vertas mano privatumas? Ar tikrai noriu peržiūrėti šį turinį (jei, pvz., naršyklės plėtinys blokuoja vaizdo įrašą atkuriantį įskiepi)?

Saugumo įrankiai

Pirma dalis

Kurso veikla

Atkreipkite dėmesį: dalis šios veiklos turinio aptarta „1 veikloje: Pavojai internete“. Galite nuspręsti, ar norite vėl peržiūrėti šią medžiagą, jei jau atlikote 1 veiklą, ar ją praleisti.

Paklauskite mokinių

Ar žinote, kiek saugūs esate naudodamiesi internetu?

Papasakokite mokiniams

Nesiimant tinkamų atsargumo priemonių, apsaugoti nuo šių pavojų internete (aprašytų ankstesniame skirsnyje) yra sunku ir dažnai neįmanoma.

Nauji pavojai internete atsiranda nuolat, todėl svarbu išlikti budriems.

Paklauskite mokinių

Ką kitas asmuo galėtų padaryti, jei jus įtikintų, kad jų interneto svetainė iš tikrųjų yra svarbi interneto svetainė?

Yra įrankių, kuriuos galite naudoti norėdami išvengti šių pavojų arba juos sumažinti. Ar kas nors žinote nors vieną?

Papasakokite mokiniams

HTTPS yra standartas, kurį interneto svetainės naudoja internetu perduodamiems duomenims šifruoti. Šifravimas gali užkirsti kelią trečiajai šaliai lengvai peržiūrėti jūsų ryšio duomenis. Jis suteikia papildomą saugumo lygį ir jį galima naudoti bet kurioje naršyklėje, pasirinkto URL pradžioje pridėjus „https://“ (pvz., <https://www.mysite.com>). Vis dėlto ne visos interneto svetainės palaiko HTTPS.

1. Jautrią informaciją (pvz., slaptažodžius, kredito kortelės informaciją) turėtumėte įvesti tik tose svetainėse, kuriose naudojamas HTTPS:// prefiksas.
2. Galite naudoti programinės įrangos įrankius norėdami užtikrinti, kad visada naudotumėte HTTPS, kai tai įmanoma.
3. Dauguma pagrindinių naršyklių naudoja saugumo rodiklius, kurie atrodo kaip spynelės greta adreso juostos, kad nurodytų HTTPS ryšius.

4. Tačiau HTTPS neužtikrina, kad jūs esate saugus, nes kai kurios kenkėjiškos interneto svetainės taip pat gali naudoti HTTPS. HTTPS apsaugo ryšį, tačiau neužtikrina, kad svetainė nėra kenkėjiška.

Technologija, palaikanti HTTPS saugumą, vadinasi saugiųjų jungimų lygmuo (angl. Secure Sockets Layer (SSL) / transporto lygio saugumas (angl. Transport Layer Security (TLS). SSL / TLS naudoja skaitmeninius šifravimo raktus, kurie veikia panašiai kaip ir tikri raktai. Jei ant popieriaus lapo draugui užrašėte paslaptį, šį lapą radęs asmuo galės perskaityti jūsų paslaptį. Vietoje to įsivaizduokite, kad jam asmeniškai davėte rakto kopiją ir paslaptis išsiuntėte atitinkamose užrakintose dėžutėse. Jei kas nors sulaikytų dėžutę, jiems būtų sunku perskaityti paslaptį neturint rakto. Jei kas nors bandytų pakeisti dėžutę panašia dėžute, jūs pastebėtumėte, kad jūsų raktas neveikia. SSL / TLS veikia tokiu pačiu būdu, tačiau interneto svetainėje.

Naršyklės saugumo rodikliai taip pat perduos išplėstinio patvirtinimo (EV) liudijimo informaciją. EV liudijimai suteikiami toms interneto svetainėms, kurios patvirtina savo tapatybę liudijimo institucijai. Naršyklėse EV rodiklis kartais parodomas kaip interneto svetainės pavadinimas arba registravimo subjektas greta adreso juostos. EV liudijimai suteikiami toms interneto svetainėms, kurios patvirtina savo tapatybę liudijimo institucijai. Naršyklėse EV rodiklis kartais parodomas kaip interneto svetainės pavadinimas arba registravimo subjektas greta adreso juostos. Jei kyla įtarimų dėl tam tikros interneto svetainės turinio, galite patikrinti, ar liudijime esantis URL atitinka naršyklės URL, tą padarykite spustelėdami „Žiūrėti liudijimą“. (Gali būti naudinga projektoriaus ekrane parodyti, kaip rasti „Žiūrėti liudijimą“.) Kaip tai atliksite, priklausys nuo naršyklės. Pavyzdžiui, jei naudojate „Chrome“, lange „Rodinys“ spustelėkite „Kūrėjas“ ir tada „Kūrėjo įrankiai“. Lange „Kūrėjo įrankiai“ spustelėkite skirtumą „Saugumas“ ir tuomet „Žiūrėti liudijimą“.

Antivirusinės programos ne tik neleidžia paleisti programinės įrangos iš nepatikimų šaltinių, bet ir gali neleisti jums lankytis nepatikimuose puslapiuose ir atsisiųsti kenkėjiškų programų.

„Duomenų vagystė“ dažniausiai vykdoma el. laiškais, kai šlamšto siuntėjas apsimeta tikrąja šalimi. Tada jis prašo jūsų slaptažodžio ir tikisi, kad jį atsiųsite el. paštu arba įvesite netikroje interneto svetainėje. Šlamšto filtrai kai kuriuos iš šių el. laiškų gali pašalinti iš pranešimų dėžutės. Norėdami, kad šlamšto filtrai veiktų geriau, visada pažymėkite visus įtartinus į jūsų pranešimų dėžutę patekusius el. laiškus kaip šlamštą.

Paklauskite mokinių

Kokių galima imtis veiksmų norint apsisaugoti nuo netyčinio kompiuteriui kenksmingų failų atsisiuntimo?

Papasakokite mokiniams

Visada gerai įsitikinkite, kad atsisiuntimus pasiekiate iš patikimų interneto svetainių. Labai gerai pagalvokite prieš atidarydami el. laiškų priedus, kurių neatpažįstate, ir spustelėdami iškylančiuosius langus bei klaidų pranešimus. Taip pat kompiuteryje galite įdiegti patikimas programas, apsaugančias nuo kenkėjiškų programų.

Slaptažodžių bendrinimas

Pirma dalis

Paklauskite mokinių

Kaip jums atrodo, kada galima bendrinti savo slaptažodį?

1. Galimi atsakymai apima bendrinamas paskyras (pvz., „Netflix“).

Kokie yra galimi su slaptažodžių bendrinimu susiję pavojai?

1. Jei kenkėjiškas asmuo gauna jūsų slaptažodį, į jūsų paskyrą galima įsilaužti. Bendrinant savo slaptažodį didėja tikimybė, kad kitas žmogus turės prieigą. Jei tas pats slaptažodis naudojamas kitose interneto svetainėse, kitas žmogus taip pat gali jas pasiekti.

Papasakokite mokiniams

Įprasta praktika yra nebendrinti slaptažodžių su niekuo, išskyrus programą, kuriai jo reikia norint prisijungti. Kaip aprašyta anksčiau, duomenų vagystė yra asmens apgavimas siekiant iš jo išgauti slaptažodį.

Tačiau kiti asmenys gali tiesiogiai prašyti jūsų slaptažodžio norėdami pasiekti jūsų paskyras ir tvirtindami, kad jūsų paskyra yra pavojuje. Nors kai kurie žmonės turi gerų ketinimų, pvz., draugas, kuris nori padėti ir pažiūrėti jums neaiškia vietą paskyroje, nėra protinga bendrinti savo slaptažodį, ypač jei jį naudojate keliose paskyrose. Jei ketinate bendrinti slaptažodį, įsitikinkite, kad jis niekur kitur nenaudojamas, ir prieigai bendrinti naudokite slaptažodžių tvarkyklę.

Kartais jūsų slaptažodžių prašantys žmonės gali būti jūsų pažįstami suaugusieji, kuriais pasitikite, pvz., jūsų tėvai, mokytojai ar darbdavys. Net jei ir pažįstate šiuos suaugusiuosius ir jais pasitikite, įprastai visiems (tiek jums, tiek jiems) yra teigiama patirtis pasikalbėti apie tai, kodėl jie to prašo ir kaip jie tvarkys jūsų slaptažodžius. Jei šie suaugusieji nėra jūsų šeimos nariai, protinga būtų tiesiogiai paklausti, ar jų manymu, yra įstatymas ar kitoks teisės aktas, pagal kurį jūs turite duoti jiems savo slaptažodžius.

Mandagūs ir aiškūs klausimai apie įstatymus ir teisės aktus ypač svarbūs, kai slaptažodžio reikalauja suaugusysis, kuris nėra jūsų šeimos narys ir jo dar nepažįstate asmeniškai, pvz., teisėsaugos pareigūnas. Jei policijos ar kitas vyriausybės pareigūnas reikalauja jūsų socialinių tinklų slaptažodžių, išlikite ramūs ir pagarbūs. Paklauskite, kodėl jie to reikalauja, ir koks įstatymas (-ai) arba teisės aktas (-ai), jų manymu, suteikia jiems teisę gauti iš jūsų šią informaciją.

Atsižvelgiant į tėvų / globėjų, mokytojo, darbdavio, teisėsaugos pareigūno, vyriausybės pareigūno ar kito suaugusiojo reikalavimo aplinkybes, jums gali tekti pateikti jiems savo slaptažodžius. Aplinkybės, kai jums gali tekti pateikti savo slaptažodžius: jei galioja įstatymas ar teisės aktas, pagal kurį turite tai atlikti, arba gauta pagalba, jūsų nuomone, viršija slaptažodžio bendrinimo pavojus.

Jei suaugusysis reikalauja iš jūsų slaptažodžių ir šis reikalavimas verčia jus jaustis nepatogiai, nedelsiant (pageidautina prieš atsakant į reikalavimą) kreipkitės į tėvus / globėjus arba kitą patikimą suaugusįjį.

Paklauskite mokinių

Kokiomis aplinkybėmis turėtumėte bendrinti savo slaptažodį internete?

1. Tik tada, kai interneto svetainė, kurią norite pasiekti, prašo jūsų slaptažodžio. Niekada nebendrinkite savo slaptažodžio niekur kitur, įskaitant el. paštu, kuris dažniausiai nėra šifruotas arba saugus.

Užduotis

Padalomoji medžiaga

Užduotis

Suskirstykite dalyvius į grupes po 2–3. Išdalinkite dalyviams šlamšto padalomą medžiagą. Po to paprašykite kiekvieno dalyvio sukurti struktūrinę schemą, kuria parodytų kitiems kaip atpažinti šlamštą. Taip pat, ar jie bendrintų konkrečią informaciją su tam tikrais žmonėmis / žmonių grupėmis.

Papasakokite mokiniams

Perskaitykite kiekvieną scenarijų ir aptarkite, ar kiekvienas pranešimas yra šlamštas ir ar tokiu atveju turėtumėte bendrinti informaciją su žmogumi arba žmonių grupe.

Kurso veikla

Skirkite dalyviams 10 minučių šiai užduočiai atlikti. Po to paprašykite grupių pasidalinti savo atsakymais.

Paklauskite mokinių

Kada galima bendrinti savo slaptažodį el. paštu?

Papasakokite mokiniams

Interneto svetainės ir kompanijos įprastai niekada neprašo jūsų slaptažodžio el. paštu. Niekada niekam neperduokite savo slaptažodžio tokiu būdu, net jei ir atrodo, kad prašymas yra tikras. El. paštas beveik niekada nėra saugus.

Antra dalis

Užduotis

Paprašykite dalyvių grįžti iš savo grupių, nes toliau pateikta užduotis yra individuali.

Skirkite dalyviams 15 minučių struktūrinėms schemoms sukurti.

Papasakokite mokiniams

Dabar popieriaus lape nubraižykite struktūrinę schemą, kurioje dalyviams būtų parodyta, kaip atpažinti šlamštą ir ar jie turėtų bendrinti tam tikrą informaciją internetu su kitais žmonėmis. Gali būti lengviau, jei savo struktūrinėje schemoje naudosite konkretų scenarijų. Tai gali būti vienas iš padalomojoje medžiagoje pateiktų scenarijų (jei nuspręsite tai daryti, užrašykite scenarijaus numerį virš savo

struktūrinės schemos) arba visiškai naujas scenarijus. Jei nuspręsite kurti savo scenarijų, trumpai jį aprašykite virš savo struktūrinės schemos.

Skirkite dalyviams 15 minučių struktūrinėms schemoms sukurti.