Kiberbiztonság, adathalászat és kéretlen tartalom

A résztvevők megismerkednek az online világ rosszindulatú felhasználóival, akik biztonsági hiányosságok után kutatnak, hogy adatokat gyűjthessenek más emberekről. A résztvevők megismerkednek az internetezés kockázataival, kidolgozzák a biztonságos magatartások stratégiáit, megtanulják azonosítani a kéretlen és rosszindulatú tartalmakat, valamint megismerik a helyes reakciókat azokban a helyzetekben, amikor valaki jelszavuk megadására kéri őket.

Anyagok

- Kéretlen tartalom játéklap

Online veszélyek

Első rész

Mondd el a diákjaidnak!

Internetezés közben veszélyek leselkedhetnek rád már olyan egyszerű műveletek közben is, mint egy weboldal megnyitása, online kommunikáció vagy adatok letöltése. Böngészés közben a felkeresett webhely, az ugyanahhoz a hálózathoz csatlakozó személyek vagy akár mások számára is lehetővé válhat tartózkodási helyed megállapítása vagy más veled kapcsolatos információk megismerése.

Kérdezd meg a diákjaidtól!

Az online sérülékenységek miatt kiknek jöhet jól személyes adataid megismerése?

1. Lehetséges válaszok például: rosszindulatú személyek, hackerek, megfigyelést végző kormányszervek stb.

Mondd el a diákjaidnak!

Eltökélt hackerek össze tudják gyűjteni rólad ugyanazokat az információkat internetezés közben, amiket az internetszolgáltatód lát. Ennek elkerülésére szolgál a biztonságos kapcsolat létesítése a felkeresett webhelyekkel. Az internetkapcsolattól függetlenül is számos webhely próbálhatja meg követni online tevékenységeidet és használati szokásaidat más platformokon is. Böngésző, tartózkodási helyed és internethasználati szokásaid alapján megpróbálják kideríteni, ki is vagy te.

Kérdezd meg a diákjaidtól!

Miért szeretnék rosszindulatú hackerek megszerezni a személyes adataidat online? Milyen adatokra vadászhatnak? Miért akarna egy webhely kijelentkezés után is tovább követni, hogy többet tudjon meg rólad?

1. A személyazonosításra alkalmas adatok és a felhasználói szokások adatai egyaránt pénzt érhetnek bizonyos szervezeteknek, vagy más módon nyereségre válthatók.

Tudja valaki, hogy a digitális világban mi egy kártevő? Mire képes?

Mondd el a diákjaidnak!

A kártevő egy rosszindulatú programkód, amely észrevétlenül fut számítógépeden. Egyes kártevők mindenféle adatot össze tudnak gyűjteni, számítógéped

merevlemezéről és böngésződből egyaránt. Bizonyos kártevők lehetővé teszik a hackerek számára, hogy teljesen átvegyék az uralmat számítógéped fölött. A legtöbb kártevő ugyanakkor nem ennyire kidolgozott. Gyakoribb, hogy csak hamis weboldalakat működtetnek adathalászat céljából (például egy bankéhoz hasonló weboldalt), vagy egy böngészőbővítményen keresztül folyamatosan hirdetéseket jelenítenek meg, anyagi hasznot hajtva készítőjüknek.

Kérdezd meg a diákjaidtól!

Mit lehet tenni a kártevők, a kémprogramok és a követés ellen?

Mondd el a diákjaidnak!

Légy elővigyázatos, mielőtt bármilyen hivatkozásra, hirdetésre vagy közösségimédia-bejegyzésre kattintanál. Az URL-cím az, amire számítottál? Ugyanez az oldal töltődik be, ha kézzel írod be a címet, vagy keresőmotorból nyitod meg a webhelyet? A fontosabb szolgáltatások (Google, Facebook, Twitter, netbankok stb.) bejelentkezési oldalait SSL/TLS kapcsolatbiztonságnak kell védenie. Az SSL/TLS nagyon megnehezíti azt a hackerek által kedvelt eljárást, hogy csatlakoznak egy hálózathoz, és az ott mások által beírt URL-címeket átirányítják egy hamis webhelyre.

Egyes webhelyek kód lefuttatásával megpróbálhatnak hozzáférni személyes adataidhoz vagy online fiókjaidhoz, ha a platform kódolása esetleg hibás. Az így megszerzett fiókhozzáféréseket gyakran levélszemétküldésre használják fel.

Csak megbízható forrásból tölts le és telepíts szoftvereket, és légy különösen óvatos futtatható fájlok letöltésekor (pl. .exe, .pkg, .sh, .dll vagy .dmg kiterjesztésű fájlok). A futtatható (más néven végrehajtható) fájlok valamilyen műveletet hajtanak végre. Időnként ez kártékony művelet is lehet. Egy futtatható fájl például törölheti merevlemezed teljes tartalmát, vagy telepíthet egy manipulált böngészőt. Ezért nagyon fontos, hogy csak megbízható forrásból telepíts bármit.

Vírusvédelmi szoftver telepítésével a legtöbb esetben megakadályozható a kártevők lefuttatása. Egyes vírusvédelmi szoftverek számítógépeden már eredetileg telepítve lehetnek (például Windows rendszer alatt a Microsoft Security Essentials), más esetekben az operációs rendszer biztonsági beállításai akadályozzák meg, hogy nem megbízható forrásból származó szoftver legyen telepítve (ez a helyzet például az Apple számítógépeknél). Ezeket a beállításokat csak nagyon alapos mérlegelés után bíráld felül.

Léteznek böngészőbővítmények, amelyek arra szolgálnak, hogy letiltsd a különböző beépülő modulokat. Ezzel jelentősen megnehezítheted az illetéktelenül kíváncsiskodó webhelyek dolgát. A bővítmények ugyanakkor hasznos funkciókat is letilthatnak a webhelyeken (például videók megnézését). A böngészőbővítmények telepítése egyéni mérlegelés kérdése, amiről az online biztonságod fontosságával kapcsolatos kompromisszumként dönthetsz. Elgondolkodhatsz például azon,

mennyire zavar téged, ha néhány webhely követ. Mennyi áldozatot ér meg neked személyes adataid védelme? Mennyire fontos, hogy megnézd az adott tartalmat (ha például a böngészőbővítményed pont letiltja egy videó lejátszását)?

Biztonságnövelő eszközök

Első rész

Interakció a leckével

Fontos: Ennek a tevékenységnek egy részét már feldolgoztuk az 1. foglalkozáson: „Online veszélyek”. Ha az 1. foglalkozáson már túl vagytok, saját belátásod szerint dönts arról, hogy érdemes-e újra végigmenni ezen a témán, vagy át lehet most ugrani.

Kérdezd meg a diákjaidtól!

Mit tudsz arról, mennyire vagy biztonságban internetezés közben?

Mondd el a diákjaidnak!

Megfelelő óvintézkedések nélkül szinte lehetetlen védekezni az online veszélyek ellen [amelyekről korábban beszéltünk].

Új és új fenyegetettségek bukkannak fel szinte naponta, ezért a felkészültség és az óvatosság elengedhetetlen.

Kérdezd meg a diákjaidtól!

Mit tehetne meg egy rosszindulatú felhasználó azután, hogy meggyőzött róla, hamisított webhelye a számodra fontos webhelyek egyike?

Néhány eszköz és technológia segíthet a kockázatok csökkentésében. Ismer valaki ilyeneket?

Mondd el a diákjaidnak!

A webhelyek az internetes adatcsere titkosítására a standard HTTPS protokollt használják. A titkosítás nagyon megnehezíti az adatforgalom visszafejtését valamilyen támadó részéről. Ez az extra biztonsági réteg bármely böngészőből használható, és a „https://” előtag jelzi az URL-címben (pl. https://www.mysite.com). Nem minden webhely támogatja ugyanakkor a HTTPS protokoll használatát.

1. Bizalmas adatokat (például jelszavakat vagy hitelkártyaadatokat) csak a https:// előtaggal megnyitott weboldalakon adj meg.

2. Vannak különböző szoftvereszközök, amelyek tudnak abban segíteni, hogy mindig HTTPS-kapcsolatot használj, amikor csak lehetséges.

3. A HTTPS-kapcsolatot a legtöbb böngészőben egy kis lakat vagy hasonló ikon is

jelzi a címsorban.

4. A HTTPS protokoll ugyanakkor még nem jelent garanciát a biztonságra, hiszen rosszindulatú weboldalak is ajánlhatnak ilyen kapcsolatot. A HTTPS a kapcsolat biztonságáért felel csupán, és arról nem mond semmit, hogy maga a webhely jó szándékú-e.

A HTTPS protokoll mögöttes biztonsági megoldásai az SSL (Secure Sockets Layer) és a TLS (Transport Layer Security). Az SSL/TLS digitális titkosítása kulcsok használatára épül, nagyjából a valódi kulcsokhoz hasonlóan. Ha felírnád egy titkodat egy darab papírra, hogy majd később odaadd valamelyik barátodnak, bárki, akinek birtokába kerül ez a papír, elolvashatná a tartalmát. Ehelyett most képzeld el azt, hogy korábban adtál egy kulcsot a barátodnak, és mindig, amikor titkot szeretnél küldeni neki, egy lelakatolt, erős dobozban teszed ezt. Ha valaki máshoz kerülne a dobozod, a megfelelő kulcs nélkül csak nagyon nehezen tudná kinyitni, hogy elolvashassa a titkodat. Ha valaki megpróbálná a dobozt kicserélni egy pont ugyanolyanra, azt meg amiatt vennéd észre, hogy a kulcsod nem illene a doboz lakatjába. Az SSL/TLS titkosítási megoldás ugyanezt alkalmazza a webhelyeknél.

A böngészők biztonsági figyelmeztetései a kiterjesztett ellenőrzésű (EV) tanúsítványokról is közölnek információt. EV-tanúsítványt csak olyan webhely kaphat, amely hitelt érdemlően azonosítja magát egy ún. hitelesítésszolgáltató előtt. A böngészők néha úgy mutatják az EV-tanúsítvány meglétét, hogy a címsorban külön megjelenítik a webhely vagy az üzemeltető szervezet nevét. EV-tanúsítványt csak olyan webhely kaphat, amely hitelt érdemlően azonosítja magát egy ún. hitelesítésszolgáltató előtt. A böngészők néha úgy mutatják az EV-tanúsítvány meglétét, hogy a címsorban külön megjelenítik a webhely vagy az üzemeltető szervezet nevét. Ha bizalmatlan vagy egy webhely tartalmával kapcsolatban, megnézheted, hogy az URL-cím megegyezik-e a tanúsítványban és a böngészőben. Ez a „Tanúsítvány megtekintése” vagy hasonló opcióval lehetséges a különböző böngészőkben. [Ha éppen ki van vetítve tartalom, jó ötlet lehet meg is mutatni, hol érhető el a tanúsítvány ellenőrzése.] A tanúsítvány ellenőrzésének menete kissé eltér az egyes böngészőkben. Chrome böngészőben például a ... ikonra kattintva meg kell nyitni a menüt, majd a „További eszközök” menüpontnál a „Fejlesztői eszközök” lehetőséget kell választani. A „Developer Tools” (Fejlesztői eszközök) „Security” (Biztonság) lapján érhető el a „View certificate” (Tanúsítvány megtekintése) lehetőség.

Ha nem telepítesz és nem futtatsz megbízhatatlan forrásból származó szoftvereket, fontos lépést tettél biztonságod felé. Ugyanakkor nélkülözhetetlen még egy megfelelő vírusvédelmi szoftver is, amely megvédhet a rosszindulatú webhelyek felkeresésétől és a kártevők letöltésétől.

Az adathalászat legfőbb eszköze az e-mail, amikor egy rosszindulatú felhasználó megbízható feladónak mutatja magát. Így próbálja megszerezni a jelszavadat: vagy bekéri e-mailben, vagy átirányít egy hamisított webhelyre, hogy ott add meg, mintha

a valódi webhelyen lennél. A levélszemétszűrők ki tudják szűrni az ilyen e-mailek egy részét. Te is segíthetsz jobbá tenni a levélszemétszűrők működését, ha a beérkezett üzeneteid között landoló minden gyanús e-mailt megjelölsz kéretlen tartalomként.

Kérdezd meg a diákjaidtól!

Hogyan előzheted meg, hogy véletlenül káros tartalmat tölts le számítógépedre?

Mondd el a diákjaidnak!

Ügyelj arra, hogy csak megbízható webhelyekről tölts le bármit is. Légy nagyon óvatos a bizonytalan e-mail-mellékletek megnyitásával, és a felugró ablakokra vagy hibaüzenetekre való rákattintással is. Hasznos lehet egy megbízható kártevőirtó programot is beszerezni és telepíteni.

Jelszavak megosztása

Első rész

Kérdezd meg a diákjaidtól!

Mit gondolsz, mikor lehet jó ötlet jelszavad megosztása valakivel?

1. Egy lehetséges válasz például valamilyen fiók (mondjuk Netflix) közös használata.

Milyen kockázatokkal jár jelszavad megosztása?

1. Ha egy rosszindulatú személy megszerzi jelszavadat, feltörheti a fiókodat. Jelszavad megosztása fokozza ennek kockázatát. Ha más webhelyeken vagy szolgáltatásokban is ugyanezt a jelszót használod, ezekhez is jogosulatlan hozzáférés nyerhető.

Mondd el a diákjaidnak!

Az ajánlott gyakorlat az, hogy a szolgáltatásba szükséges bejelentkezésen kívül senkivel ne oszd meg jelszavadat. Korábban már beszéltünk az adathalászatról, amikor rosszindulatú személyek megtévesztéssel vesznek rá valakit a jelszava megadására.

Olyan is előfordulhat ugyanakkor, hogy valaki egészen nyíltan kéri tőled jelszavad megosztását, arra hivatkozva, hogy fiókod veszélyben lehet. Ezek között lehet jó szándékú is, például egy barátod, aki tényleg valami furcsát látott mondjuk a profilodban, általánosságban mégis az a szabály, hogy ne oszd meg senkivel a jelszavadat, különösen, ha több fiókhoz is ugyanazt használod. Ha valamiért mégis jelszavad megosztására készülsz, ügyelj arra, hogy az ne legyen máshol használva, és jelszókezelőn keresztül kezeld a megosztást.

A jelszavadat elkérők között lehetnek általad jól ismert, megbízható felnőttek, például szüleid, tanáraid vagy a főnököd. Bár ismered őket és megbízol bennük, számodra és számukra is jobb, ha egyidejűleg átbeszélitek, miért kérik ezt, és mit terveznek tenni a megkapott jelszavakkal. A közvetlen családtagjaidon kívüli felnőtteknél egész konkrétan rákérdezhetsz, milyen törvény vagy szabály alapján gondolják, hogy joguk van elkérni a jelszavadat.

Udvariasan, de egyértelműen rákérdezni a jogalapot megteremtő törvényre vagy szabályra különösen fontos a személyesen korábban nem ismert felnőttek, például egy rendőr esetében. Ha egy rendőr vagy más hivatalos személy a közösségimédia-fiókod jelszavát kéri tőled, maradj higgadt és tiszteletteljes. Kérdezz rá, miért kéri

ezt, és milyen törvény vagy szabály alapján gondolja, hogy joga van elkérni tőled ezt az információt.

A helyzettől függően lehet, hogy tényleg jogszerű a kérés, és meg kell mondanod a jelszavadat az azt kérő felnőttnek, aki lehet szülő/gondviselő, tanár, munkaadó, rendőr, hivatalos személy vagy más. Ilyen eset például, ha tényleg van rá törvény vagy szabály, amely miatt eleget kell tegyél a kérésnek, vagy ha saját belátásod szerint úgy véled, nagyobb haszna van, ha most kivételt teszel, mint amekkora kockázatot a jelszó megosztása hordoz.

Ha egy felnőtt a jelszavaid megadására szólít fel, és ettől kényelmetlenül érzed magad, mihamarabb kérd szüleid/gondviselőid vagy más megbízható felnőtt tanácsát, lehetőleg még azelőtt, hogy reagálnál a kérésre.

Kérdezd meg a diákjaidtól!

Milyen esetekben megfelelő a jelszavad megosztása online?

1. Csak akkor add meg online a jelszavadat, amikor az adott webhelyre vagy szolgáltatásba jelentkezel be. A jelszavadat ne oszd meg sehol máshol, például e-mailben sem, ami általában nem titkosított, és így nem biztonságos.

Feladat

Játéklap

Feladat

A résztvevők alkossanak 2-3 fős csoportokat. Oszd ki a „Kéretlen tartalom” résztvevői játéklapot. Minden résztvevő dolgozzon ki egy folyamatábrát, amely sorvezetőként másoknak is segít azonosítani, hogy a kapott üzenet kéretlen/rosszindulatú tartalom-e, és segít eldönteni, hogy megadják-e a kért információt a küldőnek.

Mondd el a diákjaidnak!

Tekintsétek át az összes esetpéldát, és beszéljétek meg, szerintetek kéretlen/rosszindulatú tartalomról van-e szó, és jó ötlet-e megadni a kért információt.

Interakció a leckével

Adj a résztvevőknek 10 percet erre a feladatra. Ezután kérd meg őket, hogy osszák meg megállapításaikat a teljes csoporttal.

Kérdezd meg a diákjaidtól!

Milyen esetekben lehet elfogadható a jelszavad megosztása e-mailben?

Mondd el a diákjaidnak!

A webhelyek és a vállalatok általános gyakorlata az, hogy e-mailben soha nem kérnek be jelszót felhasználóiktól. Soha ne add meg a jelszavadat ilyen módon, még ha a feladó valódinak tűnne is. Az e-mail nem tekinthető biztonságos csatornának.

Második rész

Feladat

A következő egy egyéni feladat lesz, ezért a résztvevők üljenek vissza a csoportokból.

Adj a résztvevőknek 15 percet a folyamatábra megalkotására.

Mondd el a diákjaidnak!

Minden résztvevő dolgozzon ki egy folyamatábrát, amely sorvezetőként másoknak is segít azonosítani, hogy a kapott üzenet kéretlen/rosszindulatú tartalom-e, és segít eldönteni, hogy megadják-e a kért információt a küldőnek. A folyamatábra

megalkotásához hasznos lehet valamelyik kapott esetpéldára támaszkodni (ekkor írd oda az esetpélda sorszámát is a lapra). De választhatsz teljesen saját példát is! Ha saját példára építesz, egy rövid bekezdésben mutasd is be még a folyamatábra előtt.

Adj a résztvevőknek 15 percet a folyamatábra megalkotására.