Nyilvános WiFi

A résztvevők megismerkednek a nyilvános WiFi-hálózatok jellemzőivel, különös tekintettel az előnyökre és a kockázatokra. Megtanulják felismerni a nem biztonságos WiFi-hálózatokat, megértik, milyen adatbiztonsági kompromisszumokat kötnek, amikor mégis csatlakoznak egy nem biztonságos hálózathoz, és képessé válnak tájékozottan dönteni arról, milyen feltételek esetén érdemes vállalni a kockázatokat.

Erőforrások

- Vezeték nélküli modem képe
- A kapcsolat biztonsága játéklap

Mi az a WiFi?

Első rész

Kérdezd meg a diákjaidtól!

Milyen eszközökről szoktál internetezni?

Ezek az eszközök hogyan csatlakoznak az internetre?

Kép használata a leckében

A WiFi az eszközök internetcsatlakozásának elterjedt módja. A WiFi-kapcsolat rádióhullámokon keresztül működik, nem szükséges hozzá kábel vagy más fizikai csatlakozás.

Képzeld el, hogy van otthon három laptop számítógéped, amelyek mindegyikén szeretnél internetkapcsolatot. Ehhez a következőkre lesz szükséged:

1. Egy hozzáférési pont: A hozzáférési pont WiFi-jelet sugároz, és így biztosítja az internet-hozzáférést. A csatlakozáshoz eszközeidnek venniük kell ezeket a jeleket. A hozzáférési pont által biztosított vezeték nélküli kapcsolat használatához néha külön engedély (felhasználónév és jelszó) szükséges.

2. Egy útválasztó: Az útválasztó (más néven router) hálózatba kapcsolja egy adott hely (iskola, könyvtár vagy lakás) összes eszközét (számítógépeket, táblagépeket, mobiltelefonokat). Az útválasztók általában tartalmaznak egy beépített hozzáférési pontot (lásd az ábrát).

> Az útválasztók hatóköre többnyire kicsi. Ezért van az, hogy ha eszközöd messze van az útválasztótól, esetleg csak gyenge WiFi-jelet fog venni, vagy el sem ér hozzá a jel. Szintén csökken a jelerősség, ha valamilyen akadály van az eszköz és az útválasztó között (például egy téglafal vagy egy épületrész).
>
> Az útválasztóhoz csatlakozva hozzáférsz a hálózathoz, de ez még nem elég az internetkapcsolathoz. Az útválasztó csak akkor tudja internetkapcsolattal kiszolgálni a hálózathoz csatlakozó eszközöket, ha közben csatlakozik egy modemhez.

3. Egy modem: A modem kapcsolatot létesít és tart fenn internetszolgáltatóddal, biztosítva számodra az internetkapcsolatot. Ez az eszköz átalakítja a külső forrásból érkező jeleket olyanokká, amelyek értelmezhetők a csatlakozó számítógépek és más digitális eszközök számára.

> Általában a hozzáférési pont és az útválasztó egyetlen eszközbe van integrálva,

és egy speciális kábellel (Ethernet-kábellel) fizikailag csatlakozik a modemhez. Ezt nevezzük vezetékes internetnek.

A mobileszközök vezeték nélküli mobilhálózati kapcsolaton keresztül is csatlakozhatnak az internethez, ha nincs a közelben használható iskolai, nyilvános vagy otthoni hálózat. A mobilhálózati kapcsolat egyfajta vezeték nélküli rádiókapcsolat, amely sokkal nagyobb területet fed le, mint egy útválasztó. A vezeték nélküli kapcsolat különleges vevőberendezéseken, ún. mobilhálózati adótornyokon keresztül terjed, így biztosítva az internetelérést a mobileszközök számára.

Második rész

Kérdezd meg a diákjaidtól!

Mik a WiFi előnyei?

Mik a WiFi főbb hátrányai?

Milyen biztonsági aggályok merülnek fel WiFi-kapcsolat használatakor, amelyekkel vezetékes internetnél nem kell számolni?

Miért szakad meg a WiFi-kapcsolat a mobilodon, ha kimész az épületből?

WiFi-hálózat választása

Első rész

Kérdezd meg a diákjaidtól!

Minden WiFi-hálózat biztonságos? Miért, illetve miért nem?

Mondd el a diákjaidnak!

Néha több WiFi-hálózat közül is választhatsz. Fontos mindig emlékezni arra, hogy egy nem megfelelő hálózathoz csatlakozva komoly kockázatoknak teheted ki magad. A nem biztonságos WiFi-hálózatok nem kérnek például jelszót a bejelentkezéshez. Nem biztonságos hálózaton más felhasználók hozzáférhetnek az adataidhoz. Megszerezhetik például a hálózaton általad küldött vagy fogadott információkat, illetve megfigyelhetik online tevékenységeidet.

A biztonságos és megbízható WiFi-hálózatok nem csupán jelszót kérnek a hozzáféréshez, de titkosítást is működtetnek, és ellenőrizhető, hogy valóban ahhoz a hálózathoz csatlakozol-e, amelynek a nevét megjelenni látod. Lehetséges például, hogy valaki létrehoz egy hálózatot pont ugyanazzal a névvel, mint iskolád hálózatáé, és a gyanútlan felhasználók adatai veszélybe kerülnek ehhez a hálózathoz csatlakozva. A biztonságos és megbízható hálózatok többszörösen is magas szintű védelmet kínálnak.

Egy fontos tényező még a WiFi-hálózat környezete vagy kontextusa is. Ha például éppen moziban ülsz, és a telefonodon WiFi-hálózatot keresve meglátod az iskolai hálózat nevét, okkal gyanakodhatsz, hogy valaki egy csaló hálózatot működtet azonos néven, hogy megszerezze például a gyanútlanul csatlakozó felhasználók jelszavait.

Jelszóval védett WiFi-hálózat konfigurálásához az üzemeltetőnek valamilyen titkosítási protokollt is be kell állítania az útválasztón. Ezek közül a legelterjedtebb a WEP (Wired Equivalent Privacy, azaz vezetékessel egyenértékű biztonság), a WPA (Wi-Fi Protected Access, azaz védett WiFi-hozzáférés) és a WPA2. Titkosítás alkalmazásakor a vezeték nélküli hálózaton keresztül küldött és fogadott minden információ szándékosan összekavarva (közvetlenül nem értelmezhetően) továbbítódik.

A titkosítás roppant módon megnehezíti, hogy egy támadó megfejthesse a hálózaton keresztül küldött adataidat. Az említett összes protokollról (WEP, WPA és WPA2) az derült ki ugyanakkor, hogy nem feltörhetetlenek. Ezért nagyon fontos a biztonságos webhelykapcsolatok megléte is az online kommunikáció során.

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

3. 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.

Mondd el a diákjaidnak!

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. 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 a résztvevőknek, 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.

Kérdezd meg a diákjaidtól!

Mire érdemes odafigyelni, amikor bármilyen új hálózathoz csatlakozol?

1. Lehetséges válaszok többek között: helyszín (a hálózat üzemeltetője), hozzáférés (kik csatlakozhatnak még ugyanahhoz a hálózathoz) és tevékenység (milyen online műveletet szeretnél végezni a hálózathoz csatlakozva).

Ki az otthoni WiFi-hálózat üzemeltetője? Hát az iskolai hálózaté? És egy kávézó WiFi-hálózatáé?

1. Az otthoni WiFi-hálózat üzemeltetői a szüleid/gondviselőid, az iskolaié a helyi és/vagy tankerületi rendszergazdák, míg a kávézó WiFi-jét a kávézó tulajdonosa üzemelteti.

Ismered személyesen ezeket az embereket? Megbízol bennük?

1. Kezdeményezz eszmecserét arról, hogy a résztvevők mennyire bíznak az említett emberekben.

Mondd el a diákjaidnak!

Fontos, hogy ismerd a WiFi-hálózat üzemeltetőjét, és ő megbízható legyen. A hálózat üzemeltetője általában megállapítható az SSID azonosító alapján.

Az SSID (szolgáltatáskészlet-azonosító vagy hálózatnév) az adott WiFi-hálózat neve, amelyet a kapcsolódási kísérletkor látsz. A név általában kiegészül a tulajdonos/üzemeltető adataival és a hálózattal kapcsolatos egyéb tudnivalókkal. Itt sem árt ugyanakkor az óvatosság, hiszen bárki, aki ért hozzá, létrehozhat egy SSID-hálózatnevet. Egy rosszindulatú felhasználó például létrehozhat egy hálózatot pont ugyanazzal az SSID-azonosítóval, mint az iskolai WiFi-hálózaté. Az ismert és megbízhatónak tekintett hálózatnév meghamisítása mögött a felhasználónevek és jelszavak illetéktelen megszerzésének szándéka állhat.

A hálózat üzemeltetőjének ismerete tehát szintén fontos annak megállapításához, hogy megbízhatónak tekintheted-e a hálózatot. Ha egy általad megbízhatónak ítélt személy vagy szervezet üzemelteti, valószínűleg bátrabban fogod használni. Egy ismeretlen hálózathoz ugyanakkor nem javasolt csatlakozni, hiszen nem tudod, ki üzemelteti a szolgáltatáshoz tartozó útválasztót. Minden hálózati forgalom áthalad az útválasztón, és lehet, hogy az üzemeltetője megfigyeli vagy rögzíti a hálózaton továbbított adatokat.

Amikor csatlakozol egy WiFi-hálózathoz, eszközöd először egy más eszközökből álló hálózathoz csatlakozik, és azon a hálózaton keresztül létesít internetkapcsolatot. Mivel az adatcsere a hálózaton keresztül történik, fontos, hogy az ahhoz csatlakozó minden más eszköz is megbízható legyen. Ez olyan mint egy csoportos feladat az

iskolában – fontos, hogy minden résztvevőben meg lehessen bízni!

A hálózat jelszavas védelme korlátozza a csatlakozási lehetőségeket. Ez azt jelenti, hogy a teljesen nyílt hálózatokhoz képest ilyenkor jobban átlátható, ki csatlakozik éppen az adott hálózathoz – otthon, barátoknál vagy éppen a kávézó WiFi-jén.

Hogy egy gyanúsnak tűnő hálózathoz végül csatlakozol-e, az mindig az online biztonság fontosságával kapcsolatos kompromisszumként dől el. Igazából mindig súlyozod annak kockázatát, hogy egy idegen hozzáférhet a személyes adataidhoz vagy jelszavaidhoz, és néha úgy döntesz, az éppen elérhető hálózathoz való azonnali csatlakozás most többet ér meg neked.

Kérdezd meg a diákjaidtól!

Jó ötlet híreket/blogokat olvasni az otthoni WiFi-hálózathoz csatlakozva? Hát az iskolai hálózaton? És egy kávézó WiFi-hálózatán?

1. Magyarázd el, hogy egy webhely tartalmának böngészése általában nem bizalmas információ. Ezt szinte bármilyen hálózathoz csatlakozva nyugodtan meg lehet tenni.

Jó ötlet hitelkártyaadatokat megadni egy weboldalon az otthoni WiFi-hálózathoz csatlakozva? Hát az iskolai hálózaton? És egy kávézó WiFi-hálózatán? Miért?

1. Beszélgessetek arról, miért biztonságos ez az otthoni hálózaton, és miért nem az egy kávézó WiFi-jét használva. Ejtsetek szót arról, hogy bár az iskolai WiFi elég megbízhatónak tekinthető, a banki adatok túl bizalmasak ahhoz, hogy megérje kockáztatni.

Jó ötlet megnézni az e-mailjeidet otthoni WiFi-hálózathoz csatlakozva? Hát az iskolai hálózaton? És egy kávézó WiFi-hálózatán?

1. Beszélgessetek arról, miért biztonságosabb ez az otthoni hálózaton, és mennyire függ a döntés az e-mail-fiók tartalmától is. Sokan használnak például több e-mail-fiókot is (mondjuk egyet a hírlevelekhez/marketingüzenetekhez, egyet pedig a barátokkal és családtagokkal folytatott levelezésre).

Mondd el a diákjaidnak!

A bizalmas adatok, például a jelszavak és a banki adatok küldését/fogadását célszerű az otthoni vagy más megbízható hálózatokra és csak SSL/TLS biztonsági megoldást alkalmazó webhelyekre korlátozni. Nyilvános vagy másokkal közösen használt hálózatokon jobb az óvatosság. Ezek a kényes információk veszélynek vannak kitéve, ha olyankor adod meg vagy éred el őket, amikor egy idegenek által is

használt hálózathoz csatlakozva internetezel.

Az információk bizalmassága nem fekete-fehér, mert személyes adatai védelméről mindenki maga hoz döntést, és hozzáállásunk egyénenként különbözhet. Célszerű minden alkalommal gondosan mérlegelni a konkrét helyzetet, és megfontolás után dönteni arról, csatlakozol-e az adott hálózathoz. A döntés előtt mindig kérdezd meg magadtól, hogy megbízol-e a hálózat üzemeltetőjében és a hálózathoz csatlakozó további személyekben, milyen online tevékenységet tervezel a hálózaton, és milyen adatokat fogsz megosztani.

Biztonságos és nem biztonságos hálózatok

Első rész

Interakció a leckével

Fontos: Ennek a tevékenységnek egy részét már feldolgoztuk a 2. foglalkozáson: „WiFi-hálózat választása”. Saját belátásod szerint dönts arról, hogy érdemes-e újra végigmenni ezen a témán, vagy át lehet most ugrani.

Mondd el a diákjaidnak!

Ahogy korábban már szó volt róla, a nem biztonságos WiFi-hálózatok nem kérnek jelszavas bejelentkezést. A nem biztonságos hálózatokon kockázatok leselkednek az általad küldött és fogadott adatokra.

A biztonságos WiFi-hálózatokon jelszavas védelem és titkosítás működik. A hálózatot beállító személy dönt arról, hogy konfigurálja-e a titkosítás használatát. Titkosítás alkalmazásakor a hálózaton keresztül küldött és fogadott információ szándékosan úgy összekavarva továbbítódik, hogy még az ugyanarra a WiFi-hálózatra csatlakozó hackerek is csak nagyon nehezen tudnák megfejteni.

A biztonságos hálózat nem jelenti egy az egyben azt, hogy adataid biztonságban lennének. Sokkal jobb a helyzet, mint egy nem biztonságos hálózaton, de egy igazán eltökélt támadó valahogy módot találhat arra, hogy hozzáférjen az adataidhoz.

A WiFi-hálózatokon három titkosítási protokoll terjedt el: a WEP (Wired Equivalent Privacy, azaz vezetékessel egyenértékű biztonság), a WPA (Wi-Fi Protected Access, azaz védett WiFi-hozzáférés) és a WPA2. A WEP és a WPA mára elavultnak számít, ezért az ezek valamelyikét használó hálózatok inkább tekintendők nem biztonságosnak. A WPA2 protokollról is kiderült, hogy feltörhető lehet.

Adataid maximális védelméhez az szükséges, hogy a felkeresett webhelyek SSL/TLS-kapcsolattitkosítást használjanak.

Kérdezd meg a diákjaidtól!

Fel tudtok idézni olyan alkalmat, amikor valamilyen jelszóval védett hálózathoz csatlakoztatok?

1. Ez lehet otthoni hálózat, iskolai WiFi vagy nyilvános helyen, például kávézókban működő WiFi-hálózat.

Fel tudtok idézni olyan alkalmat, amikor egy nem biztonságos hálózathoz

csatlakoztatok?

És olyat, amikor biztonságos hálózathoz csatlakoztatok?

Mondd el a diákjaidnak!

A használni kívánt WiFi-hálózat titkosítását ellenőrizhetitek eszközötök hálózati és vezeték nélküli beállításai között.

Második rész

Interakció a leckével

A foglalkozás megkezdése előtt keress rá az interneten, hogy a használt operációs rendszeren hogyan kell a WiFi-hálózat titkosítását ellenőrizni. Ezután mutasd be, hogyan kell ellenőrizni a használt hálózaton alkalmazott titkosítást. MacOS rendszeren például a Rendszerbeállítások -> Hálózat -> Wi-Fi beállítást kell választani, majd rákattintani a hálózat nevére. A Wi-Fi lapon megjelenik az elérhető hálózatok listája, és mindegyiknél szerepel az általa alkalmazott titkosítás is.

Mondd el a diákjaidnak!

Nem minden kapcsolat egyforma. A nem biztonságos hálózatokra bárki csatlakozhat, és nem egyértelmű, ki felügyeli a hálózatot. Ha nem biztonságos hálózathoz csatlakozol, az internetes tevékenységeid esetleg nyomon követhetők lesznek. Ha SSL/TLS-kapcsolattitkosítás nélkül böngészel, bárki, aki ugyanahhoz a hálózathoz csatlakozik, megfigyelheti adatforgalmadat – nemcsak az általad betöltött oldalakat, de például az azokon megadott jelszavaidat is.

Interakció a leckével

A résztvevők technikai felkészültségétől függően beszélhetsz a virtuális magánhálózatokról (VPN) is, bemutatva a WiFi-kapcsolaton keresztüli internetezésnek ezt a kiegészítő biztonsági rétegét. A Források szakaszban találsz néhány hivatkozást, amelyeken a VPN-ről szóló további információ érhető el.

A kapcsolat biztonságának megállapítása

Rész címe

Interakció a leckével

A résztvevők alkossanak 2-3 fős csoportokat. Oszd ki „A kapcsolat biztonsága” résztvevői játéklapot, és adj mindegyik csoportnak egy feldolgozandó esetet. Adj a résztvevőknek 5 percet az eset megvitatására. Ezután kérd meg őket, hogy osszák meg megállapításaikat a teljes csoporttal. A játéklapon zölddel láthatók a válaszok.

Feladat

Első rész

Feladat

Add a résztvevőknek a következő feladatot:

1. Rajzolják meg egy átlagos napjuk idővonalát, és jelöljék be azokat a WiFi-hálózatokat, amelyekhez a különböző napszakokban csatlakozni szoktak.

2. Ezután válasszanak ki két hálózatot ezek közül, és egy rövid bekezdésben mutassák be. Kik csatlakoznak még ahhoz a hálózathoz? Mennyire biztonságos?

3. A két kiválasztott hálózatot mutassák be abból a szempontból is, milyen lehetőségeket jelentenek számukra, és melyek a potenciális kockázataik.