Veřejná síť Wi-Fi

Účastníci lekce se dozví o veřejných sítích Wi-Fi a o výhodách a rizicích, které s připojením přes tyto Wi-Fi souvisejí. Konkrétně se účastníci této lekce naučí rozpoznávat nezabezpečené sítě Wi-Fi, zjistí, jaké kompromisy jsou spjaté s jejich použitím, a v neposlední řadě se naučí informovaně rozhodovat o tom, kdy se k nezabezpečené síti Wi-Fi připojit a použít ji.

Zdroje

Obrázek bezdrátového modemu
Podklady Bezpečnost připojení

Co je Wi-Fi?

1. část

Zeptejte se studentů

Jaká zařízení používáte k přístupu na internet?

Jak se tato zařízení připojují k internetu?

Obrázek aktivity ve třídě

Wi-Fi je běžně využívaný způsob připojení zařízení k internetu. Wi-Fi využívá k připojení zařízení rádiové signály, takže se obejde bez fyzického nebo kabelového připojení.

Představte si, že doma máte tři notebooky, které chcete připojit k internetu. K tomu, abyste to mohli udělat, budete potřebovat následující:

1. Přístupový bod: Přístupový bod (AP) je cokoli, co přenáší (vysílá) signál Wi-Fi a poskytne připojení k internetu. Aby se vaše zařízení mohlo k internetu připojit, musí tento signál zachytit. Někdy je potřeba zvláštní oprávnění (například uživatelské jméno a heslo), abyste se mohli přihlásit a používat bezdrátový signál, který AP vysílá.

2. Router: Router je zařízení, které na určitém místě (třeba ve škole, v knihovně nebo doma) vytváří síť mezi všemi příslušnými zařízeními (jako jsou počítače, tablety nebo mobilní telefony). Obvykle mají routery vestavěný přístupový bod (viz diagram nahoře).

> Routery mají omezený (obvykle krátký) dosah. Proto se může stát, že při přílišném vzdálení vašeho zařízení od routeru se signál Wi-Fi přeruší nebo zeslábne. Také pokud se mezi vás a router dostane nějaká překážka (jako budova nebo zděná zeď), signál se tím omezí.
>
> I když vám připojení k routeru nabízí přístup k síti, nejedná se o přístup k internetu. Aby se mohlo k internetu připojit víc zařízení ze sítě, musí být router připojený k modemu.

3. Modem: Modem je zařízení, které vytváří a udržuje připojení k příslušnému poskytovateli internetových služeb, a tím vám umožňuje přístup k internetu. Převádí signály z místa, které se nachází mimo vaši lokalitu, na signály, které dokáže přečíst váš počítač nebo jiné digitální zařízení.

> Běžně bývá AP i router součástí jednoho zařízení, které je fyzicky připojené k

modemu pomocí ethernetového kabelu. Když se tedy hovoří o „kabelovém“ připojení k internetu, myslí se tím právě zmíněný ethernetový kabel.

Mobilní zařízení můžou k připojení k internetu také využít mobilní připojení, zvlášť pokud se nenachází ve škole, v knihovně nebo domácí síti. Mobilní připojení funguje na principu bezdrátového rádiového signálu, který má mnohem větší oblast pokrytí než router. K tomu, aby se vaše mobilní zařízení mohlo připojit k internetu, využívá mobilní připojení vysílače mobilní sítě.

2. část

Zeptejte se studentů

Jaké výhody má Wi-Fi?

Jaké jsou některé nevýhody Wi-Fi?

Jaká rizika můžou nastat v souvislosti se zabezpečením v případě připojení pomocí Wi-Fi v porovnání s kabelovým připojením k internetu?

Proč dochází při opuštění budovy ke ztrátě přístupu k Wi-Fi na telefonu?

Výběr sítě Wi-Fi

1. část

Zeptejte se studentů

Jsou všechny sítě Wi-Fi bezpečné? Proč ano, případně proč ne?

Řekněte studentům

Někdy si můžete vybrat, kterou síť Wi-Fi chcete použít. Je důležité si uvědomit, že připojit se ke špatné síti může být riskantní. Nezabezpečenou síť Wi-Fi poznáte například tak, že od vás k přihlášení nevyžaduje heslo. Pokud se připojíte k nezabezpečené síti, můžou si její ostatní uživatelé zobrazit vaše informace. Informace, které přes danou síť posíláte, můžou třeba ukrást, nebo můžou sledovat, co děláte.

Zabezpečené a důvěryhodné sítě Wi-Fi jsou naopak ty, které vyžadují heslo a mají zapnuté šifrování. U takových sítí jste si také jistí, že název sítě reprezentuje přesně tu síť, do které se přihlašujete. Pokud se například přihlásíte k síti, která má stejný název jako vaše školní síť, může to vést až k odhalení informací o účtu. Z toho důvodu se za zabezpečené a důvěryhodné sítě považují ty, které nabízejí tu nejvyšší ochranu.

Určitě je třeba zvážit kontext nebo lokalitu příslušné sítě Wi-Fi. Pokud jste například v kině a při hledání sítě Wi-Fi se vám zobrazí název školní sítě, musíte být opatrní a vzít v úvahu možnost, že se může jednat o falešnou školní síť, která se tímto způsobem snaží shromažďovat hesla od nic netušících studentů.

Při nastavování sítě Wi-Fi chráněné heslem musí její vlastník na routeru zapnout šifrovací protokol. Běžné šifrovací protokoly jsou Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) a WPA2. Tyto protokoly zajišťují šifrování (nebo také kódování) informací, které se přes danou síť bezdrátově odesílají.

Účelem šifrování je ztížit hackerům možnost zobrazit si informace, které posíláte. Ovšem u všech zmíněných protokolů (WEP, WPA i WPA2) bylo prokázáno, že jsou pro hackery snadným cílem. Proto je také důležité při přenosu informací na internetu spoléhat na bezpečné webové připojení.

HTTPS je standardní protokol, který používají weby k šifrování dat přenášených přes internet. Šifrování může zabránit tomu, aby si data z vašeho připojení zobrazila jakákoli třetí strana. Poskytuje další vrstvu zabezpečení a dá se použít v jakémkoli prohlížeči. Stačí před příslušnou URL adresu přidat “https://” (například https://www.mojestránka.com). Ovšem ne všechny weby protokol HTTPS podporují.

1. Citlivé informace (jako třeba hesla, údaje o platebních kartách apod.) byste měli

zadávat jenom na weby s předponou HTTPS://.

2. Většina hlavních prohlížečů má bezpečnostní indikátor vedle adresního řádku. Má podobu symbolu zámku a označuje, že se jedná o zabezpečené připojení HTTPS.

3. Ovšem bohužel ani protokol HTTPS nezaručuje bezpečnost, protože ho podporují i některé škodlivé weby. Protokol HTTPS zabezpečuje připojení samotné, ale nemůže zaručit, že se jedná o poctivý web.

Řekněte studentům

Technologie s názvem Secure Sockets Layer (SSL) a Transport Layer Security (TLS) poskytují zabezpečení HTTPS. Protokoly SSL a TLS používají digitální šifrovací klíče, které fungují podobně jako skutečné klíče. Pokud byste kamarádovi napsali na papír nějaké tajemství, mohl by si ho přečíst každý, kdo papír najde. Představte si, že místo toho kamarádovi osobně předáte kopii klíče a potom své tajemství pošlete v zamčené krabici, která se dá tímto klíčem odemknout. Pokud by se krabice dostala do rukou někomu jinému, bylo by pro daného člověka těžké se k tajemství dostat, protože by neměl klíč. A pokud by se někdo pokusil vaši krabici vyměnit za podobnou, všimli byste si, že není vaše, protože by do ní nepasoval váš klíč. Protokoly SSL a TLS fungují na stejném principu, ale na webu.

Indikátory zabezpečení prohlížeče budou také poskytovat informace o certifikátu rozšířeného ověření (EV). EV certifikáty dostanou weby, které svoji identitu ověří u certifikační autority. V prohlížečích má někdy indikátor rozšířeného ověření podobu názvu webu nebo registrujícího subjektu a najdeme ho vedle adresního řádku prohlížeče. Pokud nemáte důvěru k obsahu určitého webu, můžete zkontrolovat, jestli URL adresa v certifikátu odpovídá URL adrese v prohlížeči. Stačí kliknout na tlačítko „Zobrazit certifikát“. [Může být užitečné účastníkům na projekčním plátně ukázat, jak možnost „Zobrazit certifikát“ najít. Jak se k této možnosti dostanete, závisí na tom, jaký prohlížeč používáte. Například v prohlížeči Chrome u možnosti „Zobrazit“ klikněte na „Vývojář“ a pak na „Nástroje pro vývojáře“. V části „Nástroje pro vývojáře“ klikněte na kartu „Zabezpečení“ a pak na „Zobrazit certifikát“.

Zeptejte se studentů

Na co byste měli myslet, když se připojujete k nové síti?

1. Možné odpovědi: na lokalitu (kdo příslušnou síť vlastní), přístup (kdo další je k síti připojený) a aktivitu (co na síti děláte).

Kdo vlastní vaši domácí síť Wi-Fi? Kdo vlastní tu školní? A kdo tu v kavárně?

1. Vaši domácí síť Wi-Fi vlastní vaši rodiče nebo opatrovníci, vaši školní síť vlastní

správci nebo město a síť v kavárně vlastní její majitel.

Znáte tyto lidi osobně? Věříte jim?

1. Zapojte účastníky do diskuse, ve které se zamyslí nad tím, jak moc těmto lidem důvěřují.

Řekněte studentům

Hostitele sítě Wi-Fi byste měli znát a důvěřovat mu. Někdy můžete majitele sítě určit pomocí identifikátoru bezdrátové sítě SSID.

Identifikátor bezdrátové sítě SSID je název sítě Wi-Fi, který se vám zobrazí při připojování. Identifikátor SSID se často používá k označení vlastníka sítě a dalších podrobností o síti. Buďte ale na pozoru, protože skoro každý, kdo ví, jak na to, si může SSID vytvořit. Někdo si například může vytvořit identifikátor SSID, který bude stejný jako ten, který používáte ve škole. V tomto příkladě se jedná o situaci, kdy někdo svoji síť vydává za známou a důvěryhodnou, aby tak získal uživatelská jména a hesla.

Ovšem pokud znáte hostitele sítě, může vám to pomoct určit, zda se jedná o bezpečnou síť. Pokud daná síť patří osobě nebo organizaci, které věříte, pak se k ní pravděpodobně nebudete bát připojit. Ovšem pokud jde o neznámou síť, neměli byste se k ní vůbec připojovat. Je to proto, že nevíte, kdo vlastní router, ke kterému se připojujete. Vzhledem k tomu, že veškerá komunikace na síti prochází routerem, může jeho majitel sledovat nebo zaznamenávat, jaké weby navštěvujete.

Když se připojíte k Wi-Fi, vaše zařízení se připojí k místní síti, ke které jsou připojená i ostatní zařízeními, a tato síť se připojí k internetu. Vzhledem k tomu, že si vaše zařízení s danou sítí vyměňuje informace, je důležité, abyste všem ostatním zařízením na této síti důvěřovali. Funguje to stejně jako skupinová práce ve škole. Pokud s nějakými lidmi pracujete na určitém projektu, musíte jim věřit.

Dobrým způsobem zabezpečení sítě je opatřit ji heslem. Tím se omezí množství lidí, kteří se k síti můžou připojit. Navíc díky tomu budete mít lepší přehled o tom, kdo je na síti – ať už se jedná o rodinu, přátele, nebo ostatní zákazníky kavárny – než kdyby byla síť úplně nezabezpečená.

To, jestli se rozhodnete připojit k síti, které zcela nedůvěřujete, bude záležet na kompromisech, ke kterým jste ochotní přistoupit, pokud jde o online bezpečnost. Měli byste zvážit, jestli jste ochotní obětovat narušení bezpečnosti na vašem účtu, ke kterému může potenciálně dojít, výměnou za pohodlí, které vám poskytne možnost připojit se k dostupné síti.

Zeptejte se studentů

Můžete si číst online zpravodajství nebo blog, když jste připojení k Wi-Fi doma? Ve škole? V kavárně?

1. Vysvětlete, že obsah webové stránky se všeobecně nepovažuje za citlivou informaci. Pravděpodobně bude bezpečné si podobné weby číst, i když budete připojení k jakékoli síti.

Můžete někomu poslat číslo platební karty, když jste připojení k Wi-Fi doma? Ve škole? V kavárně? Proč?

1. Zapojte účastníky do diskuze o tom, proč je nejbezpečnější to udělat, když budou připojení k Wi-Fi doma, ale ne například v kavárně. Také proberte, proč se nevyplatí riskovat a použít k tomuto účelu školní síť (i když je pravděpodobně důvěryhodná), a zdůrazněte, že se jedná o velmi citlivou informaci.

Můžete si zkontrolovat osobní e-mail, když jste připojení k Wi-Fi doma? Ve škole? V kavárně?

1. Prostřednictvím diskuze dojděte k závěru, že je pravděpodobně nejbezpečnější si e-mail kontrolovat na domácí síti. Bude ale záležet i na tom, jaký obsah se na vašem e-mailu nachází. Někteří lidé mají například víc e-mailových účtů, které jim slouží k různým účelům (jeden účet mají třeba jen pro účely marketingu nebo propagace a druhý používají ke komunikaci s přáteli a rodinou).

Řekněte studentům

Citlivé informace, jako jsou třeba hesla nebo informace o bankovních účtech, je nejbezpečnější posílat nebo si prohlížet na zabezpečené soukromé síti a na webech využívajících protokoly SSL nebo TLS, ale ne na sdílené veřejné síti. Pokud k citlivým soukromým informacím přistupujete ze sdílené sítě, kterou používají lidé, které neznáte nebo kterým nevěříte, nebo tyto informace z takové sítě odesíláte, vystavujete své informace riziku.

Nemusíte si vždy být jistí tím, jestli jsou vaše informace citlivé, nebo ne. Soukromí totiž každý člověk vnímá trochu jinak a jen vy rozhodujete o tom, které informace budete považovat za citlivé. Je důležité zvážit každou situaci individuálně a rozhodnout se, jestli se vám vyplatí se k dané síti připojit. Předtím, než se rozhodnete, jestli se k dané síti připojit, zeptejte se sami sebe, jestli důvěřujete vlastníkovi sítě a ostatním lidem, kteří jsou k ní připojení. Rozhodujte se také podle aktivity, kterou na internetu chcete provést, a podle toho, jaké informace budete sdílet.

Zabezpečené a nezabezpečené sítě

1. část

Interakce ve třídě

Poznámka: část obsahu v rámci této aktivity už byla probraná v aktivitě číslo 2 s názvem „Výběr sítě Wi-Fi“. Necháváme zcela na vás, zda budete chtít tento materiál projít znovu, nebo zda ho přeskočíte.

Řekněte studentům

Jak už jsme zmínili dřív, nezabezpečená síť Wi-Fi od vás k přihlášení nevyžaduje heslo. Použití nezabezpečených sítí představuje riziko pro všechna data, která v rámci dané sítě odesíláte a přijímáte.

Zabezpečené sítě Wi-Fi jsou ty, které k přihlášení vyžadují heslo a mají zapnuté šifrování. Člověk, který danou síť nakonfiguruje, také rozhoduje o tom, zda zapne šifrování. Šifrování kóduje informace, které v dané síti odesíláte a přijímáte. Z toho důvodu je pro hackery v rámci stejné sítě Wi-Fi mnohem obtížnější se k vašim informacím dostat.

To, že je určitá síť zabezpečená, nezaručuje, že jsou vaše data v bezpečí. Rozhodně je to bezpečnější než použít nezabezpečenou síť, ale i tak může šikovný hacker najít způsob, jak se dostat k vašim informacím.

Sítě Wi-Fi využívají tři běžné šifrovací protokoly: Jsou to Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) a WPA2. WEP a WPA jsou zastaralé protokoly a sítě, které se na ně spoléhají, by měly být považované za nezabezpečené. Navíc se ukázalo, že protokol WPA2 je také pro hackery snadným cílem.

Pokud chcete zajistit, aby byly vaše informace maximálně chráněné, zkontrolujte, že weby, které používáte, jsou zašifrované pomocí protokolů SSL nebo TLS.

Zeptejte se studentů

Dokáže někdo z účastníků uvést příklad sítě, kterou použil a která je chráněná heslem?

1. Mezi takové příklady budou patřit například jejich domácí sítě Wi-Fi, školní síť Wi-Fi nebo Wi-Fi na některých veřejných místech, jako je například kavárna.

Dokáže někdo z účastníků uvést příklad nezabezpečené sítě, kterou někdy použil?

A dokáže někdo uvést příklad zabezpečené sítě?

Řekněte studentům

To, jestli je síť Wi-Fi šifrovaná, se dá zjistit tak, že prozkoumáte danou síť nebo bezdrátová nastavení ve svém zařízení.

2. část

Interakce ve třídě

Teď bude následovat praktické cvičení. Ale ještě předtím proveďte na internetu průzkum a zjistěte, jak u jednotlivých operačních systémů zkontrolovat typ šifrování sítě Wi-Fi. Pak předveďte, jak zjistit, jaký druh šifrování používá příslušná síť. Například v operačním systému macOS klikněte na Předvolby systému -> Síť -> Vybrat Wi-Fi -> zvolte příslušný název sítě. Na kartě Wi-Fi se zobrazí seznam známých sítí a sloupec, ve kterém je uvedený typ šifrování.

Řekněte studentům

Každé připojení je jiné. Když je síť nezabezpečená, může se k ní připojit kdokoli. Navíc není jasné, kdo ji spravuje. Připojením k nezabezpečené síti se vystavujete riziku. Důvodem je to, že pokud nepoužíváte připojení využívající protokol SSL nebo TLS, mohl by si informace, které přijímáte a odesíláte (jako například informace o vámi prohlížených webech, tj. konkrétní stránky, hesla atd.) v rámci sítě zobrazit kdokoli.

Interakce ve třídě

V závislosti na technických znalostech účastníků lekce můžete probrat použití virtuální privátní sítě (VPN), která slouží jako další vrstva zabezpečení při používání Wi-Fi. Další informace najdete v oddílu Zdroje, v části zaměřené na připojení k VPN.

Jak rozpoznat bezpečné připojení

Název části

Interakce ve třídě

Rozdělte účastníky do skupin po dvou až třech. Rozdejte jim podklady zaměřené na bezpečnost připojení a každé skupině přiřaďte jednu situaci. Dejte účastníkům 5 minut na to, aby dané situace prodiskutovali. Potom skupiny požádejte o to, aby své poznatky sdílely s ostatními. Odpovědi jsou v podkladech vyznačené zeleně.

Zadání

1. část

Zadání

Požádejte účastníky, aby udělali následující:

1. Nejprve by měli nakreslit časovou osu svého běžného dne a vyznačit do ní sítě Wi-Fi, ke kterým se během tohoto dne připojují.

2. Ze sítí zobrazených na časové ose by měli účastníci vybrat dvě a potom každou z nich v krátkém odstavci popsat. Požádejte je, aby se vyjádřili k tomu, kdo další je k síti připojený. Nebo jak bezpečná daná síť je.

3. Kromě toho by měli účastníci popsat, jaké výhody skýtá připojení ke zmíněným dvěma sítím a jaká se s nimi naopak pojí rizika.