Offentligt wifi-nätverk

Deltagarna kommer att lära sig om offentliga wifi-nätverk samt deras fördelar och risker. De kommer i synnerhet att lära sig känna igen osäkra wifi-nätverk när de är tillgängliga, förstå för- och nackdelar som osäkra wifi-nätverk medför och ta välgrundade beslut om tillfällen för att ansluta till och använda osäkra wifi-nätverk.

Resurser

- Bild av trådlöst modem
- Material för utdelning om anslutningssäkerhet

Vad är wifi?

Del ett

Fråga dina elever

Vilka enheter använder ni för att komma ut på internet?

Hur ansluts de enheterna till internet?

Bild för kursinteraktion

Wifi är ett vanligt sätt att ansluta enheter till internet på. Wifi använder radiosignaler för att ansluta enheter utan fysisk eller kabelansluten uppkoppling.

Föreställ dig att du har tre bärbara datorer hemma som du vill ansluta till internet. För att göra det behöver du följande:

1. En åtkomstpunkt: En åtkomstpunkt är allt som sänder en Wifi-signal och ger tillgång till internet. Dina enheter måste fånga upp signalerna för att anslutas till internet. Ibland behöver du särskild behörighet (t.ex. ett användarnamn och lösenord) för att logga in och använda den trådlösa signalen som en åtkomstpunkt sänder.

2. En router: En router är en enhet som bildar ett nätverk mellan alla enheter (t.ex. datorer, surfplattor och mobiltelefoner) på en viss plats (t.ex. skola, bibliotek eller hemma). Vanligtvis har routrar en inbyggd åtkomstpunkt (se diagrammet ovan).

> Routrar har en begränsad (vanligtvis kort) räckvidd. Det är därför du får en svag eller utebliven wifi-signal om din enhet befinner sig för långt bort från routern. Om något befinner sig mellan dig och routern (t.ex. en byggnad eller mur) kommer även det att sänka din signal.
>
> Även om det går att komma in på ett nätverk genom att ansluta till en router innebär det inte tillgång till internet. För att flera enheter på ett nätverk ska kunna anslutas till internet måste en router vara ansluten till ett modem.

3. Ett modem: Ett modem är en enhet som skapar och upprätthåller en anslutning till din internetleverantör så att du får tillgång till internet. Det konverterar signaler som kommer utifrån din plats till signaler som datorn och andra digitala enheter kan läsa av.

> I en vanlig konfiguration är åtkomstpunkten och routern en enda enheten som vanligtvis är ansluten till modemet med hjälp av en sladd som kallas Ethernet-sladd. Det är vad personer menar med en ”kabelansluten” internetuppkoppling.

Mobilenheter kan även använda en mobilanslutning för att ansluta till internet, i synnerhet om de inte befinner sig i ett nätverk på en skola, ett bibliotek eller hemma. Mobilanslutningar är en typ av trådlös radiosignal som har mycket större täckningsområde än en router. Mobilanslutningar använder särskilda sändtagare, som kallas mobilmaster, så att din mobilenhet kan anslutas till internet.

Del två

Fråga dina elever

Vilka är fördelarna med wifi?

Vad finns det för nackdelar med wifi?

Vilka säkerhetsproblem kan förekomma vid användning av wifi kontra en kabelansluten internetuppkoppling.

Varför går tillgången till wifi förlorad på din telefon när du går ut från en byggnad?

Välja ett wifi-nätverk

Del ett

Fråga dina elever

Är alla wifi-nätverk säkra? Varför/varför inte?

Berätta för dina elever

Ibland får du välja vilket wifi-nätverk som du vill använda. Det är viktigt att komma ihåg att det finns allvarliga risker om du ansluter dig till fel nätverk. Osäkra wifi-nätverk är exempelvis sådana som inte kräver något lösenord för att logga in på. Om du är ansluten till ett osäkert nätverk kan andra personer på samma nätverk se din information. De kan stjäla information som du sänder över nätverket eller bevaka det du gör.

Å andra sidan är säkra och tillförlitliga nätverk sådana som kräver ett lösenord, har aktiverad kryptering och sådana där du kan vara säker på att nätverket du är ansluten till är det som dess namn utger sig för att vara. Att exempelvis logga in på ett nätverk som utger sig för att vara din skolas nätverk kan leda till att kontoinformation avslöjas. Nätverk som är säkra och tillförlitliga är sådana som därför ger mest skydd.

Något att ta hänsyn till är wifi-nätverkets sammanhang eller plats. Om du exempelvis är på bio och ser din skolas nätverksnamn på din telefon när du letar efter en wifi-anslutning bör du överväga huruvida det nätverket försöker imitera eller ”blåsa” din skolas nätverk för att samla in lösenord från ovetande elever.

När ägaren konfigurerar ett lösenordsskyddat wifi-nätverk måste den personen välja att aktivera routerns krypteringsprotokoll. Vanliga krypteringsprotokoll är WEP (Wired Equivalent Privacy), Wi-fi Protected Access (WPA) eller WPA2. Protokollen gör att informationen som sänds trådlöst över nätverket krypteras (eller ”förvrängs”).

Kryptering har skapats för att göra det svårare för hackare att se vad du skickar. Alla av de protokollen (WEP, WPA och WPA2) har däremot visat sig vara sårbara för hacking. Det är därför viktigt att också anförtro sig till säkra webbanslutningar när information sänds online.

HTTPS är en standard som används av webbplatser för att kryptera data som skickas över internet. Krypteringen kan förhindra tredje parter från att enkelt se data från din anslutning. Den tillför ett extra säkerhetslager och kan användas i alla webbläsare genom att lägga till ”https://” före webbadressen som du går in på (t.ex. https://www.mysite.com). Alla webbplatser har däremot inte stöd för HTTPS.

1. Du bör endast ange känslig information (t.ex. lösenord och kreditkortsuppgifter)

på webbplatser med prefixet HTTPS.

2. De flesta vanliga webbläsarna har säkerhetsindikatorer som ser ut som lås nära adressfältet för att visa HTTPS-anslutningar.

3. HTTPS garanterar tyvärr inte att du är säker, eftersom vissa skadliga webbplatser också kan ha stöd för HTTPS. HTTPS säkrar anslutningen men garanterar inte att webbplatsen är en godartad aktör.

Berätta för dina elever

SSL (Secure Sockets Layer)/TLS (Transport Layer Security) är namn på teknik som håller HTTPS säkert. SSL/TLS använder digitala krypteringsnycklar som ungefär fungerar riktiga nycklar. Om du har skrivit ner en hemlighet på papper åt din vän kan alla som hittar lappen se din hemlighet. Tänk dig istället att du gav din vän en kopia av en nyckel personligen och sedan skickade dina hemligheter i likadana låsta lådor. Om någon hade fått tag på lådan hade personen haft svårt att se din hemlighet utan nyckeln. Om någon hade försökt byta ut lådan mot en liknande låda hade det märkts att din nyckel inte hade passat. SSL/TLS fungerar på samma sätt, fast med en webbplats.

Webbläsares säkerhetsindikatorer kommer även att förmedla information om EV-certifikat (Extended Validation). EV-certifikat delas ut till webbplatser som verifierar deras identitet för certifikatbehöriget. I webbläsare kan EV-indikatorn ibland se ut som webbplatsens namn eller registreringsenheten bredvid adressfältet. Om du är misstänksam till innehållet på en viss webbplats kan du se om webbadressen i certifikatet stämmer överens med webbadressen i webbläsaren genom att klicka på ”Visa certifikat”. [Det kan vara praktiskt på skärmen att visa deltagarna du de hittar ”Visa certifikat”. Hur du visar det beror på webbläsaren. I Chrome går du exempelvis till ”Visa” och klicka på ”Utvecklare” och sedan på ”Utvecklarverktyg”. På ”Utvecklarverktyg” klickar du på fliken ”Säkerhet” och sedan på ”Visa certifikat”.

Fråga dina elever

Vad bör man tänka på när man ansluter till ett nytt nätverk?

1. Möjliga svar omfattar: plats (eller personen som äger nätverket), tillgång (eller vilka fler som är anslutna till nätverk) och aktivitet (eller vad du gör på nätverket).

Vem äger ditt wifi-nätverk hemma? I skolan? På ett kafé?

1. Dina föräldrar/vårdnadshavare äger ditt wifi-nätverk hemma, administratörerna och/eller distriktet äger nätverket i skolan och ägaren äger nätverket på kaféer.

Känner du dem personligen? Litar du på de personerna?

1. Få deltagarna att diskutera om hur de kan lita på de personerna på olika sätt.

Berätta för dina elever

Du bör känna och lita på personen som är värd för wifi-nätverket. Ibland går det att avgöra vem ägaren som använder nätverkets SSID är.

SSID (Service Set Identifier) är benämningen på ett wifi-nätverk som du kan se när du försöker ansluta. SSID används ofta för att förmedla vem som äger nätverk och andra detaljer om nätverket. Var dock försiktig eftersom nästan alla (som vet hur man gör) kan skapa ett SSID. Någon kan exempelvis skapa ett SSID som är identiskt med det som du använder i skolan. Det här är ett exempel på förfalskning av ett känt och tillförlitligt nätverk för att potentiellt samla in användarnamn och lösenord.

Att veta vem som är värd för nätverket kan hjälpa dig att fastställa om nätverket är säkert. Om det tillhör en person eller organisation som du litar på kommer det förmodligen kännas tryggt att ansluta till det. Om det däremot är ett okänt nätverk bör du inte ansluta dig, eftersom du inte vet vem som äger routern som du ansluter till. Eftersom all trafik på nätverket går via routern kan ägaren bevaka eller registrera din webbtrafik.

När du ansluter till wifi ansluts din enhet till ett lokalt enhetsnätverk, och det nätverket ansluter till hela internet. Eftersom din enhet byter information med nätverket är det viktigt att lita på de andra enheterna som du är ansluten till, och det innebär alla enheter på nätverket. Det är precis som grupparbete i skolan. Man vill kunna lita på de andra personerna man jobbar med.

Att använda ett lösenord på nätverket kan begränsa vilka som kan ansluta till nätverket. Det innebär att du får en bättre uppfattning om vilka som befinner sig på nätverket, dvs. om det är familj, vänner eller andra gäster på ett kafé, än om nätverk hade varit fullständigt öppet.

Huruvida du bestämmer dig för att ansluta till ett nätverk som kan verka misstänkt hänger på för- och nackdelarna du är villig att ta när det gäller säkerhet online. Du kan fråga dig själv: Hur bör jag väga risken för att mitt konto får inbrott mot bekvämligheten med ansluta till ett tillgängligt nätverk?

Fråga dina elever

Bör man läsa nyheter online/en blogg med ditt wifi-nätverk hemma? I skolan? På ett kafé?

1. Förklara att innehållet på en webbplats i allmänhet inte är känslig information.

Du kan förmodligen göra det på vilket nätverk som helst.

Bör du skicka ett kreditkortsnummer via ditt wifi-nätverk hemma? I skolan? På ett kafé? Varför?

1. Be deltagarna att diskutera varför det är säkrast att göra det med wifi-nätverket hemma och inte wifi-nätverket på kafé? Diskutera även att det kanske inte är värt risken att använda en skolas nätverk eftersom just den informationen är mycket känslig, trots att en skolas nätverk förmodligen är säkert.

Bör du läsa din personliga e-post med ditt wifi-nätverk hemma? I skolan? På ett kafé?

1. Diskutera hur det förmodligen är säkrast att göra det med deras hemnätverk, beroende på innehållet på e-postkontot. Vissa personer har exempelvis flera e-postkonton som de använder i olika avseenden (t.ex. ett e-postkonto för marknadsföring/kampanjer och ett annat e-postkonto för vänner och familj).

Berätta för dina elever

Känslig information, bland annat lösenord och bankuppgifter, är bättre att skicka/läsa på ett privat och säkert nätverk och på webbplatser med SSL/TLS, istället för på ett delat offentligt nätverk. Den privata informationen äventyras om du skickar eller öppnar den på ett delat nätverk som används av personer du inte känner eller litar på.

Det kanske inte är tydligt hur känslig eller okänslig information är eftersom sekretess är ett personligt beslut som du måste ta själv. Det är viktigt att bedöma varje enskild situation för att fastställa huruvida du bör ansluta till nätverket eller inte. Fråga dig själv om du litar på nätverkets ägare, andra som är anslutna till det, vilken aktivitet du ägnar dig åt online och vilken information du delar, innan du bestämmer dig för att ansluta eller inte.

Säkra och osäkra nätverk

Del ett

Kursinteraktion

Obs! En del av innehållet i den här aktiviteten har diskuterats i ”Aktivitet 2: Att välja ett wifi-nätverk.” Vi litar på ditt omdöme när det gäller huruvida du vill gå igenom det här materialet igen eller hoppa över det.

Berätta för dina elever

Osäkra wifi-nätverk är som sagt sådana som inte kräver något lösenord för att logga in på. Att använda osäkra nätverk utgör en risk för de data du sänder och tar emot över nätverket.

Säkra wifi-nätverk är sådan som kräver ett lösenord och har en aktiverad kryptering. Personen som konfigurerade nätverket är den som väljer huruvida krypteringen aktiveras eller inte. Krypteringen förvränger informationen som du skickar och tar emot över ett nätverk, så att det blir mycket svårare för en hackare på samma wifi-nätverk att se vad du skickar eller tar emot.

Bara för att ett nätverk är säkert betyder inte att dina data är säkra. Det är betydligt säkrare än att använda ett osäkert nätverk. Men en beslutsam hackare kan ändå hitta ett sätt att få tillgång till din information på.

Det finns tre vanliga krypteringsprotokoll för wifi-nätverk: De är WEP (Wired Equivalent Privacy), Wi-fi Protected Access (WPA) eller WPA2. WEP och WPA är föråldrade, och nätverk som bygger på de protokollen bör anses vara osäkra. WPA2 har dessutom visat sig vara sårbara för hacking.

För att kontrollera att din information skyddas i största möjliga utsträckning bör du se till att de webbplatser du använder är krypterade med SSL/TLS.

Fråga dina elever

Kan någon komma på ett exempel på ett lösenordsskyddat nätverk som ni har använt?

1. Vissa exempel omfattar deras wifi hemma, en skolas wifi och wifi-nätverk på offentliga platser som kaféer.

Kan någon komma på ett exempel på ett osäkert nätverk som ni har använt?

Har ni några exempel på ett säkert nätverk?

Berätta för dina elever

Du kan kontrollera huruvida ett wifi-nätverk är krypterat genom att granska nätverksinställningarna eller inställningarna för trådlösa anslutningar på din enhet.

Del två

Kursinteraktion

Före det här inlärningsmomentet ska du göra en internetsökning för att gå igenom hur man kontrollerar typer av wifi-nätverkskryptering för olika operativsystem. Visa sedan hur man tar reda på vilken typ av kryptering ett nätverk använder. På MacOS klickar du exempelvis på Systeminställningar -> Nätverk -> Välj wifi -> Välj lämpligt nätverksnamn. Under fliken Wifi finns en lista över kända nätverk och en spalt som visar vilken krypteringstyp som används.

Berätta för dina elever

Alla anslutningar är inte likadana. När ett nätverk är osäkert kan vem som helst ansluta till nätverket, och det är oklart vem som kontrollerar nätverket. Att ansluta sig till ett osäkert nätverk gör dig sårbar eftersom informationen som du sänder och tar emot, t.ex. din webbtrafik (bland annat sidor och lösenord), potentiellt kan ses av någon på nätverket om du inte använder en SSL-/TLS-anslutning.

Kursinteraktion

Beroende på dina deltagares tekniska kunskaper bör ni eventuellt diskutera användningen av virtuella privata nätverk (VPN) som ett extra säkerhetslager vid användning av Wifi. Gå in på VPN-länkarna i avsnittet Resurser för mer information.

Att känna igen en säker anslutning

Titel

Kursinteraktion

Dela in deltagarna i grupper om 2–3. Dela ut Anslutningssäkerhet: Dela ut deltagarnas material och tilldela var och en av grupperna ett scenario. Ge deltagarna 5 minuter att diskutera sina scenarion. Be sedan grupperna att dela med sig av sina svar. Svaren står i grönt i det utdelade materialet.

Uppgift

Del ett

Uppgift

Be deltagarna att:

1. Rita en tidslinje av en vanlig dag där de markerar wifi-nätverken som de ansluter sig till.

2. Be deltagarna bland de valda, uppritade nätverken på tidslinjen att välja ut två och i ett kort stycke för vart och ett av nätverken beskriva nätverket. Vilka fler är anslutna till nätverket? Hur säkert är det?

3. För de två valda nätverken ska du även be deltagarna beskriva vilka möjligheter och risker som en anslutning till de nätverken eventuellt medför.