Cybersäkerhet, nätfiske och spam

Deltagarna kommer att lära sig om skadliga internetanvändare som kan försöka utnyttja säkerhetsluckor för att samla information om deltagarna. Deltagarna kommer att kunna beskriva riskerna med att vara online, utveckla strategier för att bete sig på ett säkrare sätt, identifiera spam-meddelanden och förklara vilka som bör be om deras lösenord.

Material

- Material för utdelning om spam

Risker online

Del ett

Berätta för dina elever

När du använder internet kan du utsätta dig själv för risker genom att bara gå in på en webbsida, kommunicera online eller ladda ner data. Ibland kan webbplatser du går in på, personer i samma nätverk eller till och med tredjeparter få reda på din plats eller annan information om dig när du surfar.

Fråga dina elever

Vilka kan utnyttja säkerhetssvagheter online och se dina personuppgifter?

1. Tänkbara svar omfattar bland annat skadliga hackare och statlig övervakning.

Berätta för dina elever

När du surfar på nätet kan skadliga hackare samla in data om dig på samma sätt som internetleverantörer. För att minska riskerna måste du använda en säker anslutning mellan dig och webbplatserna du försöker gå in på. Oavsett din anslutning försöker många webbplatser spåra dina användningsmönster på fler plattformar. De kan se vad du har för webbläsare, plats och andra användningsmönster för att ta reda på vem du är.

Fråga dina elever

Varför kan skadliga hackare komma åt din information online? Vilken information letar personer efter? Varför skulle en webbplats där du inte är inloggad på vilja hålla koll på vem du är?

1. All personligt identifierbar information och information som kan säljas eller användas för ekonomisk vinning.

Vet någon vad en skadlig programvara är? Vad kan den göra?

Berätta för dina elever

En skadlig programvara är en hotfull kod som i hemlighet körs på din dator. En del skadliga program kan samla in data från vilken del som helst av din lokala dator, från din hårddisk till dina webbläsardata. De kan även låta hackare kontrollera din dator och använda den som de vill. De flesta skadliga program är däremot enklare, t.ex. webbplatser som utger sig för att vara säkra portaler som banker eller filtillägg som

placerar annonser i din webbläsare för att tjäna pengar.

Fråga dina elever

Vad kan du göra för att skydda dig mot skadliga program, spionage eller spårning?

Berätta för dina elever

Var försiktig när du klickar på länkar, annonser eller inlägg på sociala medier. Stämmer webbadressen överens med den du hade förväntat dig? Får du upp samma sida när du skriver in den själv eller söker efter webbplatsen? En bra regel är att SSL/TLS bör skydda inloggningssidor för ett viktigt konto (som Google, Facebook, Twitter eller bankkonton). SSL/TLS gör det väldigt svårt för en hackare på samma nätverk att skicka dig en falsk webbplats om du skriver in rätt webbadress, vilket annars hade kunnat vara väldigt enkelt.

Vissa webbplatser kommer att kunna köra koder för att nå din personuppgifter eller dina onlinekonton, om de plattformarna begår ett kodningsmisstag. De kan sedan använda dina konton för att skicka spam till andra.

Du bör endast ladda ner och installera program från tillförlitliga källor och vara noggrann när du laddar ner programfiler (filtilläggen .exe, .pkg, .sh, .dll eller .dmg). Programfiler är allt som kör en åtgärd. Ibland kan de leda till dåliga åtgärder. Någon kan exempelvis kan skriva en programfilstext för att radera någons hårddisk eller installera en falsk webbläsare. Därför bör du endast installera innehåll från tillförlitliga källor.

Du kan använda antivirusprogram för att förhindra att du köra skadliga program. Vissa antivirusprogram ingår med din dator (t.ex. Microsoft Security Essentials för Windows), och vissa operativsystem, t.ex. system på Apple-datorer, har säkerhetsinställningar som blockerar program från otillförlitliga källor från att installeras. Därför bör du noggrant tänka efter innan du kringgår de inställningarna.

Du kan även överväga att webbläsartillägg exempelvis kan blockera insticksprogram som gör det svårare för webbplatser att ta reda på vem du är eller spåra dig. Samma insticksprogram kan däremot blockera webbplatsers drift, till exempel möjligheten att titta på videor. Huruvida du bestämmer dig för att installera webbläsartillägg hänger på dina inställningar samt för- och nackdelarna du är villig att ta när det gäller säkerhet online. Du kan fundera på frågor som: ”Hur obekvämt är det för mig att spåras?” ”Hur mycket är min sekretess värd?” ”Hur mycket vill jag se det här innehållet (om webbläsartillägget exempelvis blockerar ett insticksprogram som återger videor)?

Säkerhetsverktyg

Del ett

Kursinteraktion

Obs! En del av innehållet i den här aktiviteten har diskuterats i ”Aktivitet 1: Risker online”. Vi litar på ditt omdöme när det gäller huruvida du vill gå igenom det här materialet igen om du redan har gått igenom aktivitet nr. 1 eller hoppa över den.

Fråga dina elever

Vet du om du är säker när du använder internet?

Berätta för dina elever

Utan vidta lämpliga säkerhetsåtgärder är det svårt, för att inte säga omöjligt, att helt och hållet skydda sig mot de riskerna online [De som beskrivs i föregående avsnitt.]

Nya risker online dyker också upp hela tiden, så det är viktigt vara på vakt.

Fråga dina elever

Vad kan en person göra om han eller hon har övertygat dig om att personens webbplats faktiskt är en viktig webbplats?

Det finns verktyg som du kan använda för att undvika eller minska riskerna. Känner någon till något sådant?

Berätta för dina elever

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. Du kan använda programverktyg för att se till att du alltid använder HTTPS när det är möjligt.

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

4. 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.

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. EV-certifikat delas ut till webbplatser som verifierar deras identitet för certifikatbehöriget. I webbläsare kan EV-indikatorn ibland se ut som sidans 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 hur du 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”.

Förutom att inte köra program från otillförlitliga källor kan antivirusprogram förhindra dig från att gå in på otillförlitliga sidor och ladda ner skadliga program.

”Nätfiske” sker främst över e-post från en spamavsändare som utger sig för att vara någon legitim. Sedan ber personen dig om ditt lösenord, i hopp om att du skickar det över e-post eller skriver in det på en falsk webbplats. Spamfilter kan förhindra en del av de e-postmeddelandena från att hamna i din inkorg. För att göra spamfiltren bättre bör du markera misstänkta e-postmeddelanden i din inkorg som spam.

Fråga dina elever

Vad kan du göra för att inte råka ladda ner filer som är skadliga för din dator?

Berätta för dina elever

Kontrollera alltid två gånger att du startar nedladdningar från tillförlitliga webbplatser. Var extremt försiktig med att öppna e-postbilagor som du inte känner igen och klicka på popup-fönster och felmeddelanden. Du bör även överväga att installera ett känt

skyddsprogram mot skadliga program på din dator.

Dela lösenord

Del ett

Fråga dina elever

När tror du att det går bra att dela ditt lösenord?

1. Tänkbara svar omfattar delade konton (t.ex. Netflix).

Vilka risker kan förekomma med att dela dina lösenord?

1. Om en skadlig person får ditt lösenord kan ditt konto hackas. Att dela ditt lösenord gör det mer sannolikt att någon kommer in på konton. Om samma lösenord används på andra webbplatser kan de komma in på de kontona också.

Berätta för dina elever

Man brukar inte dela lösenord med någon förutom sidan eller appen som kräver det för inloggning. Precis som beskrivits tidigare är nätfiske att lura någon till att dela sitt lösenord.

Vissa personer kan däremot uttryckligen be om ditt lösenord för att komma åt dina konton och påstå att ditt konto är utsatt för fara. Även om vissa personerna kan ha goda avsikter, t.ex. en god vän som vill hjälpa dig att titta på något på ditt konto som förvirrar dig är det inte klokt att dela ditt lösenord, i synnerhet om du använder det lösenordet på flera konton. Om du planerar att dela ett lösenord bör du kontrollera att det inte används någon annanstans och använda ett lösenordsprogram för att dela tillgången.

Ibland kan personerna som ber dig om dina lösenord vara vuxna personer som du känner och litar på, t.ex. dina föräldrar, lärare eller din arbetsgivare. Även om du känner och litar på de vuxna personerna är det vanligtvis positivt för alla (både dig och dem) att prata om varför de skickar ut begäran och hur de kommer att hantera dina lösenord. I synnerhet när det gäller vuxna utanför familjen är det klokt att be dem direkt om det finns någon lag eller annan sorts regel som de tror kan föra det obligatoriskt för dig att ge dem dina lösenord.

Att ställa artiga och tydliga frågor om lagar och regler är särskilt viktigt när en lösenordsförfrågan kommer från en vuxen person utanför familjen och som du inte känner personligen, t.ex. någon från en brottsbekämpande myndighet. Om du blir tillfrågad av en polis eller statlig tjänsteman om dina lösenord på sociala medier bör du hålla dig lugn och visa respekt. Fråga varför de frågar om detta och vilka lagar eller regler som de anser ger dem rätt att få den informationen om dig.

Beroende på omständigheterna kring en förfrågan från en förälder/vårdnadshavare, lärare, arbetsgivare, person från brottsbekämpande myndighet, myndighetsperson eller annan vuxen kan du behöva ge dem dina lösenord. Omständigheter som hade gjort dig tvungen att uppge dina lösenord är bland annat om det finns fastställda lagar eller regler om att du måste göra det eller om du bedömer fördelen du får av deras hjälp väger tyngre än riskerna med att dela ditt lösenord.

Om du får en fråga från en vuxen om dina lösenord, och den förfrågan känns obekväm på något sätt, ska du omedelbart söka upp en förälder/vårdnadshavare eller annan tillförlitlig vuxen, helst innan du måste svara på förfrågan.

Fråga dina elever

Under vilka omständigheter bör du dela ditt lösenord online?

1. Endast när du uppmanas lämna ut ditt lösenord på webbplatsen du försöker komma in på. Dela aldrig ditt lösenord någon annanstans, bland annat på e-post, som vanligtvis inte är krypterad eller osäker.

Uppgift

Material för utdelning

Uppgift

Dela in deltagarna i grupper om 2–3. Dela ut deltagarmaterialet om spam Be sedan deltagarna göra ett flödesschema för att visa andra hur de kan identifiera spam och huruvida de bör dela specifika informationen med särskilda individer/grupper med personer.

Berätta för dina elever

Läs upp vart och ett av scenariona och diskutera om varje meddelande är spam och om du bör dela information med personen eller gruppen med personer i scenariot.

Kursinteraktion

Ge deltagarna 10 minuter att göra det. Be sedan grupperna att dela med sig av sina svar.

Fråga dina elever

När bör du dela ditt lösenord på e-post?

Berätta för dina elever

Webbplatser och företag brukar aldrig be om ditt lösenord på e-post. Du bör aldrig skicka ditt lösenord till någon på det sättet, även om det verkar som om källan är legitim. E-post är nästan aldrig säkert.

Del två

Uppgift

Be deltagarna komma tillbaka från grupperna eftersom följande övning är för enskilda deltagare.

Ge deltagarna 15 minuter på sig att skapa sina flödesscheman.

Berätta för dina elever

På ett papper ska du nu rita ett flödesschema för att visa personer hur de kan identifiera spam och huruvida de bör dela viss information online med andra. Det kan hjälpa att använda ett specifikt scenario att basera flödesschemat på, antingen ett av de scenarion som visats i det utdelade materialet (om du väljer att göra det ska du

skriva scenariots nummer ovanför flödesschemat) eller göra ett helt nytt. Om du väljer att utforma ett eget scenario ska du beskriva det i ett kort stycke ovanför ditt flödesschema.

Ge deltagarna 15 minuter på sig att skapa sina flödesscheman.