



**Cybersecurity
Academy**



Är du säker?

Cybersäkerhet i elevernas vardag – kunskap som gör skillnad

Lärarhandledning åk 7–9

Lärarhandledning

Sammanfattning

Cybersecurity Academy är ett initiativ som erbjuder utbildning inom cybersäkerhet. Syftet är att öka kunskapen om ett säkert och ansvarsfullt användande av internet samt att stärka elevers digitala kompetens. Genom undervisning, föreläsningar och workshops får eleverna förståelse för hur deras aktiviteter på nätet kan påverka dem själva och andra – och hur de kan skydda sina uppgifter.

Det här undervisningsmaterialet för högstadiet är utformat för att du som lärare själv ska kunna arbeta med cybersäkerhet i klassrummet. Materialet är ämnesövergripande och kopplat till Lgr22, framför allt inom samhällskunskap, svenska och teknik. En sammanställning av kopplingarna till läroplanen finns på sidan 23. Du behöver inte ha någon förkunskap inom området eller undervisa i teknik.

Materialet i broschyren består av tre lektioner som tillsammans ger en bred introduktion till cybersäkerhet ur ett vardagsperspektiv. Varje lektion bygger på en kort introducerande film samt tillhörande övningar och diskussioner. Filmerna finns även på lättsvenska och med undertexter på engelska, arabiska, tigriska och somaliska.

Lektion 1 – Ditt digitala fotavtryck

Förstå hur din data används. Eleverna utforskar vad ett digitalt fotavtryck är, hur data samlas in av appar och tjänster och varför deras information är värdefull för andra. Lektionen lägger grunden för de kommande två lektionerna genom att skapa förståelse för den digitala verklighet vi alla rör oss i.

Lektion 2 – Klicka smart

Identifiera och genomskåda hot. Med förståelsen från lektion 1 som grund tittar eleverna nu på hur deras data kan utnyttjas mot dem – i form av nätbedrägerier, phishing och deepfakes. De tränar sig i att känna igen varningssignaler och övar på att vara kritiska mot det de möter online.

Lektion 3 – Digital rustning

Agera och skydda dig. I den avslutande lektionen omsätter eleverna sina kunskaper i handling. De lär sig konkreta verktyg för att skydda sig: starka lösenord, tvåfaktorsautentisering och ett medvetet förhållningssätt till digitala tjänster.

Digitalt komplement: AI-lektioner

AI förändrar snabbt förutsättningarna för cybersäkerhet – både som verktyg för bedragare och som teknik eleverna möter i sin vardag. Därför har vi tagit fram ett digitalt komplement med AI-lektioner som fördjupning till broschyrens tre lektioner eller som ett fristående arbetsområde. Eftersom AI-området utvecklas snabbt har vi valt att hålla AI-materialet digitalt, det gör det enklare att uppdatera i takt med att tekniken förändras.

AI-lektionerna innehåller fyra delar: ett projektarbete där eleverna utforskar hur AI kan användas som verktyg i en designprocess (7 lektioner), ett projektarbete som undersöker likheter och skillnader mellan mänskligt tänkande och AI (5 lektioner), en teknikhistorisk lektion om AI:s utveckling (1 lektion), samt tips och källor för att arbeta med källkritik och desinformation i en tid när AI förändrar hur information skapas och sprids (tips och länksamling).

© Unga Forskare

www.ungaforskare.se

Lärarhandledningen kan beställas via utbudet.se.
Det är helt kostnadsfritt och fraktfritt för skolan.

En digital version finns att ladda ner på cybersecurityacademy.se.

Författare:

Martina Sandgren
Max Vinger
Judith Maiers

Grafisk form:

Art-O-Matic, Stockholm

Tryckeri:

AMO-Tryck AB, Solna

Tryckår:

2026, version 1.0

Innehåll

Lärarhandledning	2
Sammanfattning	2
Bakgrund	4
Om Cybersecurity Academy	4
Lektion 1 – Ditt digitala fotavtryck	6
Ett digitalt vardagsliv	6
Oaktsamt beteende online	7
Ditt digitala fotavtryck	7
Klicka bara ja! Eller?	7
Varför samlas data in?	9
Ta kontroll över din data	10
Lektion 2 – Klicka smart	11
Vår digitala värld och dolda faror	11
Klicka smart	12
Bluffdetektiv	13
Har dina uppgifter läckt?	15
Skydda dig mot nätbedrägerier	16
Lektion 3 – Digital rustning	17
Vad har du att skydda?	18
Digital rustning	18
Skydda din data med...	19
... lösenord	19
... tvåfaktorsautentisering (2FA/MFA)	21
Har du lärt dig hur du skyddar dig?	21
Säkerhet är en vana	22
Anknytningar till Lgr22	23
Vem står bakom projektet?	24

Bakgrund

Vi lever i ett digitaliserat samhälle där stora mängder information lagras, delas och bearbetas varje dag. Kommunikation, lärande och sociala relationer sker i hög grad online och de flesta människor har idag personlig information sparad på flera olika platser – i mobilen, i sociala medier, i e-post och i olika digitala tjänster.

Samtidigt utvecklas tekniken snabbt. Artificiell intelligens (AI) är idag en naturlig del av många digitala tjänster och påverkar hur vi söker information, kommunicerar och fattar beslut. AI skapar stora möjligheter, men innebär också nya utmaningar kopplade till desinformation, integritet, etik och säkerhet.

Parallellt med den digitala utvecklingen ökar också antalet cyberrelaterade hot, såsom bedrägerier, dataintrång och spridning av skadlig kod. Dessa hot kan komma från enskilda individer, organiserad brottslighet eller statliga aktörer. För att kunna agera säkert i den digitala världen krävs både kunskap och medvetenhet om risker och hur man skyddar sig.

Barn och unga är idag ständigt uppkopplade. Enligt Internetstiftelsens rapport *Svenskarna och internet* använder i princip alla barn internet dagligen, ofta från tidig ålder. De använder digitala plattformar för att kommunicera, spela, lära och ta del av information. Samtidigt möter de risker som de inte alltid har förutsättningar att hantera på egen hand.

När vi pratar om cybersäkerhet är det viktigt att lyfta både risker och möjligheter. Ökad kunskap bidrar inte bara till att minska sårbarhet, utan också till att skapa trygghet och ge elever förutsättningar att använda digitala verktyg på ett ansvarsfullt och medvetet sätt.

Om Cybersecurity Academy

Cybersecurity Academy är ett initiativ som drivs i samarbete mellan den ideella organisationen Unga Forskare och aktörer inom teknikbranschen. Verksamheten finansieras genom samarbeten och stöd från bland annat Myndigheten för civilt försvar, vilket gör att hela utbudet är kostnadsfritt för skolor.

Initiativet ger skolor möjlighet att arbeta med cybersäkerhet på flera sätt. Vi erbjuder föreläsningar, workshops och undervisningsmaterial som kan användas tillsammans eller var för sig. Genom våra insatser får eleverna både kunskap om risker på nätet och verktyg för att hantera dem i praktiken.

Föreläsningar

Våra föreläsningar ger en introduktion till ämnet och tar upp aktuella frågor som säkerhet på nätet, källkritik, digitala spår, bedrägerier och hur personlig information kan spridas. Innehållet anpassas efter elevernas ålder och syftar till att öka medvetenheten och väcka intresse för cybersäkerhet.

Workshops

Våra workshops leds av utbildade instruktörer och bygger på ett lustfyllt och interaktivt lärande. De kan exempelvis handla om cybersäkerhet, artificiell intelligens (AI), programmering eller desinformation, och anpassas efter elevernas ålder och förkunskaper. Workshoppen fyller också en viktig roll i att främja nyfikenhet och intresse för teknik – många elever får upp ögonen för att teknik är rolig, mångsidig och oftast har koppling till saker de redan brinner för.

Undervisningsmaterial

Vi erbjuder undervisningsmaterial i form av lärarhandledningar som gör det möjligt för lärare att arbeta vidare med cybersäkerhet i klassrummet. Materialet är anpassat för olika åldersgrupper i grundskolan och kan användas både som fristående lektioner och som längre arbetsområden. Lektionsmaterialet är ämnesövergripande och kräver inte IT-kompetens.

Lärarfortbildning För lärare erbjuder vi fortbildning i cybersäkerhet, antingen som en digital kurs eller som fortbildning på plats i skolan. Fortbildningen kan genomföras som en kortare introduktion eller som ett mer fördjupat arbete.



Läs mer och boka på cybersecurityacademy.se

IBM SkillsBuild

IBM SkillsBuild är en kostnadsfri läroplattform som drivs av IBM och erbjuder ett brett utbud av kurser inom teknik och digitala färdigheter. Plattformen passar både elever som vill utforska ett nytt område och dem som vill fördjupa sig – kurserna spänner från grundläggande introduktioner till mer djupgående material som avslutas med ett digitalt certifikat.

Bland kursområdena finns bland annat artificiell intelligens, cybersäkerhet, datavetenskap, UX-design, webbutveckling, hållbarhet och källkritik. Materialet är framtaget i samarbete med universitet, IT-expert och organisationer inom utbildning och forskning och är anpassat för högstadie- och gymnasieelever. Kurserna är uppbyggda i korta moduler som fungerar lika bra för självstudier som för klassrumsarbete – det är enkelt att pausa och fortsätta, och man väljer själv tempo och fördjupningsgrad.

Merparten av innehållet är på engelska, men kursmaterial från Cybersecurity Academy och andra svenska organisationer finns tillgängligt på svenska.



Utforska plattformen på https://ibm.biz/ungaforskare_t

Lektion 1 – Ditt digitala fotavtryck

Det här är den första av tre lektioner om cybersäkerhet i vardagen. Den lägger grunden för de kommande lektionerna genom att utforska vad ett digitalt fotavtryck är och varför elevernas data är värdefull. Lektion 2 (Klicka smart) bygger vidare på detta och visar hur data kan utnyttjas mot eleverna. Lektion 3 (Digital rustning) ger eleverna konkreta verktyg för att skydda sig.

Mål

Efter lektionen ska eleverna kunna:

- Definiera cookies och vad de används till
- Diskutera hur cookies kan vara en del av en affärsmodell
- Diskutera rätten till sin data
- Ha kunskap om hur de själva kan agera för att skydda sin data

Material

Lektionsupplägget är framtaget med tanke att inte kräva något som inte redan finns i de flesta klassrum.

- Projektor med högtalare för att visa filmen
- Projektor ifall man vill använda powerpointpresentationen

Delar i lektionsförslaget

Del	Typ	Tid
Ett digitalt vardagsliv	Lärlarledd introduktion med presentation	5 min
Oaktsamt beteende online	Film (Tänk säkert) + diskussion	10 min
Ditt digitala fotavtryck	Film (Ditt digitala fotavtryck)	5 min
Klicka bara ja! Eller?	Lärlarledd genomgång med presentation + demonstration	15 min
Varför samlas data in?	Diskussionsövning i grupper	15 min
Ta kontroll över din data	Lärlarledd avslutning	5 min

Ett digitalt vardagsliv



Bild 1–3 i presentationen

Inledning

Presentera dagens ämne: cybersäkerhet och det digitala fotavtrycket. Lyft att ungefär halva våra liv idag sker online och att vi måste kunna manövrera i datadjungeln.

Din data kan vara valuta online: Varje gång vi rör oss på nätet lämnar vi spår efter oss – information som kan kopplas till oss som användare. Vi kanske inte tror att de är intressanta för andra, men en del data kan faktiskt vara guld värt för någon annan.

Inledande frågeställning: Har någon en gissning eller vet någon vad ett digitalt spår kan vara?

Exempel man kan ta upp: sökhistorik, bilder som man lägger upp, vilka man följer på olika appar och sociala medier, hur länge man är på en hemsida, hur länge man kollar på en bild, vad man köper, vad man klickar på, vad man kommenterar på.

Oaktsamt beteende online



Bild 4 i presentationen

En del av spåren lämnar vi medvetet, som när vi fyller i ett formulär eller lägger upp något på sociala medier. Men mycket sker utan att vi tänker på det. Nu ska vi titta på två korta filmer som handlar om just det: våra digitala fotavtryck.

Video – Tänk säkert

Visa den korta filmen som illustrerar oaktsamt beteende online:



<https://youtu.be/K4FqzSqrjwE>

Obs! Länkar till filmer kan bli utdaterade. För aktuella länkar till samtliga filmer, se det digitala komplementet *Är du säker? Arbetsblad och filmlänkar – Högstadiet*. Om en länk inte fungerar, kontrollera att du har den senaste versionen av länksamlingen. Filmerna finns också på skolmaterial.ungaforskare.se/tank-sakert.

Frågeställning för diskussion: Varför delar vi med oss så mycket online som vi kanske inte skulle ha gjort i verkliga livet?

Ditt digitala fotavtryck



Bild 5–6 i presentationen

Även om vi kanske aldrig skulle dela med oss så frikostigt som Roger i filmen – varken i verkliga livet eller digitalt – lämnar vi ändå spår på nätet hela tiden, ofta utan att vi ens tänker på det. Varje gång vi besöker en hemsida, söker på något eller scollar i ett flöde samlas information om oss och vårt beteende in. En av de vanligaste teknikerna för det är cookies.

Video – Ditt digitala fotavtryck



https://www.youtube.com/playlist?list=PLIk39hnHx0Lv0ayyDRa50Z2tDGdne_b9e

Klicka bara ja! Eller?



Bild 7–13 i presentationen

Cookies

Repetera och utveckla det som sades i videon.

Inledande frågeställning: Vad är cookies och vad används de till?

- Cookies ser ofta ut som en liten frågeruta när man går in på en hemsida, där aktören bakom sidan vill att man ska klicka och göra ett val att tillåta eller avvisa cookies.

Teknisk fördjupning om cookies

Att godkänna cookies är att godkänna att textfiler sparas i din webbläsare när du besöker olika webbplatser. De används av företag och andra organisationer för att samla in information om ditt beteende online – och i vissa fall kan även illasinnade aktörer utnyttja dem, så som hackare. Informationen ses som mycket värdefull, både för kommersiella syften och av säkerhetsskal. Därför är det viktigt att förstå vad man faktiskt godkänner.

- Cookies gör att företag/hemsidor kan spara information om dig.
- När man till exempel går in på sidan en vecka senare plockas den tidigare sparade informationen fram och på så sätt anpassas sidan till dig. Sidan kan då till exempel:
 - Förenkla inloggningen så att du slipper fylla i användarnamn och lösenord varje gång
 - Hålla reda på vilka varor du har lagt i din varukorg när du handlar på nätet
 - Hålla reda på att du inte röstar två gånger i en omröstning

Underdomäner

När du går in på en viss hemsida kan denna i sin tur öppna andra sidor, så kallade underdomäner.

- Exempel: När du öppnar SVT:s hemsida skickas och tas även data från SMHI:s hemsida för att kunna visa dig dagens väder.
- Hemsidor kan öppna många olika underdomäner utan att du märker det. Bland annat för att kunna anpassa innehåll eller reklam mot just dig.

Riktad reklam

Riktad reklam är en av de vanligaste sakerna som cookies används till.

Frågeställning: Är det någon som varit med om att man fått reklam för något man sökt på?

Vissa kakor kan användas för att följa vad du gör på olika sidor. Till exempel för att rikta reklam till just dig. Det är därför plötsligt hela ditt flöde blir fullt med annonser för sneakers om du har googlat på det. Hemsidor säljer vidare information om dig till andra aktörer.

Man kan välja i webbläsaren (Google Chrome, Firefox, Microsoft Edge, Safari med flera) vilka och hur kakor ska få lagras.

Fördjupning om lagstiftning kring personlig information

Vår personliga information är skyddad genom bland annat GDPR på EU-nivå och lagen om elektronisk kommunikation (LEK) i Sverige. Lagstiftningen innebär att företag och organisationer inte får samla in eller spara dina personuppgifter utan att du har gett ditt samtycke. Det är därför hemsidor måste fråga dig om cookies – du ska ha möjlighet att själv välja vad du godkänner.

Demonstration – Cookieinställningar

Du kan lätt demonstrera hur man ändrar inställningar för cookies i webbläsaren, eller be eleverna själva att testa. Nedan är en instruktion för Google Chrome men det går enkelt att hitta motsvarande instruktion för andra webbläsare och det brukar vara liknande förfarande.

För Google Chrome

- Gå in på: chrome://settings/privacy eller klicka på chrome-menyn
- Klicka på Inställningar eller Settings (engelska) i menyn
- Välj Sekretess och säkerhet (Privacy and security)
- Klicka på Cookies och annan webbplatsdata (Cookies and other site data)
- Här kan du:
 - Tillåta alla cookies (Allow all cookies)
 - Blockera tredje-parts cookies (Block third-party cookies)
 - Blockera alla cookies (Block all cookies)
 - Anpassa inställningar för specifika webbplatser

Hantera cookies direkt på en hemsida

Hemsidor kan göra det mer eller mindre svårt att hantera cookies.

Hemsidan måste direkt ha som alternativ på det första fönstret som kommer upp att godkänna (agree) eller avvisa (reject) alla valbara cookies. Men ibland så följer inte företag reglerna. 2022 dömdes Google i Frankrike på 150 miljoner euro för att de inte gav användaren alternativ för att avvisa cookies på ett enkelt sätt.

Det går att anpassa ytterligare genom att man kan välja vissa specifika inställningar om man klickar på hantera cookies (manage cookies) eller går in på cookie-inställningar efteråt. Man måste ha möjlighet att ändra sig, även om man tackat ja tidigare.

Varför samlas data in?



Bild 14–18 i presentationen

Den här delen av lektionsupplägget består av tre diskussionsfrågor. Frågorna kan användas för diskussioner i helklass eller i mindre grupper. Upplägg och tid är tänkt att anpassas utifrån grupp.

1. Finns det en affärsidé?

Låt eleverna diskutera vad de tror anledningen är att inställningarna för cookies ofta är ganska svårtolkade och jobbiga att stänga av jämfört med att bara acceptera.

Det finns en potentiell vinst för företag att samla in info eftersom data går att sälja vidare. En förklaring till de komplicerade designerna kan därför vara att man helt enkelt utnyttjar att de flesta inte orkar läsa igenom och därför väljer den enkla vägen ut att bara acceptera cookies. De vill ha användarens information och räknar med att vi är lite lata.

En lite mer generös tolkning av åtminstone en del av problematiken är att olika företag helt enkelt använder olika språk och har olika design, men att det skapar förvirring för användaren.

2. Vad är motivet med att samla in cookies?

Här är det tänkt att man kan diskutera vad varje enskild aktör kan ha för motiv med att samla in cookies. Det går naturligtvis att välja vilka aktörer man tar upp för att anpassa till målgruppen.

- Vad skulle Stadium kunna använda cookies för?
 - Spara varukorg
 - Riktad reklam
 - Spara inloggning
 - Spara bankuppgifter
 - Spara position för att föreslå närmaste butik
 - Spara adress för ordrar
- Vad skulle SAS kunna använda cookies för?
 - Spara påbörjade bokningar
 - Riktad reklam
 - Spara inloggning
 - Spara bankuppgifter
 - Spara din position för att kunna automatiskt föreslå flygplats att resa från

- Vad skulle Netflix kunna använda cookies för?
 - Spara info om vilka episoder/filmer du sett
 - Spara inloggning
 - Spara bankuppgifter för betalningar
 - Spara din position för att kontrollera att ett konto bara används av ett hushåll
- Vad skulle Dagens Nyheter kunna använda cookies för?
 - Spara inloggning
 - Spara bankuppgifter för betalningar
 - Spara din position för att ge dig lokala nyheter
 - Spara information om vad du läst för att ge dig förslag på annat du kanske skulle tycka kan vara intressant

3. Vem vill du ska få ta del av dina cookies?

Efter att ha diskuterat olika aktörers motiv med att samla in cookies kan man nu diskutera vilka av dem, om några, man känner sig bekväm med att dela cookies med. Det finns såklart inga rätta svar utan är tänkt att leda eleverna till att ta egna medvetna beslut.

Vad skulle en hackare kunna använda cookies för?

Det vanligaste sättet som cookies används på ett skadligt sätt är genom falska sidor som antingen tjänar pengar på att samla in en stor mängd av information och sälja vidare eller genom rena bedrägerier. En annan risk med cookies, som hackare kan utnyttja när hemsidor har dålig säkerhet, är att stjäla särskilda cookies som låter dem "låtsas" vara en vanlig användare och på så sätt lura systemet att släppa in dem i andra användares konton. Det kallas session hijacking och är ett sätt att få tillgång till känslig information som kan finnas på ditt konto.

Ta kontroll över din data

Avslutning

Under lektionen har vi sett att företag samlar in data om oss, att den informationen är värdefull och att den kan säljas vidare. Men det leder till en viktig insikt: många av de tjänster vi använder varje dag – sociala medier, spel, appar – kostar ingenting. Ändå tjänar företagen bakom dem stora pengar. Hur går det ihop? Jo, när en tjänst är gratis betalar du ofta med din information istället. Utan att vi alltid tänker på det blir vi själva produkten.

Det betyder inte att man måste sluta använda internet – men att man kan göra det mer medvetet. Du kan justera cookie-inställningar på hemsidor och i din webbläsare, fundera en extra gång på vad du lägger ut och vilka behörigheter du ger appar. Små val gör skillnad.

Avsluta gärna med att fråga eleverna hur de känner kring det ni pratat om. Försök att få dem att lämna med känslan att de har makt över sin data – inte att internet är farligt, utan att de nu vet mer om hur det fungerar och vad de kan göra åt det.

Lektion 2 – Klicka smart

Det här är den andra av tre lektioner om cybersäkerhet i vardagen. Den bygger vidare på Lektion 1 (Ditt digitala fotavtryck) och visar hur information kan utnyttjas i form av bedrägerier och manipulativa bluffar. Lektion 3 (Digital rustning) avslutar materialet med konkreta verktyg för att skydda sig.

Mål

Efter lektionen ska eleverna kunna:

- Ge några exempel på nätbedrägerier och hur de går till
- Beskriva hur nätbedrägerier påverkar individen och samhället i stort
- Skydda sig bättre online genom att känna igen varningssignaler

Material

Lektionsupplägget är framtaget med tanke att inte kräva något som inte redan finns i de flesta klassrum.

- Projektor med högtalare för att visa filmen
- Projektor ifall man vill använda powerpointpresentationen
- Whiteboard
- Pennor
- Arbetsblad (finns som digitalt komplement *Är du säker? Arbetsblad och filmlänkar – Högstadiet*)

Delar i lektionsförslaget

Del	Typ	Tid
Vår digitala värld och dolda faror	Lärlarled introduktion med presentation	5 min
Klicka smart	Film (Klicka smart) + diskussion	10 min
Bluffdetektiv	Gruppövning med arbetsblad	5 min
Har dina uppgifter läckt?	Lärlarled genomgång med presentation + övning	15 min
Skydda dig mot nätbedrägerier	Lärlarled avslutning	5 min

Vår digitala värld och dolda faror



Bild 1–2 i presentationen

Inledning

Presentera dagens ämne: cybersäkerhet och bedrägerier.

Vi lever stora delar av våra liv online. I spel, sociala medier, klasschattar och appar. Det känns ofta tryggt och självklart.

Bakom varje pling, länk och meddelande kan det dock finnas någon som försöker lura dig, det sker varje dag och kan ske vem som helst.

Många unga luras i spel eller i chattar. Men även många vuxna luras, exempelvis att ge ut privat information eller att skicka över pengar. Allt detta är något som kallas nätbedrägerier.

Bedrägerier kan komma i form av massutskick av sms, mejl, annonser eller bluffhemsidor. Detta kallas för phishing – man fiskar efter måltavlor. Men det kan även ske riktat med en specifik måltavla i åtanke.

Idag ska vi lära oss att bli ”bluffdetektiver” för att känna igen när någon försöker lura oss, och hur vi kan skydda oss på nätet.

Nätbedrägerier på samhällsnivå

Offentliga aktörer och stora företag måste ha digital närvaro och digitala tjänster. Exempelvis har vi 1177 med digitala journalsystem, och arbetsgivare måste ha listor med kontaktuppgifter och bankkontonummer till sina anställda för att kunna betala ut lön. Den här typen av känslig information är värdefull för kriminella – ett vanligt tillvägagångssätt är att ta sig in i ett system, stjäla data och sedan kräva pengar för att inte sprida den vidare.

Detta skapar problem för hela samhället. Kanske har ni hört om att personuppgifterna till vad man tror är 80 % av svenska kommuners anställda (ca en miljon personuppgifter) har läckt till darknet från systemleverantören Miljödatas databaser. De som låg bakom var hackergruppen Datacarry, och de krävde 1,5 bitcoin, som i mitten av september 2025 var värt drygt 1 600 000 kr. Vi vet inte exakt hur det gick till, men en möjlig förklaring är att de kan ha använt phishing för att ta sig in.

Klicka smart



Bild 3–4 i presentationen

Bedrägerier på nätet är sällan slumpmässiga – de är utformade för att spela på våra känslor och få oss att agera snabbt utan att tänka efter. Nu ska vi titta på en kort film som visar hur det kan se ut.

Video – Klicka smart



https://www.youtube.com/playlist?list=PLIk39hnHx0LSv2uVCgmBYzEx-3TMf__gP

Obs! Länkar till filmer kan bli utdaterade. För aktuella länkar till samtliga filmer, se det digitala komplementet *Är du säker? Arbetsblad och filmlänkar – Högstadiet*. Om en länk inte fungerar, kontrollera att du har den senaste versionen av länksamlingen. Filmerna finns också på skolmaterial.ungaforskare.se/tank-sakert.

Filmen visade hur bedrägerier på nätet kan se ut – och hur lätt det kan vara att gå på dem. Men varför fungerar det egentligen? Varför lyckas bedragare lura människor, trots att vi vet att bluffar finns? Det handlar om den mänskliga faktorn.

Den mänskliga faktorn

Phishing, social engineering och malware är tre olika tekniker som hackare använder för att ta sig in i system och konton. Gemensamt för dem är att de ofta riktar sig mot människan snarare än mot tekniken – det är helt enkelt lättare att manipulera en person än att forcera ett välskyddat system. Stora attacker, som den mot Miljödata, kombinerar ofta flera av dessa tekniker.



Bild 5–16 i presentationen

Kännetecken

Repetera och utveckla från filmen.

Inledande frågeställning: Vad kännetecknar ett nätbedrägeri eller ”nätbluff”?

- De är försök att lura dig och kommer därför ofta i form av helt vanliga meddelanden på sms, DM:s eller bluffhemsidor.
- De har ofta en stressande ton, med tidsbrister eller nedräkningar. De vill få dig att inte tänka efter.
- De kan ofta vara otroligt bra erbjudanden, som ”alla vinner”-annonser eller någon som vill ge något gratis till dig.

Exempel på bluffar

Konkreta exempel på vanliga nätbedrägerier. Visa upp de fyra exemplen utan att analysera dem. Dela in eleverna i grupper eller par och låt dem titta närmare på exemplen och bedöma om de är sanna eller bedrägeriförsök. Resonera och diskutera efteråt. Om du vill kan du även ge lite tips vad de kan kolla på, se nedan. Exemplet finns i powerpointpresentationen och som arbetsblad i det digitala komplementet *Är du säker? Arbetsblad och filmlänkar – Högstadiet*.

- **Phishing-SMS/epost:** Ett meddelande som ser ut att komma från banken, posten, skolan eller en vän kan vara en bluff.
 - Du kan alltid dubbelkolla genom att kontakta avsändaren på ett annat sätt om du känner dem.
 - Logga alltid in själv via officiella appar eller googla, följ inte länkar om du är det minsta osäker.
- **Bluffhemsidor:** Ibland får man länkar till hemsidor via phishing eller så hamnar man på en hemsida genom att råka skriva lite fel i adressen. De här hemsidorna kan se ut att vara legitima, men är i verkligheten till för att lura dig på något sätt. Ofta på information, exempelvis inloggningsuppgifter till spel eller andra konton.
 - Dubbelkolla att adressen till hemsidan är korrekt. Om den inte börjar med http: eller https: kan det också vara tecken på att den inte är så legitim som den verkar vara.
 - Logga alltid in själv via officiella appar eller googla, följ inte länkar om du är det minsta osäker.
- **Bluffannonser:** Kända varumärken är populära att imitera – ett fejkat konto med välkänt namn och logotyp kan se trovärdigt ut vid en snabb blick.
 - Är det för bra för att vara sant? Gratispriser som kräver att du klickar på en länk eller fyller i uppgifter är ett klassiskt varningstecken.
 - Kolla kontot noga: saknar det en verifieringsbock, har det få inlägg eller skapades det nyligen? Det talar för att det är fejk.
 - Sök upp varumärkets officiella konto och se om erbjudandet finns där också – gör det inte det är det troligen en bluff.
 - Klicka aldrig på länkar i annonser eller inlägg från okända konton – gå alltid direkt till varumärkets officiella hemsida.

- **Deepfake:** AI kan idag användas för att skapa realistiska men helt falska videor och röstinspelningar, så kallade deepfakes. Kriminella utnyttjar detta för att lura människor, till exempel genom att fejka kända personer i videor.
 - Exempel: En deepfake-video av youtubern MrBeast spreds där han verkade ge bort dyra priser nästan gratis. Videon såg äkta ut, men var helt AI-genererad och skapad för att lura tittare att klicka på en blufflänk.
 - Deepfakes kan vara mycket svåra att avslöja. Var extra skeptisk mot videor där någon erbjuder något som verkar för bra för att vara sant – även om personen ser och låter äkta.
 - Det här är ett exempel på när avancerade AI-verktyg, som idag är tillgängliga för de flesta, används av kriminella för att begå bedrägeri.

Diskussionsövning

Dela in eleverna i små grupper. Låt varje grupp titta på exemplen ovan och svara på:

- Vad är det som känns konstigt eller misstänkt med det här meddelandet/ erbjudandet? Vilka varningssignaler hittar ni?
- Vad tror ni kan hända om man klickar på länken eller lämnar ut uppgifter här?

Anteckna gärna på tavlan efter diskussionen:

- Brådskande språk: "måste agera inom 48 timmar"
- Konstig avsändare/mejladress: "ser fel ut".
- Erbjudanden som "verkar för bra för att vara sanna".
- Begäran om känsliga uppgifter
- Länkar till andra sidor än de officiella (kolla på [https/](https://)[http](http://) också).
- Vad skulle aktören vilja med mina inloggningsuppgifter?

Malware

Vad händer egentligen när man klickar på en blufflänk? I många fall är konsekvensen att skadlig kod – så kallad malware – laddas ner till enheten utan att användaren märker det.

Malware (malicious software) eller så kallad skadlig kod sprids ofta genom blufflänkar i mejl, sms, annonser, infekterade nedladdningslänkar eller i tävlingar. Det kan vara många olika typer av kod, så som virus, maskar, spionprogram och trojanska hästar. En användare kan, efter att ha klickat på en sådan länk, ha laddat ner skadlig kod som i sin tur stjälar lösenord, bankuppgifter eller annan känslig information.

AI som verktyg i bedrägerier

Phishing har blivit ett av de vanligaste bedrägerisätten online och har effektiviserats av AI. Det används för att automatisera processen med övertygande meddelanden och göra det möjligt för bedragare att attackera snabbare och i större skala.

AI används också för att skapa deepfakes – falska ljud- och videoinspelningar som kan vara svåra att skilja från äkta. Deepfakes, som används i det sista exemplet med MrBeast, är något som framställs med hjälp av specifika typer av AI-modeller. Med dagens deepfakes, exempelvis för ljud, behöver man endast några sekunders ljudinspelning för att göra en ny, falsk inspelning med en fejkad röst som kan användas för phishing via exempelvis telefon. Därför måste vi vara försiktiga med vad vi själva lägger upp online, exempelvis videor som vi blir skickade eller lägger ut. Det kan vara viktigt att prata om det hemma med sina närmaste om hur man ska agera om man tror att man är under ett bedrägeriförsök via video eller ljud.

AI-bildmodeller används även mot unga i så kallade sextortion scams – utpressning i syfte att få pengar eller tvinga personen att skicka sexuella bilder. Det är viktigt att markera att detta är ett allvarligt brott. Den som utsätts är ett brottsoffer med rätt till stöd, och det ska anmälas till polisen.

Har dina uppgifter läckt?



Bild 17–18 i presentationen

En av de svåraste sakerna med dataläckor är att de sällan syns direkt. När ett företag eller en tjänst utsätts för ett intrång och användaruppgifter stjäls, märker de flesta ingenting – inga varningsmeddelanden, inga konstiga inloggningar, inget som känns annorlunda. Uppgifterna kan ligga ute på darknet i månader eller år innan något händer, och när det väl händer är det inte säkert att man kopplar det till läckan.

Det betyder att man kan ha fått sina uppgifter stulna utan att ha en aning om det. Fråga gärna eleverna: Hur tror ni att man märker om ens uppgifter har läckt? Låt dem diskutera kort innan ni går vidare – svaret är ofta att man inte märker det alls.

Övning – testa på haveibeenpwned.com

Det finns ett verktyg som gör det möjligt att kontrollera om ens e-postadress eller telefonnummer har förekommit i en känd dataläcka. Sidan heter Have I Been Pwned och finns på haveibeenpwned.com.

Sidan drivs av Troy Hunt, en välkänd och respekterad säkerhetsforskare som samlar in information om kända dataläckor och gör det möjligt för privatpersoner att kontrollera om deras uppgifter finns med. Det är en seriös och säker tjänst som används av både privatpersoner och organisationer världen över.

Så här går det till:



Gå in på haveibeenpwned.com

Skriv in en e-postadress i sökfältet och klicka på **Check**

Sidan visar om adressen förekommit i någon känd dataläcka.

Hur tolkar man resultatet?

Om sidan visar grönt med texten «Good news — no pwnage found» betyder det att e-postadressen inte hittats i någon känd läcka. Det är ett bra tecken, men det betyder inte nödvändigtvis att uppgifterna aldrig läckt – bara att de inte finns i de läckor som registrerats i databasen.

Om sidan visar rött med information om en eller flera läckor betyder det att e-postadressen förekommit i minst en känd dataläcka. Sidan visar vilka tjänster som drabbats och ungefär vilken typ av information som läckt – till exempel e-postadress, lösenord, telefonnummer eller adress.

Vad ska man göra om ens uppgifter har läckt?

Gå igenom punkterna nedan med eleverna:

- Byt lösenordet på den drabbade tjänsten omedelbart – och på alla andra tjänster där du använt samma lösenord.
- Aktivera tvåfaktorsautentisering (2FA) om det inte redan är påslaget – det fördjupas i Lektion 3.
- Var extra uppmärksam på misstänkta mejl, sms eller samtal den närmaste tiden – läckta uppgifter används ofta för riktade phishingförsök.
- Prata med en vuxen om du är osäker på vad du ska göra.

Skydda dig mot nätbedrägerier

Avslutning

Under den här lektionen har vi sett att bedrägerier på nätet sällan handlar om avancerad teknik – de handlar om att lura människor. Phishing, bluffannonser, falska hemsidor och deepfakes är alla utformade för att spela på våra känslor: stress, nyfikenhet, rädsla eller lockelsen av att vinna något. Det viktigaste verktyget för att skydda sig är därför inte en app eller ett program, utan det vi har tränat på idag: att stanna upp och tänka efter.

Sammanfatta gärna de viktigaste tumreglerna tillsammans med eleverna:

- **Stanna upp.** Om något känns brådiskande, spännande eller för bra för att vara sant – ta ett steg tillbaka.
- **Dubbelkolla.** Kontakta avsändaren på ett annat sätt. Gå in på officiella hemsidor själv istället för att följa länkar. Kolla avsändaradressen nog.
- **Prata med någon.** Om du är osäker, prata med en vuxen eller en kompis. Bedragare vill att du ska agera ensam och snabbt – gör tvärtom.

Avsluta gärna med att lyfta att det inte är något att skämmas över om man har blivit lurad – det händer även vuxna och stora organisationer, som vi såg med exemplet Miljödata. Det viktiga är att man vet vad man ska göra och att man vågar berätta.

Lektion 3 – Digital rustning

Det här är den tredje och avslutande lektionen om cybersäkerhet i vardagen. Den samlar ihop det eleverna lärt sig i Lektion 1 och 2 och omsätter det i handling – konkreta verktyg och vanor för att vara säkrare online. Passar utmärkt som avslutning på ett arbetsområde, men fungerar också fristående.

Mål

Efter lektionen ska eleverna kunna:

- Förklara varför deras digitala data är värdefull och behöver skyddas.
- Beskriva tre grundläggande principer för digitalt självförsvar (starka lösenord, tvåstegsverifiering och medvetna digitala vanor).
- Känna till att de kan agera för att skydda sig själva online och känna till verktyg för att göra detta.

Material

Lektionsupplägget är framtaget med tanke att inte kräva något som inte redan finns i de flesta klassrum.

- Projektor med högtalare för att visa filmen
- Projektor ifall man vill använda powerpointpresentationen
- Utskrivna frågor till tipspromenaden (finns som digitalt komplement *Är du säker? Arbetsblad och filmlänkar – Högstadiet*)
- Pennor och papper eller annat för att göra tipspromenaden

Delar i lektionsförslaget

Del	Typ	Tid
Vad har du att skydda?	Film (Digital rustning, del 1) + diskussion	5 min
Digital rustning	Film (Digital rustning, del 2) + diskussion	5 min
Skydda din data	Lärlarled genomgång med presentation + praktiska moment	30 min
Har du lärt dig hur du skyddar dig?	Quiz/tipsrunda i grupper	15 min
Säkerhet är en vana	Lärlarled avslutning	5 min

Vad har du att skydda?



Bild 1–2 i presentationen

Inledning

Inled lektionens tema med: Tänk på allt som finns i din telefon och på dina konton – bilder, meddelanden, inloggningar, kanske till och med bankuppgifter. Den här lektionen handlar om vad du konkret kan göra för att skydda det som är ditt. Vi börjar med en kort film som sätter scenen.

Video – Digital rustning

Börja med att visa den första delen av filmen (tid 00:00-00:32).



<https://www.youtube.com/playlist?list=PLIk39hnHx0Lt-DBDkAmPB3x6Jl4iJaf22>

Obs! Länkar till filmer kan bli utdaterade. För aktuella länkar till samtliga filmer, se det digitala komplementet *Är du säker? Arbetsblad och filmlänkar – Högstadiet*. Om en länk inte fungerar, kontrollera att du har den senaste versionen av länksamlingen. Filmerna finns också alltid på skolmaterial.ungaforskare.se/tank-sakert.

- Pausa filmen när problembilden byggts upp och presenterats
- Återkoppla till det som visades: alla lever en stor del av vardagen online, vi har ett digitalt liv (sociala medier, gaming, osv). Unga spenderar ungefär 7 timmar online per dag i Sverige.
- Öppen fråga: Hur många av er använder appar som TikTok, dataspel, Instagram eller chattar med vänner online varje dag? Anpassa gärna exemplen utifrån målgruppen.
- Är gruppen mer bekväm kan man be dem att uppskatta mer exakt tid eller göra frågan som en fyra-hörn-övning. Exempelvis 0-5h, 6-10h, över 10h, och öppet hörn.
- Huvudbudskap: Hur skyddar du det som är ditt när upp mot halva livet är digitalt? Små val kan få stora konsekvenser, idag ska vi lära oss verktyg för att bli mer säkra online.

Digital rustning



Bild 2–3 i presentationen

Visa resten av videon:



<https://www.youtube.com/playlist?list=PLIk39hnHx0Lt-DBDkAmPB3x6Jl4iJaf22>

När något går fel: Börja med att bekräfta att det är vanligt att något går fel men att ju mer medveten man är desto mindre risk att det händer.

Vanliga problem som kan uppstå:

- Ett för simpelt lösenord leder till kapat konto
- En blufflänk snor din info
- Någon kräver dig på pengar eller annat för att ge tillbaka ett konto

Det är lätt att tänka att ”det händer inte mig” och att många gör så, men en av tre ungdomar har fått ett konto hackat.

Dela gärna med dig om du har en personlig erfarenhet eller om någon elev är bekväm med att dela med sig. Verkliga exempel är ofta bättre än påhittade exempel och sänker stigmat av att känna skam kring det.

Skydda din data med...



Bild 4–5 i presentationen

Nu ska vi gå från att förstå hoten till att lära oss konkreta verktyg för att skydda oss. Vi börjar med en kort demonstration.



Demonstration – hur snabbt knäcks ett lösenord?

Gå in på <https://www.expressvpn.com/password-generator> och testa ett typiskt svagt lösenord, till exempel "katten123". Låt eleverna se hur snabbt det kan knäckas. Ställ sedan frågan: vad tror ni krävs för att göra ett lösenord säkert? Häng kvar vid frågan – vi återkommer till lösenordskontrollerna i slutet av avsnittet.

... lösenord



Bild 6–16 i presentationen

Ett lösenord är mer än bara ett skydd – det är ett bevis på vem du är. När du loggar in på en webbplats är lösenordet det som bekräftar din identitet: bara du känner till det, och därför fungerar det som ett digitalt ID. Kommer någon annan över ditt lösenord kan de alltså inte bara komma åt ditt konto – de kan låtsas vara du. Det är därför lösenordsval spelar så stor roll, vi går igenom fem principer som gör ett lösenord säkert.

1. Långt: Visa ett klassiskt kombinationslås med tre siffror (0–9). Hur många kombinationer finns det? Svaret är $10 \times 10 \times 10 = 1\,000$. Det kan man testa ganska snabbt. Men lägg till en fjärde siffra och det blir $10 \times 10 \times 10 \times 10 = 10\,000$ kombinationer – tio gånger fler. Ju längre, desto svårare att knäcka. Samma princip gäller lösenord: varje tecken man lägger till mångdubblar antalet möjliga kombinationer.

Tips: Det här kan göras till en kort matteövning. Låt eleverna själva räkna ut hur många kombinationer som är möjliga med tre, fyra och fem siffror.

2. Blandade tecken: Tänk tillbaka på kombinationslåset – det hade bara siffror (0–9), alltså 10 möjligheter per position. Men tänk om vi även kan använda bokstäver (a–ö, 29 stycken) och siffror? Då har vi 39 möjligheter per position istället för 10, och antalet kombinationer ökar enormt. Lägg till stora bokstäver och symboler som ! och # och det blir ännu fler. Det är därför ett bra lösenord blandar siffror, små och stora bokstäver samt symboler.

Brute force-attacker

En professionell hackares dator kan potentiellt testa miljoner lösenord i sekunden. Att bara testa lösenord på måfå kallas för en brute force-attack. Att testa alla potentiella koder för ett kodlås med tre symboler görs otroligt snabbt. Därför är det bra att ha minst 14 tecken i sina lösenord. Använd därför gärna en lösenordsfras så att du kan komma ihåg det.

3. Unikt: Varje konto ska ha sitt eget lösenord. Anledningen är enkel: om ett lösenord läcker i en dataläcka testar hackare samma lösenord på andra tjänster. Har du samma lösenord på flera ställen riskerar du alla de kontona på en gång. Det kan låta överväldigande att ha ett unikt lösenord för varje konto – men det finns verktyg som gör det hanterbart, och det kommer vi till strax.

4. Svårt att gissa: Lösenord som innehåller personlig information – namn, födelseår, husdjur, favoritlag – är det första en hackare testar. Fråga eleverna: vad skulle någon kunna ta reda på om er genom att titta på era sociala medier? Just de sakerna ska inte finnas i ett lösenord.

5. Lätt att komma ihåg: Ett lösenord som man inte kommer ihåg är värdelöst. Lösningen är lösenordsfraser, till exempel Kattenåt3pannkakorigår!. De är långa, svåra att gissa, men lätta att komma ihåg som en bild i huvudet.

Tips! Lösenordshanterare

En lösenordshanterare är ett program eller en app som sparar alla dina lösenord åt dig i ett krypterat valv. Du behöver bara komma ihåg ett enda lösenord – huvudlösenordet – för att komma åt alla andra. Programmet kan också skapa starka, slumpmässiga lösenord åt dig, så att varje tjänst får ett eget unikt lösenord utan att du behöver hitta på eller memorera dem själv.

Lösenordshanterare anses av IT-säkerhetsexperten vara ett av de bästa verktygen för att skydda sina konton. Många är gratis att använda och finns som appar, webbläsartillägg och program för datorn. Exempel på välkända lösenordshanterare är Bitwarden (gratis och öppen källkod), 1Password och den inbyggda lösenordshanteraren i Google Chrome eller Apples iCloud-nyckelring.

Fördelar: Du behöver bara komma ihåg ett lösenord. Alla andra kan vara långa, slumpmässiga och unika – det som gör dem starkast. Många lösenordshanterare varnar också om ett av dina lösenord har förekommit i en dataläcka.

Nackdelar: Om någon får tillgång till ditt huvudlösenord kan de potentiellt nå alla dina konton. Därför är det extra viktigt att huvudlösenordet är starkt – gärna en lång lösenordsfras – och att du aktiverar tvåfaktorsautentisering på lösenordshanteraren själv.

Övning 1 – Skapa en lösenordsfras

Låt eleverna använda det de just lärt sig för att skapa en egen lösenordsfras. Uppgiften är att komma på en lösenordsfras som uppfyller kriterierna ni just gått igenom: den ska vara lång (minst 14 tecken), innehålla en blandning av stora och små bokstäver, siffror och symboler, och vara lätt att komma ihåg. Skriv gärna upp några exempel på tavlan, till exempel "JagälskarjOrdgubbsglass*" eller "Kattenåt3pannkakorigår!".

Poängtera att lösenordsfrasen de skapar i övningen inte ska bli deras riktiga lösenord till alla tjänster – varje tjänst behöver sitt eget unika lösenord. Syftet är att träna på hur man tänker när man skapar ett starkt lösenord, så att de har det med sig nästa gång de behöver skapa ett nytt – eller ser över sina befintliga lösenord efter lektionen och ändra till starkare.

Övning 2 – Testa lösenordets styrka



Kommer ni ihåg demonstrationen i början – hur snabbt "katten123" kunde knäckas?

Nu är det elevernas tur att testa. Gå tillbaka till <https://www.expressvpn.com/password-generator> och låt eleverna testa en lösenordsfras som liknar den de just skapade.

Viktigt: Eleverna ska aldrig testa med ett riktigt lösenord. Be dem använda ett påhittat lösenord som liknar det de skulle kunna använda – det räcker för att se skillnaden. Låt dem jämföra: vad händer om man testar "katten123" jämfört med "Kattenåt3pannkakorigår!"? Skillnaden i uppskattad tid brukar vara slående och gör poängen om längd och komplexitet väldigt konkret.

Teknisk fördjupning: Men skyddar inte företagen mitt lösenord?

Seriösa företag sparar inte ditt lösenord i klartext. Istället omvandlas det genom en teknik som kallas hashning – en form av kryptering som fungerar i en riktning. Det betyder att lösenordet görs om till en lång, till synes slumpmässig kod som inte går att omvandla tillbaka. Ditt lösenord "@superSnällaSilverSara9" kan till exempel se ut så här i databasen:

165128C12A859FB481915A5388ADE526

Inte ens företaget självt kan läsa ditt lösenord. Men det skyddet har en svaghet: om databasen läcker – som i en känd dataläcka, till exempel den mot systemleverantören Miljödata, kan hackare använda sina datorer för att testa enorma mängder lösenord och jämföra resultaten mot de läckta hasharna. Svaga och vanliga lösenord som "katten123" knäcks på sekunder, oavsett hur bra hashningen är. Det är som att ha ett avancerat kassaskåp med en kod på tre siffror – skåpet i sig är starkt, men koden är för enkel.

Det är därför det spelar så stor roll att ditt lösenord är starkt, långt och unikt.

... tvåfaktorsautentisering (2FA/MFA)

Ett starkt lösenord är en bra grund – men vad händer om det ändå läcker i en dataläcka, eller om någon lyckas lista ut det? Det är här tvåfaktorsautentisering kommer in. 2FA innebär att du behöver två olika saker för att logga in: först ditt lösenord, och sedan en engångskod som skickas till en annan enhet, oftast din mobil. Tanken är enkel – även om någon får tag på ditt lösenord kommer de inte in utan den andra faktorn. Det är som att ha både ett lås och en säkerhetskod på ytterdörren.

Koppling till vardagen: Fråga om någon av eleverna redan använder 2FA. Nämn populära appar och tjänster där det går att aktivera, som Instagram, Discord, Gmail och Roblox. Poängtera att det bara tar en minut att slå på och att det gör stor skillnad för säkerheten. Rekommendationen är enkel: aktivera alltid 2FA där möjligheten finns.

Har du lärt dig hur du skyddar dig?

Tipspromenad

Dela in klassen i mindre grupper och låt dem göra tipspromenaden. Alternativt kan man köra frågorna som ett vanligt quiz. Arbetsbladet Tipsrunda (inkl separat facit med förklaringar) finns som digitalt komplement i *Är du säker? Arbetsblad och filmlänkar – Högstadiet*.

Tipspromenaden innehåller frågor som rör alla tre lektionerna i materialet. Den fungerar även bra om klassen bara har gjort lektion 3, eftersom frågorna handlar om grundläggande cybersäkerhetskompetenser som eleverna möjligtvis redan har. Resultatet kan också ge en bra bild av vad som eventuellt behöver fördjupas vidare i klassrummet.

Säkerhet är en vana

Avslutning

Under den här lektionen har vi gått från att förstå varför vår data behöver skyddas till att lära oss konkreta verktyg för att göra det: starka lösenord, lösenordshanterare och tvåfaktorsautentisering. Det är en bra grund, men digital säkerhet är inte något man fixar en gång och sedan glömmer. Tekniken utvecklas hela tiden, och med den förändras också hoten. Det som är ett säkert lösenord idag kan bli knäckbart i framtiden, och nya typer av bedrägerier kommer att dyka upp.

Det viktigaste att ta med sig är därför inte bara verktygen, utan vanan att tänka på sin digitala säkerhet – att regelbundet se över sina lösenord, vara uppmärksam på nya hot och våga fråga när något känns osäkert.

Sammanfatta gärna lektionens viktigaste punkter tillsammans med eleverna:

- Se över dina lösenord. Är de starka nog? Har du samma lösenord på flera ställen? Överväg att använda en lösenordshanterare.
- Aktivera tvåfaktorsautentisering på dina viktigaste konton – det tar en minut och gör stor skillnad.
- Prata med en vuxen om något känns fel eller om något har hänt online. Det är inte något att skämmas över – det är att vara smart.

Anknytningar till Lgr22

Från ”Skolans uppdrag”

Eleverna ska kunna orientera sig och agera i en komplex verklighet med stort informationsflöde, ökad digitalisering och snabb förändringstakt. [...] Det är också nödvändigt att eleverna utvecklar sin förmåga att kritiskt granska information, fakta och förhållanden och att inse konsekvenserna av olika alternativ.

Skolan ska bidra till att eleverna utvecklar förståelse för hur digitaliseringen påverkar individen och samhällets utveckling. Alla elever ska ges möjlighet att utveckla sin förmåga att använda digital teknik. De ska även ges möjlighet att utveckla ett kritiskt och ansvarsfullt förhållningssätt till digital teknik, för att kunna se möjligheter och förstå risker samt kunna värdera information.

Från ”Mål”

Skolans mål är att varje elev

- kan använda såväl digitala som andra verktyg och medier för kunskapssökande, informationsbearbetning, problemlösning, skapande, kommunikation och lärande
- kan använda sig av ett kritiskt tänkande och självständigt formulera ståndpunkter grundade på kunskaper och etiska överväganden

Samhällskunskap (åk 7-9)

Från Ämnets syfte:

Eleverna ska också ges verktyg att kritiskt granska hur olika aktörer försöker påverka samhällsutvecklingen genom information, ståndpunkter och argument i olika sammanhang och källor.

Information och kommunikation:

- Hur media produceras, distribueras och konsumeras samt vilka möjligheter och svårigheter det kan innebära för mediernas roll i ett demokratiskt samhälle.
- Nyhetsvärdering och hur den kan påverka människors bilder av omvärlden. Hur individer och grupper framställs i media, till exempel utifrån kön och etnicitet, och hur detta kan påverka normbildning och värderingar.

Granskning av samhällsfrågor:

- Lokala, nationella och globala samhällsfrågor och olika perspektiv på dessa.
- Kritisk granskning av information, ståndpunkter och argument som rör samhällsfrågor i såväl digitala medier som i andra typer av källor.

Rättigheter och rättsskipning:

- Friheter, rättigheter och skyldigheter i demokratiska samhällen. Dilemman som hänger samman med demokratiska rättigheter och skyldigheter, till exempel gränsen mellan yttrandefrihet och kränkningar i sociala medier.

Svenska (åk 7-9)

Från Ämnets syfte:

Undervisningen ska också bidra till att eleverna får förståelse för att sättet man kommunicerar på kan få konsekvenser för en själv och för andra människor. Därigenom ska eleverna ges förutsättningar att ta ansvar för det egna språket i olika sammanhang och medier.

Språkbruk:

- Språkbruk, yttrandefrihet och integritet i digitala och andra medier och i olika sammanhang.
- Skillnader i språkanvändning beroende på syfte, mottagare och sammanhang. Språkets betydelse för att utöva inflytande.

Informationssökning och källkritik:

- Informationssökning på bibliotek och på internet, i böcker och massmedier samt genom intervjuer.
- Hur man sovrar i en stor informationsmängd och prövar källors tillförlitlighet med ett källkritiskt förhållningssätt.

Tala, lyssna och samtala:

- Olika former av samtal. Att delta aktivt, uttrycka känslor, tankar och kunskaper, lyssna, ställa frågor och föra resonemang, samt formulera och bemöta argument.

Teknik (åk 7-9)

Teknik, människa, samhälle och miljö

- Internet och några andra globala tekniska system samt deras fördelar, risker och begränsningar.
- Möjligheter, risker och säkerhet vid teknikanvändning i samhället, däribland vid lagring av data.

Tekniska lösningar:

- Hur komponenter och delsystem benämns och samverkar inom tekniska system, till exempel informations- och kommunikationsteknik och transportsystem.

Vem står bakom projektet?

Cybersecurity Academy är ett gemensamt initiativ av den ideella organisationen Unga Forskare och IBM samt andra företag i teknikbranschen. Projektet är kostnadsfritt för skolor tack vare finansiering av IBM, partnerföretagens bidrag och uppdragsmedel från Myndigheten för civilt försvar (MCF).



Unga Forskare är en ideell organisation som finns för att ge unga förutsättningar att utveckla sitt intresse för naturvetenskap, matematik och teknik. Unga Forskare grundades 1977 och består idag av ett sextiototal föreningar med ca 10 000 medlemmar. Med ett stort antal nationella verksamheter och skolmaterial jobbar Unga Forskare för att nyfikenheten och intresset för naturvetenskap, teknik och matematik ska ha en självklar plats i ungas liv.



IBM Sverige är ett IT-företag som erbjuder affärssystem, programvaror och andra IT-relaterade produkter och tjänster till företagskunder. Tillsammans med andra företag och organisationer från teknikbranschen har IBM ett ansvar för hur de produkter och tjänster de levererar påverkar samhället. IBM vill därför stärka elevers och skolors kunskap om cybersäkerhet.



**Myndigheten
för civilt försvar**

Myndigheten för civilt försvar är en statlig myndighet med ansvar för att stödja samhällets beredskap för olyckor, kriser och civilt försvar. Avdelningen för cybersäkerhet och säkra kommunikationer har bl.a. till uppgift att samordna arbetet med samhällets informationssäkerhet – från organisationer, kommuner, andra myndigheter och företag, till enskilda individer.

TÄNK SÄKERT



NATIONELLT
CYBERSÄKERHETSCENTER



Polisen

Tänk säkert

Tänk säkert är en kampanj som drivs av Nationellt Cybersäkerhetscenter tillsammans med Polisen för att öka allmänhetens medvetenhet om cybersäkerhet. Det här lektionsmaterialet har tagits fram av Cybersecurity Academy med stöd av kampanjmedel.

Nationellt cybersäkerhetscenter (NCSC) är en del av Försvarets radioanstalt och utgör navet för Sveriges cybersäkerhet. Genom att samordna insatser vid allvarliga cyberangrepp, ge stöd och rådgivning samt främja samverkan och kunskapsdelning bidrar NCSC till att höja cybersäkerheten i samhället och stärka Sveriges förmåga att förebygga, upptäcka och hantera cyberhot.