Cybersecurity Academy

Är du säker?

Cybersäkerhet i elevernas vardag – kunskap som gör skillnad

Lärarhandledning åk 4–6

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 mellanstadiet 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, tigrinska 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. Lektionen innehåller övningar om kombinatorik kopplade till lösenordssäkerhet, en valfri fördjupning om kryptering samt en tipsrunda som bonusmaterial.

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 8
Klicka bara ja! Eller? 8
Varför samlas data in? 10
Ta kontroll över din data 11

Lektion 2 – Klicka smart 12
Vår digitala värld och dolda faror 13
Klicka smart 13
Bluffdetektiv 14
Skapa en egen bluff 15
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
Kombination av tecken 20
... tvåfaktorsautentisering (2FA/MFA) 22
Bonusmaterial: Har du lärt dig hur du skyddar dig? 22
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. Workshopsen 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-experter och organisationer inom utbildning och forskning och riktar sig främst till högstadie- och gymnasieelever. För lärare finns det mycket värdefullt innehåll att ta del av, bland annat en fortbildningskurs i cybersäkerhet. Elever i mellanstadiet som vill fördjupa sina kunskaper kan också hitta intressanta kurser på plattformen.

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

Ett digitalt vardagsliv

Bild 1–4 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.

Övning – Vad gör du på nätet?

Börja med en 4-hörn-övning där eleverna får fundera och ta ställning till hur mycket de surfar på internet, vad de gör online och hur de mår på nätet. Förklara att du kommer ställa några frågor och att de ska svara genom att ställa sig i ett av rummets fyra hörn. Varje hörn står för ett eget svar. Ett av hörnen bör vara öppet för elevers egna förslag. Efter att barnen ställt sig i hörnen, fråga om någon vill motivera sitt svar.

Hur ofta surfar du på nätet?

en gång i veckan	några gånger i veckan	varje dag	annat

Vad gör du på nätet?

spelar spel	kollar på Youtube, TikTok, Instagram	chattar med mina kompisar	annat

Hur mycket tid spenderar du online per dag?

några minuter	en timme	flera timmar	annat

Trivs du bra med det du gör på nätet?

ja, alltid	ibland ja, ibland nej	nej, inte riktigt	annat

Med vem pratar du om vad du gör online?

mina kompisar	mina föräldrar	ingen	annat

Använd svaren som en brygga till resten av lektionen:
”Ni är online mycket, men vet ni vilka spår ni lämnar?”.

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, 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 kommenterar på.

Oaktsamt beteende online

Bild 5–6 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 – Mellanstadiet*. 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 7 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 scrollar 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 8–12 (15) 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.
- 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

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 säkerhetsskäl. Därför är det viktigt att förstå vad man faktiskt godkänner.

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.

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

Valfritt: 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 16–19 i presentationen

Den här delen av lektionsupplägget består av tre diskussionsfrågor. Frågorna kan användas för diskussioner i helklass eller i mindre grupper.

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. De vill ha användarens information och räknar med att vi är lite lata.

En lite mer generös tolkning 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?

Diskutera vad varje enskild aktör kan ha för motiv. Välj aktörer som passar målgruppen.

- Stadium
  - Spara varukorg
  - Riktad reklam
  - Spara inloggning
  - Spara position för närmaste butik
- Netflix
  - Spara vilka filmer du sett
  - Spara inloggning
  - Spara din position för att kontrollera att kontot bara används av ett hushåll
- En hackare
  - Falska sidor som samlar in information och säljer vidare, eller rena bedrägerier. Hackare kan också stjäla cookies för att ’låtsas’ vara en vanlig användare och komma åt andras konton.

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

Diskutera vilka aktörer man känner sig bekväm med att dela cookies med. Det finns inga rätta svar – syftet är att leda eleverna till att ta egna medvetna beslut.

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.

Fråga eleverna: Hur går det ihop? Ni använder appar som TikTok, Snapchat, Instagram och YouTube – vilka av dem betalar ni för? Är de verkligen gratis?

När en tjänst är gratis betalar du ofta med din information istället. Utan att vi alltid tänker på det blir vi själva produkten. Diskutera gärna vidare:

- Hur känns det att veta att företag samlar data om er? Är det lugnt eller känns det otryggt?
- Vad kan man göra om man vill begränsa mängden data man delar?

Det betyder inte att man måste sluta använda internet – men att man kan göra det mer medvetet. Här är konkreta saker man kan göra:

- Kolla inställningarna i dina appar – behöver appen verkligen ha tillgång till kameran, mikrofonen eller din position?
- Acceptera inte alla cookies automatiskt – välj ”bara nödvändiga”.
- Det finns sökmotorer som inte sparar dina sökningar, till exempel DuckDuckGo (duckduckgo.com) och Startpage (startpage.com).

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. Små val gör skillnad.

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 – Mellanstadiet*)

Delar i lektionsförslaget

Del	Typ	Tid
Vår digitala värld och dolda faror	Lärarledd introduktion med presentation	5 min
Klicka smart	Film (Klicka smart) + diskussion	10 min
Bluffdetektiv	Gruppövning med arbetsblad	20 min
Skapa en egen bluff (åk 4; valfri fördjupning åk 5–6)	Kreativ övning i par	20 min
Har dina uppgifter läckt? (åk 5–6)	Lärarledd genomgång + övning	10 min
Skydda dig mot nätbedrägerier	Lärarledd avslutning	5 min

Lektionen är anpassad för att fungera i hela mellanstadiet. I åk 4 ingår ”Skapa en egen bluff”, i åk 5–6 ersätts det momentet av ”Har dina uppgifter läckt?”, men båda momenten kan göras om tid finns.

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 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.

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.

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.

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 – Mellanstadiet*. 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. Men varför fungerar det egentligen? Det handlar om något som kallas den mänskliga faktorn, att det ofta är lättare att lura en människa än att hacka en dator.

Hackare använder framför allt tre tekniker. Fråga eleverna om de känner igen orden och vad de tror att de betyder:

- **Phishing** – vad låter det som? (Fishing/fiska.) Man ”fiskar” efter offer genom att skicka bluffmejl, bluff-sms eller bluffmeddelanden till många personer och hoppas att någon nappar.
- **Social engineering** – vad kan ”social” och ”engineering” betyda var för sig? Det handlar om att manipulera människor genom att spela på känslor: stress, nyfikenhet eller vilja att hjälpa. Till exempel att ringa och låtsas vara från skolan för att få ut information. På svenska kan man säga social manipulation.
- **Malware** – ordet är ihopsatt av ”malicious” (elakt) och ”software” (program). Det är skadliga program som kan installeras på din dator eller telefon utan att du märker det, till exempel när du klickar på en blufflänk.

Gemensamt för alla tre är att de riktar sig mot människan, inte mot tekniken. Det är därför vi behöver bli bluffdetektiver!

Bluffdetektiv

Bild 5–14 i presentationen

Nu vet vi vilka tekniker bedragare använder. Men hur känner man igen en bluff i verkligheten? Det är inte alltid lätt – bluffar är designade för att se äkta ut.

Fråga eleverna: Om ni fick ett meddelande just nu – vad skulle få er att misstänka att det är en bluff? Samla svaren och komplettera med dessa kännetecken:

- De ser ut som helt vanliga meddelanden – sms, DM:s eller hemsidor som liknar riktiga.
- De har ofta en stressande ton: ”du måste svara inom 24 timmar”, ”ditt konto stängs”. De vill att du ska agera utan att tänka efter.
- De erbjuder något som verkar för bra för att vara sant – gratis saker, vinster, pengar.

Exempel på bluffar

Konkreta exempel på vanliga nätbedrägerier. Visa upp exemplen, dela sedan in eleverna i grupper och låt dem titta närmare. Exemplen finns i powerpointpresentationen och som arbetsblad i det digitala komplementet *Är du säker? Arbetsblad och filmlänkar – Mellanstadiet*.

- **Phishing-SMS/epost:** Ett sms som ser ut att komma från skolan, eller ett mejl som verkar vara från ett spelkonto – det kan vara phishing. Du kan alltid dubbelkolla genom att kontakta avsändaren på ett annat sätt. Logga alltid in själv via officiella appar eller googla, följ inte länkar om du är det minsta osäker.
- **Spelbedrägeri:** I spel som Roblox, Fortnite och Minecraft förekommer bluffar där någon erbjuder gratis skins, robux eller andra föremål. Ofta leder länkarna till falska inloggningssidor som stjäl dina kontouppgifter. Kom ihåg: riktiga spelbolag ger inte bort saker via chattar eller DM:s.
- **Deepfake/videobedrägeri:** AI kan idag användas för att skapa realistiska men helt falska videor och röstinspelningar, så kallade deepfakes. Kriminella utnyttjar detta för att lura människor. 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.

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? Vilka varningssignaler hittar ni?
- Vad tror ni kan hända om man klickar på länken eller lämnar ut uppgifter?

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/http också).
- Vad skulle aktören vilja med mina inloggningsuppgifter?

AI som verktyg i bedrägerier

Phishing har blivit ett av de vanligaste bedrägarisätten online och har effektiviserats av AI. Deepfakes är falska ljud- och videoinspelningar som kan vara svåra att skilja från äkta. Med dagens teknik behövs bara några sekunders ljudinspelning för att göra en falsk inspelning med en fejkad röst. Därför måste vi vara försiktiga med vad vi lägger upp online. Prata gärna hemma om hur ni ska agera om ni tror att någon försöker lura er via video eller ljud.

Skapa en egen bluff

(åk 4; valfri fördjupning för åk 5–6)

Det här momentet passar särskilt bra för yngre elever eller som fördjupning om tid finns.

Eleverna har just övat på att genomskåda bluffar. Nu vänder vi på det: de får tänka som en bedragare.

Dela in eleverna i par. Varje par ska hitta på ett eget bluffmeddelande, det kan vara ett sms, ett meddelande i ett spel eller en annons. De ska använda minst två av varningssignalerna som klassen just gått igenom, till exempel brådskande språk, ett erbjudande som verkar för bra för att vara sant eller en begäran om känsliga uppgifter.

Paren presenterar sedan sin bluff för ett annat par eller för klassen. De andra ska genomskåda den: vilka varningssignaler hittar ni? Vad borde mottagaren göra?

Har dina uppgifter läckt?

(åk 5–6)

Bild 15–16 i presentationen

Det här avsnittet passar bäst för äldre mellanstadieelever (åk 5–6) som har egna e-postkonton och viss vana vid digitala tjänster. Om du bedömer att det inte passar din klass kan du hoppa över övningen och gå direkt till avslutningen. Kunskapen om dataläckor tas då upp i samband med lösenordsavsnittet i Lektion 3 istället.

Ibland händer det att företag och tjänster blir hackade och att information om deras användare stjäls – till exempel e-postadresser, lösenord eller telefonnummer. Det kallas för en dataläcka. Det knepiga är att man sällan märker det. Det kommer inga varningsmeddelanden och inget som känns annorlunda. Uppgifterna kan ligga ute på nätet länge utan att man vet om det.

Fråga gärna eleverna: Hur tror ni att man märker om ens uppgifter har läckt? Låt dem diskutera kort – 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.

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.
- 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 utan de handlar oftast om att lura människor. Phishing, 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 att stanna upp och tänka efter.

Sammanfatta gärna de viktigaste tumreglerna tillsammans med eleverna:

- **Stanna upp.** Om något känns brådskande, 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.
- **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. 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 tipspromenad (finns som digitalt komplement *Är du säker? Arbetsblad och filmlänkar – Mellanstadiet*)
- Utskrivna arbetsblad för krypteringsövningen (finns som digitalt komplement *Är du säker? Arbetsblad och filmlänkar – Mellanstadiet*)
- Pennor och papper

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 med... • ... lösenord – övningar och kombinatorik – exkurs kryptering • ... tvåfaktorsautentisering	Lärarledd genomgång + praktiska moment (kan kompletteras med övningar)	20–40 min
Tipspromenad (bonus)	Quiz/tipsrunda i grupper	15 min
Säkerhet är en vana	Lärarledd avslutning	5 min

Lektionen har en flexibel struktur. Kärninnehållet tar ca 35 minuter. Övningarna om kombinationer och krypteringsexkursen är valfria fördjupningar som kan göras i anslutning eller som separata pass. Tipspromenaden är bonusmaterial som täcker alla tre lektionernas teman och fungerar bäst som avslutande aktivitet efter att klassen gjort hela materialet.

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. I den här lektionen handlar det 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 – Mellanstadiet*. 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 2–4 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 5-13; 16-23 i presentationen (rekommenderat upplägg för åk 4-5)

Bild 5-9; 14-23 (rekommenderat upplägg för åk 6)

Nu ska vi gå från att förstå hoten till att lära oss konkreta verktyg för att skydda oss.

... lösenord

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

Den första principen är att ett lösenord ska vara långt. Tänk på en pinkod till en telefon. Varje siffra kan vara 0–9, alltså 10 möjligheter. En ensiffrig kod har bara 10 kombinationer, och en fyrsiffrig kod har 10 000. Varje siffra man lägger till gör det många gånger svårare att gissa rätt. Samma princip gäller lösenord – men hur stor skillnad gör det egentligen? Vi testar.

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. Ni kommer komma tillbaka till sidan senare för att testa med ett långt lösenord.

Övningar

Varför lösenordets längd spelar roll

Övningarna nedan förklarar varför lösenordets längd spelar så stor roll.

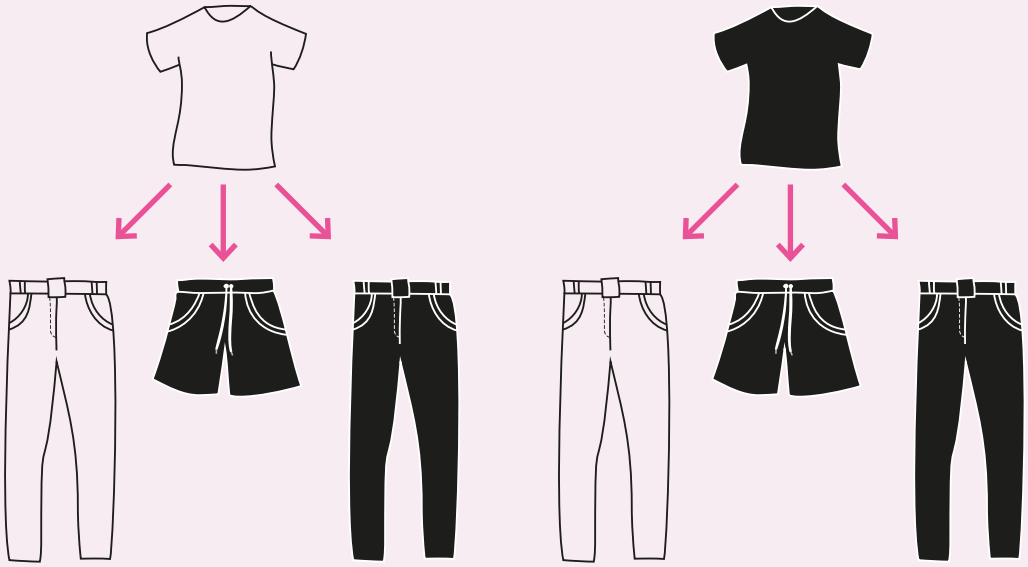
Kombination av klädesplagg

(åk 4–5)

Bilder till övningen ligger i powerpointpresentationen, alternativt kan du rita på tavlan eller dela ut arbetsbladet Kombinatorik.

Föreställ er att ni har några få favoritkläder som ni vill ha på er så ofta som möjligt. Hur många kombinationer kan du ha av 2 t-shirts, 2 par långa byxor och 1 par korta byxor?

Rita på tavlan vilka kombinationer som finns. Varje t-shirt kan kombineras med antingen en av de långa byxorna eller de korta byxorna. Alltså: 2 × 3 = 6 kombinationer.



Vad händer om du får en t-shirt och ett par byxor till? Nu: 3 × 4 = 12.

Bara två klädesplagg till ger dubbelt så många kombinationsmöjligheter!

Kombination av tecken

(åk 6)

Låt eleverna räkna hur många tecken ett vanligt tangentbord har och sedan försöka räkna ut hur många olika kombinationer det finns för ett lösenord på 6, 10 och 14 tecken.

Lärdom: Fler positioner ger fler kombinationer. Det leder oss till nästa princip.

2. Blandade tecken: PIN-koden hade bara siffror (0–9), alltså 10 möjligheter per position. Men tänk om vi även kan använda bokstäver? Då får vi många fler möjligheter per position, och antalet kombinationer ökar enormt. Det är därför ett bra lösenord blandar siffror, små och stora bokstäver samt symboler som ! och #.

3. Unikt: Varje konto ska ha sitt eget lösenord. 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.

4. Svårt att gissa: Lösenord som innehåller personlig information – namn, födelseår, husdjur – 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 småfågel-tassa-explosion. De är långa, svåra att gissa, men lätta att komma ihåg som en bild i huvudet. Skriv gärna upp några exempel på tavlan.

Övning 1 – Skapa en lösenordsfras

Låt eleverna komma på en lösenordsfras som uppfyller kriterierna: lång (en bra tumregel: sikta på minst 14 tecken.), blandade tecken och lätt att komma ihåg. Poängtera att frasen inte ska bli deras riktiga lösenord, syftet är att träna tänkesättet.

Övning 2 – Testa lösenordets styrka

Gå tillbaka till https://www.expressvpn.com/password-generator och låt några elever testa sina lösenordsfraser (inte riktiga lösenord). Jämför med ”katten123” från demonstrationen i början. Skillnaden brukar vara dramatisk och gör principerna konkreta.

Exkurs: Kryptering – hur skyddas lösenord?

Det här avsnittet kan göras i direkt anslutning till lösenordsdelen eller som en fristående fördjupning.

Vi har pratat om hur man gör bra lösenord. Men vad händer med lösenordet efter att du skrivit in det? Företag och tjänster sparar inte ditt lösenord i klartext, det vore som att lämna nyckeln i dörren. Istället omvandlas det till en lång rad tecken med hjälp av en teknik som kallas hashning. Det fungerar ungefär som en köttkvarn: man kan stoppa in köttet och få ut färs, men man kan inte göra tillbaka färsen till kött. På samma sätt kan man omvandla ett lösenord till en hash, men inte göra tillbaka hashen till lösenordet.

Det innebär att även om en hackare stjäl databasen med hashade lösenord kan de inte direkt se vad lösenorden är. Men om lösenordet är svagt – kort, vanligt eller förutsägbart – kan hackaren ändå knäcka det genom att testa vanliga lösenord och jämföra. Det är därför starka lösenord är så viktiga: ju starkare lösenord, desto svårare att knäcka hashen.

Hashning är ett exempel på en teknik för att skydda information. Det bredare begreppet kallas kryptering – att göra information oläslig för alla utom den som har rätt nyckel. Hashning är en speciell variant där det inte ens finns en nyckel tillbaka, men grundidén är densamma: göra det omöjligt att läsa utan rätt kunskap. Ett av de äldsta exemplen på kryptering är Caesarchiffret, där man förskjuter varje bokstav ett visst antal steg i alfabetet.

Övning – Knäck Caesars lösenord: Dela ut arbetsbladet ’Knäck Caesars lösenord’ (instruktioner och facit finns i arbetsbladet). Övningen har tre delar:

- Del 1 – Symbolchiffer: Eleverna använder en nyckel där varje bokstav är en ikon (hus, hjärta, dödskalle osv.) för att avkoda Caesars lösenord.
- Del 2 – Caesarchiffer: Eleverna använder en bokstavsförskjutning (A=B, B=C osv.) för att avkoda fem lösenord.
  Lösenorden är: KATTUNGE, FROSTSKOGEN, HEJ, LÖSENORD, JAGHARTREGULAHUNDAR.
- Del 3 – Ranka lösenorden: Eleverna sorterar de fem lösenorden från säkrast till svagast.
  Rätt ordning: JAGHARTREGULAHUNDAR (säkrast), FROSTSKOGEN, KATTUNGE, LÖSENORD, HEJ (svagast).

... tvåfaktorsautentisering (2FA/MFA)

Ett starkt lösenord är en bra grund, men vad händer om det ändå läcker? Då kommer tvåfaktorsautentisering 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. 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 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.

Bonusmaterial: Har du lärt dig hur du skyddar dig?

Det här momentet är en tipspromenad som fungerar utmärkt som avslutande aktivitet efter att klassen har gjort alla tre lektionerna i materialet. Frågorna täcker alla tre lektionernas teman – digitala fotavtryck, nätbedrägerier och digital rustning – och ger en bra bild av vad eleverna har tagit med sig. Tipspromenaden kan också användas fristående, till exempel som uppvärmning vid ett senare tillfälle eller som repetition.

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 – Mellanstadiet*.

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 och tvåfaktorsautentisering. (Om ni har gjort krypteringsövningarna: Och hur lösenord skyddas bakom kulisserna.) 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 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?
- 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 4–6)

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 digitala och andra medier kan användas ansvarsfullt utifrån sociala, etiska och rättsliga aspekter.

Granskning av samhällsfrågor:
- Hur budskap, avsändare och syfte kan urskiljas och granskas med ett källkritiskt förhållningssätt i såväl digitala medier som i andra typer av källor som rör samhällsfrågor.

Svenska (åk 4–6)

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 språkbruket i olika sammanhang och medier.

Språkbruk:
- Ansvarsfullt agerande vid kommunikation i digitala och andra medier.

Informationssökning och källkritik:
- Hur man jämför källor och prövar deras tillförlitlighet med ett källkritiskt förhållningssätt.

Tala, lyssna och samtala:
- Olika former av samtal. Att lyssna aktivt, ställa frågor, uttrycka tankar och känslor samt resonera och argumentera i olika samtalssituationer och i samband med demokratiska beslutsprocesser.

Teknik (åk 4–6)

Teknik, människa, samhälle och miljö
- Konsekvenser av teknikval: olika tekniska lösningars för- och nackdelar för människa och miljö.

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 sextiotal 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 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

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.