Cybersecurity Academy

Digital rustning

Lärarhandledning åk 7–9 och Gymnasiet

Lärarhandledning

Sammanfattning

Cybersecurity Academy är ett projekt inom IT-säkerhet som erbjuder utbildning i nätsäkerhet för elever och lärare. Syftet med projektet är att sprida kunskap om ett ansvarsfullt användande av internet och stärka elevers digitala kompetens.

Det här lektionsmaterialet syftar till att introducera elever till vikten av digitalt självförsvar, ge dem konkreta verktyg för att skydda sin personliga data online, och stärka deras känsla av handlingskraft.

Tanken med den här lärarhandledning är att du som lärare själv ska kunna jobba med IT-frågor i klassrummet. Du behöver inte ha särskild IT-kompetens eller undervisa i teknik utan IT-ämnen i detta material behandlas ur ett samhällsperspektiv. Som passar i många olika ämnen.

Utöver det här materialet finns två andra lektionsförslag med filmer som Cybersecurity Academy har tagit fram med stöd från kampanjen Tänk säkert. De heter *Ditt digitala fotavtryck* och *klicka smart*.

Inom Cybersecurity Academy erbjuder vi även skolor att ta del av kostnadsfria föreläsningar med en IT-expert och ett större undervisningsmaterial för att fördjupa elevernas kunskaper. Inklusive ett digitalt lektionsmaterial på den digitala utbildningsplattformen SkillsBuild.

I det här undervisningsmaterialet ingår:

- Kort film som introducerar ämnet, finns på svenska, lätt svenska och med undertexter på engelska, arabiska, somaliska och tigrinska
- Lärarhandledning med förslag på lektionsupplägg och övningar
- Arbetsblad med tipsrunda/quiz
- Powerpointpresentation med anteckningar

www.ungaforskare.se

Materialet finns tillgängligt digitalt på cybersecurityacademy.se

Författare:
Max Vinger
Martina Sandgren

Tryckår:
2025, version 1.0

Innehåll

Lärarhandledning 2

Sammanfattning 2

Innehåll 3

Bakgrund 4

Om Cybersecurity Academy 4
Syfte 4

Översikt 5

Mål 5
Tidsåtgång 5
Material 5
Delar i lektionsförslaget 5
Mer material på ämnet 5

Lektionsförslag 6

Den digitala vardagen - en nyckelfråga 6
Digital rustning 6
Verktyg för att försvara sig 6
Har du lärt dig hur du skyddar dig? 9
Nu har du en rustning 9

Arbetsblad: Tipsrunda 10

Mer material på ämnet 13

Andra filmer med lektionsförslag 13
Digitala lektioner i SkillsBuild 13
Boka föreläsning med IT-expert 13

Vem står bakom projektet 14

Bakgrund

Vi lever idag i ett samhälle där stora mängder information och data lagras, bearbetas och kommuniceras med stöd av informationsteknik (IT). Människors vardag är full av digital kommunikation och informationsbehandling och vi har alla värdefull information på olika ställen – i mobilen, i e-posten, i plånboken, i sociala medier samt i molntjänster. Samtidigt sker det en tydlig ökning av incidenter såsom dataintrång, bedrägerier och spridning av skadlig kod. Bakom detta ligger enskilda individer men också organiserad brottslighet, terrorister och statsmakter. Medvetenheten om risker i den digitala världen och kunskapen om hur man kan skydda sig är av stor betydelse.

Barn och ungdomar spenderar en stor del av sin tid online: enligt studien Svenskarna och internet (2021) använder 98 % av mellanstadiebarnen internet dagligen. 9 av 10 är på sociala medier dagligdags och sociala medier som Youtube och tv-kanalernas webbplatser är mellanstadiebarnens främsta nyhetskälla.

Om Cybersecurity Academy

Cybersecurity Academy är ett projekt inom IT-säkerhet som erbjuder utbildning i nätsäkerhet för elever och lärare. Syftet med projektet är att sprida kunskap om ett ansvarsfullt användande av internet så att elever tidigt lär sig att skapa säkra vanor på nätet. Unga är snabba och duktiga på att använda ny teknik som appar och internettjänster, men det är vi vuxna som behöver hjälpa dem utveckla förmågan att vara källkritiska, kunna bedöma risker och förstå konsekvenser.

Initiativets utbildningsmaterial för skolan består av en föreläsning som hålls av IT-experter, tryckt och digitalt lektionsmaterial för att du som lärare ska kunna arbeta vidare med IT-frågor i klassrummet. Genom att koppla digitaliseringens roll till de globala målen i det här lektionsmaterialet vill vi bredda bilden av teknik. Vi kan också tidigt göra barnen medvetna om framtida globala risker och ge dem verktyg att hantera dessa på ett för dem positivt sätt.

Utöver det arrangerar vi lärarfortbildningar, föreläsningar för föräldrar samt lovskolor och fritidsaktiviteter för IT-intresserade ungdomar.

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 projektmedel från MSB (Myndigheten för samhällsskydd och beredskap).

Syfte

Syftet med Cybersecurity Academy är att öka kunskapen om ett säkert användande av internet. Genom att lära unga hur uppgifter på nätet kan spridas och hur de kan skapa bra lösenord för att skydda sina uppgifter lägger vi en av grunderna till säkra vanor inför ett framtida vuxenliv. Med allt fler tjänster och data lagrat online är detta viktigt för alla i samhället.

Projektet kopplar dessutom digitaliseringen till de globala målen. Digitalisering är inte ett självändamål utan ett medel som kommer hjälpa oss att lösa en del av de globala utmaningarna. Eleverna ska få insikt i vikten av digitaliseringens roll och IT-säkerhetsfrågor inte minst för att själva kunna bidra till att skapa ett hållbart samhälle. Initiativet ska också inspirera eleverna inom teknikområdet och öppna deras ögon för nya yrkesroller.

Översikt

I det här materialet finns en film som är tänkt att skapa diskussion kring digitala fotavtryck samt tillhörande fördjupande övningar och diskussioner. Alla delar är tänkta att kunna användas fristående men de ligger i en föreslagen ordning för att bygga upp en röd tråd om man använder flera eller samtliga delar av lektionsupplägget.

Mål

Efter lektionen ska eleverna kunna:

- Förstå att deras digitala data är värdefull och behöver skyddas.
- Tre grundläggande principer för digitalt självförsvar (starka lösenord, tvåstegsverifiering, känna igen bluffar).
- Känna till att de kan agera för att skydda sig själva online och känna till verktyg för att göra detta.

Tidsåtgång

Bedömningarna är ungefärliga och det går att justera utifrån grupp. Filmen är drygt 2 minuter lång så för att bara se filmen och diskutera den behövs bara 10–20 minuter. Att göra samtliga delar av materialet är tänkt att ta ungefär 50–60 minuter.

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
- Pennor och papper eller annat för att göra tipspromenaden

Delar i lektionsförslaget

- **Den digitala vardagen - en nyckelfråga.** Första delen av filmen och diskussion
- **Digital rustning.** Andra delen av filmen och diskussion
- **Verktyg för att försvara sig.** Hur man försvarar sig och sin information mot digitala hot. Inklusive praktiska exempel och miniövningar
- **Har du lärt dig hur du skyddar dig?** Tipsrunda/quiz om det eleverna lärt sig
- **Nu har du en rustning.** Avslutande sammanfattning

Mer material på ämnet

- **Andra filmer med lektionsförslag.** Två andra filmer om digitala fotspår och nätbedrägerier. Inklusive tillhörande lektionsförslag.
- **Digitala lektioner i SkillsBuild.** Fyra digitala lektioner på olika ämnen inom cybersäkerhet som eleverna kan jobba med.
- **Föreläsning med IT-expert.** Kostnadsfri föreläsning som går att boka via cybersecurityacademy.se

Lektionsförslag

Den digitala vardagen - en nyckelfråga

Bild 1–4 i powerpointpresentationen

Inledning: Börja med att visa den första delen av filmen (tid 00:00-00:32).
https://www.youtube.com/playlist?list=PLIk39hnHx0Lt-DBDkAmPB3x6Jl4iJaf22

- Pausa filmen när problembilden byggts upp och presenterats
- **Återkoppla till det som visades:** alla lever en stor del av vardagen online, vi har digitalt liv (sociala medier, gaming, osv). Unga spenderar ungefär 7h 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 även låta dem svara 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 4–5 i powerpointpresentationen

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 som snor din info
    - Någon som 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 1 av 3 ungdomar har fått ett konto hackat
    - Dela gärna med dig om du har en personlig erfarenhet eller om någon elev är bekväm att dela med sig. Verkliga exempel är ofta bättre än påhittade exempel och sänker stigmat av att känna skam kring det
- Det finns skydd!

Verktyg för att försvara sig

Bild 6–18 i powerpointpresentationen

Starka lösenord: Det första verktyget för att försvara sig själv på nätet

- **Retorisk fråga:** Vad är ett lösenord?
    - Lösenord är lås som bara du som äger det har nyckeln till, för att kunna låsa in allt det du gör online.

- Lösenordet finns sparat i krypterat format på servern för tjänsten där man försöker logga in. Att det är krypterat innebär att man gjort det oläsligt så länge man inte har lösenordet

Teknisk fördjupning: Kryptering och hashning

Företag sparar inte våra lösenord som de är i ”plain text”, utan krypterar dem när de sparas i en databas som ”hashes” (görs om genom haschalgoritmer). Exempelvis:

Lösenordet: superSnällaSilverSara
Dess hash:165128C12A859FB481915A5388ADE526

Om hemsidan blir hackad så kan de krypterade lösenorden läcka, och om de är dåliga lösenord så gör det ingen skillnad att man krypterat dem, hackare kan använda datorer för att knäcka krypteringen på lätta lösenord och få tag på kontona. Om dåliga krypteringar används så är det ännu lättare och därför avgörande hur bra lösenordet bakom är. De kan också testa vanliga lösenord och då gör det ingen skillnad hur bra hashalgoritmen är.

- **Vad är ett starkt lösenord?**
  - Långt (minst 14 tecken),
  - unikt (inte återanvänds),
  - lätt att minnas men svårt att gissa. Man ska inte ta lösenord som andra använt, till exempel "qwerty123456" eller som man kan gissa utifrån användaren.
  - En teknik att använda är lösenordsfraser (exempel: "småfågel-tassa-explosion”)

Tvåfaktorsautentisering (2FA/MFA): Ett extra lås på dörren

- Nästa teknik man kan använda är 2FA - ett "extra lås på dörren". Först lösenord, sedan en kod till en annan enhet, ofta mobil.
  - Går ut på att man "lägger alla ägg i en korg". Detta gör det mycket svårare för hackare att komma in, eftersom det inte räcker med att knäcka lösenordet.
- **Koppling till vardagen:** Fråga om någon av eleverna använder 2FA
  - Nämn populära appar där 2FA finns (Instagram, Discord, Gmail, Roblox). Man kan fråga om någon använder någon av dessa appar och poängtera att det bara tar en minut att slå på.
  - Olika 2FA har olika fördelar, ex så behöver du inte homma ihåg ditt fingeravtryck, men om det i framtiden är något som stjäls så kan du inte få ett nytt.
  - 2FA gör en inte omöjlig att hacka. Förutom att både din mobil och ditt lösenord kan bli stulna samtidigt så finns även en scammetod som kallas SIM-swapping. Den går ut på att en hackare utnyttjar att man kan be om ett nytt SIM-kort för att få 2FA att skicka meddelandet till dem.

Bluffar: Det finns många fällor och faror online. Många aktörer har specialiserat sig för att försöka lura oss. Nätbedrägerier är mycket vanligt och bästa sättet att skydda sig är att försöka genomskåda dem.

- **Varningssignaler att ta upp:** ”Är du produkten?”, "Var försiktig med vad du klickar på" och fråga dig själv om det ”Är för bra för att vara sant?" Dessa är några av de viktigaste tumreglerna.

- **Är "Gratistjänster" verkligen gratis?** Vilka appar eller tjänster ni använder betalar ni inget för? Är de alltså gratis? Hur tjänar de egentligen pengar?
    - Prata om att "användaren blir produkten" utan att veta om det helt.
    - Det vi gör online kan samlas in och "kartläggas". Det vi lägger ut, det vi söker på eller det vi kollar på kan sparas och användas för marknadsföring, men även säljas vidare och kan även hamna i oärliga aktörers händer.
    - Fundera en extra gång på vad du lägger ut och klicka inte alltid på acceptera alla cookies så minskar du denna risk.
- Om något verkar ”för bra för att vara sant”, är det oftast just det. Eller om någon vill att du ska ge dem känslig information som inloggningsuppgifter, stanna upp och tänk efter.
    - Blufflänkar (phishing) som ser ut att komma från vänner eller betrodda källor är ett sådant exempel. Även erbjudanden eller tävlingar online som man vill klicka på kan innehålla virus. De kan kapa dina konton

Exempel på bedrägeri: Länk till videon om man vill demonstrera: https://x.com/MrBeast/status/1709046466629554577?ref%5C_src=twsrc%5Etfw

- Filmen visar en deepfake-scam av den kända youtubern MrBeast som ser ut att ge ut priser i princip gratis.
- Andra liknande exempel skulle kunna vara erbjudande om att du har vunnit något värdefullt via en reklambild.
- Det här är ett exempel på när avancerade AI verktyg, som idag är tillgängligt för de flesta, används av kriminella för att begå bedrägeri.
- Man måste där alltid vara uppmärksam och fundera ”känns detta trovärdigt” eller ”är det för bra för att vara sant.

Malware

Malware (malicious software) eller så kallad skadlig kod sprids ofta genom blufflänkar i mejl, sms, annonser, infekterade nedladdnings-länkar 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 misstänkt länk, ha ladda ner skadlig kod som i sin tur stjäl lösenord, bankuppgifter eller annan känslig information. Ett exempel på detta är denna video som visar en deap fake av den populära yotubern Mr. Beast. Den visar hur aktörer med illvilligt uppsåt kan utnyttja vår oaktsamhet och gömma sig bakom avancerade bedrägeri-verktyg som blivit tillgängliga för fler och fler att använda.

Miniövning - genomskåda bluffmeddelandet: Nedan följer ett exempel på ett bluffmeddelande. Prata om de olika varningstecknen, se hur många de kan komma på själva. Exempel på varningstecken är:

- Attraktiv identitet för bedragare att anta - Många av oss vill gärna agera om skolan eller myndigheter kontaktar oss.
- Begäran om känsliga uppgifter
- Underlig länk, skulle det verkligen skickas ut så här?
- Vi kan bli kanske stressade och lägger in kontouppgifter på en länkad sida som vi fått via meddelandet.
- Meddelandet och avsändaren ser inte trovärdig ut. Stavfel och underlig mejladress

Har du lärt dig hur du skyddar dig?

Bild 19 i powerpointpresentationen

Tipspromenad: Dela in klassen i mindre grupper och låt dem göra tipspromenaden. Alternativt kan man köra frågorna som ett vanligt quiz.

Nu har du en rustning

Bild 20–22 i powerpointpresentationen

Avslutning: sammanfatta vad ni pratat om under lektionen.

- **Sammanfattning:** Här kan man repetera budskapet från filmen: Aktivera 2FA, skaffa ett starkt lösenord med en lösenordshanterare och var beredda på att det kan finnas aktörer som vill lura er online.
- Vikten av att prata med vuxna: Påminn om att de alltid ska prata med en vuxen om något känns fel eller om något har hänt online.

Arbetsblad: Tipsrunda

1. Svagheter i lösenord

Du hittar ett papper i datasalen där någon har skrivit sitt lösenord: Sofia2009. Vilken är den största svagheten?

A) Det är för kort

B) Det innehåller personliga uppgifter (namn + födelseår)

C) Det är inte unikt

---

2. Lösenordsfraser

Vilket av dessa är säkrast men ändå lätt att minnas?

A) P4ssW0rd!

B) katt-Pannkaka-1700-flyger

C) GalDa90?-saX3>d

---

3. Tvåfaktorsautentisering (2FA)

En kompis säger: ”Jag har 2FA på Instagram, så jag är helt säker från alla hackers”. Vilket troligt hot skulle du fortfarande varna för?

A) Hackare kan ibland kapa SMS-koder genom SIM-swapping

B) Instagram kan hackas ändå, så det spelar ingen roll

C) 2FA fungerar bara på datorer, inte på mobiler

---

4. Gratis-appar

Du laddar ner en gratis app för att redigera bilder. Den vill ha tillgång till: kameran, mikrofonen, dina kontakter och platsen du befinner dig på.

Vad är troligast?

A) Appen samlar in mer data än vad den behöver

B) Appen behöver all data för att fungera

C) Gratis-appar använder aldrig din data när den är avstängd

---

5. Phishing-mail

Du får ett mail från ”Google Support”: ”Ditt konto stängs om du inte verifierar dig här: http://googl-support-login.com” Vilket är det tydligaste tecknet på att det är bluff?

A) Länken ser konstig ut

B) Google skickar aldrig mail

C) Texten innehåller ordet ”verifiera”

---

6. Deepfake-fällan

Du ser en video där en känd influencer säger: ”Swisha 100 kr och få en exklusiv hoodie skickad hem direkt”. Vad är klokast att tänka?

A) Kolla på influencerns officiella konton för att se om erbjudandet finns där

B) Klicka på länken snabbt, innan hoodiesarna tar slut

C) Fråga vänner i chatten om de också har sett videon

---

7. Datainsamling

Vilken av dessa är inte ett exempel på att du blir ”produkten” online?

A) Facebook använder dina intressen för att visa riktad reklam

B) Roblox sparar vilka spel du spelar mest

C) Du köper ett datorspel i butik med kontanter

---

8. Säkerhetsmedvetenhet

En vän berättar stolt: ”Jag har samma lösenord till alla konton, men det är 18 tecken långt och väldigt svårt att gissa!”. Vad är problemet?

A) Lösenordet är inte svårt att gissa om du vet hans namn

B) Att använda samma lösenord överallt gör att om ett konto hackas, så riskeras alla andra

C) 18 tecken är för långt – svårt att skriva in

---

9. Digital stress

Varför skickar bedragare ofta bluffmeddelanden med ord som ”Ditt konto stängs om 2 timmar!”?

A) För att du ska bli stressad och fatta snabba beslut

B) För att det är roligare för dem

C) För att de annars glömmer bort bluffen

---

10. Online Community

Din kompis får sitt konto kapat på Discord, och bedragaren skickar länkar till alla i gruppen. Vad är bäst att göra?

A) Klicka för att se om länken verkligen är farlig

B) Ignorera, det är ju inte ditt problem

C) Varna andra i gruppen och tipsa kompisen att kontakta support och byta lösenord

---

Facit

1. B
2. B
3. A
4. A
5. A
6. A
7. C
8. B
9. A
10. C

Mer material på ämnet

Utöver det här materialet finns två andra motsvarande lektionsförslag på närstående ämnen inom cybersäkerhet. Inom Cybersecurity Academy erbjuder vi även skolor att ta del av kostnadsfria föreläsningar med en IT-expert och ett större undervisningsmaterial för att fördjupa elevernas kunskaper. Inklusive ett digitalt lektionsmaterial på den digitala utbildningsplattformen SkillsBuild. Allt undervisningsmaterial och föreläsningarna är ämnesövergripande och kompletterar varandra, men kan även användas fristående.

Andra filmer med lektionsförslag

Utöver det här materialet finns två andra med filmer och lektionsförslag. De heter *Ditt digitala fotavtryck* och *Digital rustning*. Den första handlar om vilka spår man lämnar efter sig online och den andra om verktyg för att rusta sig mot digitala hot. Samtliga filmer finns på svenska och lätt svenska med undertexter på engelska, arabiska, somaliska och tigrinska.

De andra filmerna och lektionsförslagen finns på:

https://skolmaterial.ungaforskare.se/

Digitala lektioner i SkillsBuild

Låt eleverna jobba direkt i den digitala utbildningsplattformen SkillsBuild. Där finns totalt fyra digitala lektioner om 1. grundläggande cybersäkerhet, 2. digitala fotspår, 3. skydda dina uppgifter och 4. hackare och etik ger eleverna både baskunskap om cybersäkerhet samt en djupare förståelse för risker och skydd på nätet. Lektionerna innehåller texter, filmer, övningar, diskussionsfrågor och andra aktiviteter

För att komma åt materialet behöver du skapa ett konto. Det är kostnadsfritt och tar bara några sekunder. På vår hemsida hittar du en länk som tar dig direkt till det svenska materialet annars är det bara att söka på Cybersecurity Academy i SkillsBuild.

Mer info om de digitala lektionerna:

https://cybersecurityacademy.se/skola/digitala-lektioner/

Länk för att skapa konto i SkillsBuild för studenter:

https://ibm.biz/ungaforskare_s

Boka föreläsning med IT-expert

Cybersecurity Academy erbjuder skolor från mellanstadiet upp till gymnasiet gratis föreläsningar om IT-säkerhet. Våra föreläsare är IT-experter som arbetar med IT säkerhetsfrågor eller studerar det på universitet. Vi erbjuder både föreläsningar på plats i skolan där det är möjligt och alltid digitalt.

Mer info om föreläsningarna:

https://cybersecurityacademy.se/skola/forelasning/

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 MSB (Myndigheten för samhällsskydd och beredskap).

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 9000 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 samhällsskydd och beredskap, MSB, 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 är en kampanj som drivs av MSB och Polisen i samarbete med en stor mängd aktörer från offentlig sektor, näringslivet och föreningslivet. Årets tema är Säkrare på nätet och kampanjen vill med enkla och handfasta råd öka på allmänhetens och småföretagares medvetenhet och kunskap så att de blir tryggare att använda det digitala samhällets tjänster.