Cybersecurity Academy

Klicka smart

Lärarhandledning åk 4–6

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 ge elever verktyg för att upptäcka och motverka bedrägerier som de möter online. Genom att veta om de vanligaste riskerna och tänka till en gång extra innan de klickar så blir eleverna mer säkra.

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 *Digital rustning*.

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 övning
- Powerpointpresentation med anteckningar

www.ungaforskare.se

Materialet finns tillgängligt digitalt på cybersecurityacademy.se

Författare:
Max Vinger
Martina Sandgren

Tryckår:
2025, version 1.0

Innehåll

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:

- Några exempel på nätbedrägerier och hur de går till
- Hur nätbedrägerier påverkar individen och samhället i stort
- Bättre skydda sig själva online genom att ha kritiska ögon och bra lösenordshygien

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
- Whiteboard
- Pennor
- Arbetsblad

Delar i lektionsförslaget

- **Vår digitala värld och dolda faror.** Introduktion till nätbedrägerier
- **Klicka smart.** Filmen om det centrala innehållet i lektionen
- **Bluffdetektiv.** Fördjupande övning där eleverna får identifiera varningssignaler i olika bluffar
- **Lösenord.** Fördjupande övning och diskussion om säkra lösenord
- **Skydda dig mot nätbedrägerier.** Sammanfattning av tips och avslut

Mer material på ämnet

- **Andra filmer med lektionsförslag.** Två andra filmer om digitala fotspår och verktyg för att skydda sig mot digitala hot. 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

Vår digitala värld och dolda faror

Bild 1–4 i powerpointpresentationen

Inledning: Starta diskussionen, presentera utmaningen

- 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 formen av massutskick av sms, mejl, annonser eller bluffhemsidor. Detta är 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.

Klicka smart

Bild 5 i powerpointpresentationen

Visa videon klicka smart:
https://www.youtube.com/playlist?list=PLIk39hnHx0LsV2uVCgmBYzEx-3TMf__gP

- **Återkoppling:** Efter filmen kan man känna in eleverna och om de känner oro, har någon berättelse att berätta eller spontana känslor eller tankar som väckts. Det kan förhoppningsvis skapa och hålla engagemang för ämnet samtidigt som det validerar eller kan hjälpa dem att bearbeta ämnet.

Den mänskliga faktorn

Phishing, social engineering och malware är tre olika tekniker som hackare använder som utnyttjar att vi människor ofta är lättare att lura än datorer. Ofta är det lättare att utnyttja den mänskliga faktorn och personen bakom skärmen i stället för att hitta svagheter i program eller i datorer. Stora attacker utnyttjar ofta flera olika tekniker.

Bluffdetektiv

Bild 6–14 i powerpointpresentationen

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 formen av helt vanliga meddelanden på sms, DM’s eller bluffhemsidor
  - De har ofta en stressande ton, med tidsbrister eller nedräkningar. 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, anonymiserade exempel på vanliga nätbedrägerier som barn och unga kan stöta på. Gå igenom och visa upp de tre exemplen. Om du vill kan du även ge lite tips vad de kan kolla på, se nedan. Exemplen finns i powerpointpresentationen och som arbetsblad i den här lärarhandledningen.

- **Phishing-SMS/epost:** Ett meddelande som ser ut att komma från banken, posten, skolan eller en vän kan egentligen 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 skriva lite fel i adressen till den som man vill in på. 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.
- **Videobluff:** När AI blir allt vanligare och allt bättre ökar även bluffar där kända personer ser ut att vara avsändare genom så kallade ”Deepfakes”
    - Är det för bra för att vara sant?
    - Är videon eller rösten lite konstig? Det kan vara tecken på att AI har använts
    - Sök fram personens officiella konto och kolla ifall inlägget finns även där. Gör det inte det kan det vara ett tecken på att det inte är från dem egentligen

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".
    - Stavfel eller konstiga formuleringar.
    - Erbjudanden som "verkar för bra för att var 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 bedrägerisätten online och har effektiviserats av AI. Det används för att automatisera processen i övertygande meddelanden och göra så att bedragare kan attackera snabbare och på en större skala.

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 fake-röst som kan användas för phishing via exempelvis telefon

Därför måste vi vara försiktig med även vad vi själva lägger upp online. Videor som du blir skickad eller lägger ut. Viktigt kan vara att prata om det hemma dina närmaste om hur ni ska agera om ni tror att ni är under ett bedrägeriförsök via video eller ljud.

AI-bildmodeller används även idag mot bland annat specifikt unga i "sextortion scams". Dvs i utpressningssyfte för att få pengar, eller att tvinga personen att skicka sexuella bilder. Det är viktigt att markera att detta är ett alvarligt brott och om man utpressas på detta sätt är man ett brottsoffer som har rätt till stöd. Det ska anmälas till polis

Lösenord

Bild 15–22 i powerpointpresentationen

Lösenordet - ditt viktigaste verktyg: Lösenord är nyckeln till allt i ens digitala liv. Det är dels ett lås som låser in det vi har online, men används även som ett bevis på vem vi är. Bara du har ju ditt lösenord, så om du kan lösa upp något på en webbplats så kan du bevisa att du är du på den webbplatsen. Därför måste vi kunna göra bra lösenord och att vi ska göra några övningar för att lära oss detta.

Kombinationslås - Mini-matteövning: Övningen är uppdelad i fyra delar som kopplar an till bra minnesregler när man skapar lösenord och motiverar varför de är bra.

- **Längre:** Vi har ett klassiskt kombinationslås som man kan använda för sitt skåp i skolan eller badhuset (9x9x9). Man kan snurra och testa alla kombinationer relativt lätt.
    - Visa gärna hur det blir fler och fler kombinationer möjliga om man lägger till en siffra (9x9x9x9).
    - Det är första pusselbiten för ett säkert lösenord, ju längre, desto bättre.
- **Flera symboler:** Visa nu samma kodlås men visa att det kan vara siffror och bokstäver som används.
    - Fråga gärna vad det gör med säkerheten.
    - Visa att vi nu har alla siffror (ha en rad med siffror) och alla bokstäver (visa alfabetet) och att nu har vi (9+29)^3 kombinationer istället. Mycket säkrare!
    - Därför är det viktigt att använda siffror, bokstäver och dessutom små och stora tecken 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 12-tecken i sina lösenord. Men använd en gärna en lösenordsfras så att du kan komma ihåg det.

- **Unika:** En tredje sak är att de ska även vara unika.
  - På våra viktigaste konton, som mejlen, så bör vi ha ett lösenord som vi inte har någon annanstans. Det ger oss säkerheten att en läcka på en annan hemsida gör mejlen sårbar.
  - Allra helst ska man såklart använda unika lösenord överallt, men bara att använda två olika är mycket bättre än att ha samma överallt!
- **Svåra att gissa:** Den fjärde grejen är att de ska vara svåra att gissa.
  - Diskutera att ett lösenord inte får ha saker i sig som kan kopplas till dem. Fråga vad något man skulle kunna ta reda på om en person online skulle kunna vara. Typ vilket år man är född, eller om man har ett djur.
  - Beskriv att detta är saker som potentiella hackare kommer pröva först innan de prövar alla tänkbara kombinationer.
- **Lätta att komma ihåg:** Den sista, och kanske allra viktigaste delen är att lösenord måste gå att komma ihåg
  - Lösenord som man inte kommer ihåg är värdelösa. Så det gäller att hitta avvägningen mellan de andra punkterna och något man faktiskt kan komma ihåg.
  - Ett sätt att göra långa lösenord som är relativt lätta att komma ihåg är lösenordsfraser (t.ex. "grönacyklar-lamslå-*slut”). Skriv gärna upp några exempel på tavlan.
  - Ett annat sätt att ha unika lösenord som man inte glömmer bort är med lösenordshanterare.

Extra utmaning: Låt eleverna tänk på en egen lösenordsfras som är lång och unik men lätt att komma ihåg för dem själva.

Skydda dig mot nätbedrägerier

Bild 23–25 i powerpointpresentationen

Avslutning: sammanfatta lite tips på hur eleverna kan vara säkrare online.

- **Tänk efter före:** "klicka inte bara för att något ser spännande ut". "Om ett erbjudande verkar för bra för att vara sant, så är det ofta det".
- **Dubbelkolla alltid avsändaren:** fråga t.ex. kompisen direkt om det är de som skickat något om meddelandet känns konstigt. Gå in separat i officiella appar och hemsidor och kolla om samma info finns där
- **Använd tvåstegsverifiering (2FA) där det finns:** Förklara enkelt att det är ett extra skydd där man behöver en kod till mobilen utöver lösenordet för att logga in. Detta gör det "mycket svårare för någon att ta sig in på ditt konto".
- **Dela aldrig lösenord eller personliga uppgifter:** förälder kan vara undantag.
- **Prata med en vuxen:** "om du är osäker eller för att vara steget före tillsammans".

Arbetsblad: Bluffdetektiv

Till höger är ett exempel på ett phishing-sms

1. Vad är det som känns konstigt eller misstänkt med det här meddelandet? Vilka varningssignaler hittar ni?

_____

_____

_____

_____

_____

_____

_____

_____

2. Vad tror ni kan hända om man klickar på länken eller lämnar ut uppgifter här?

_____

_____

_____

_____

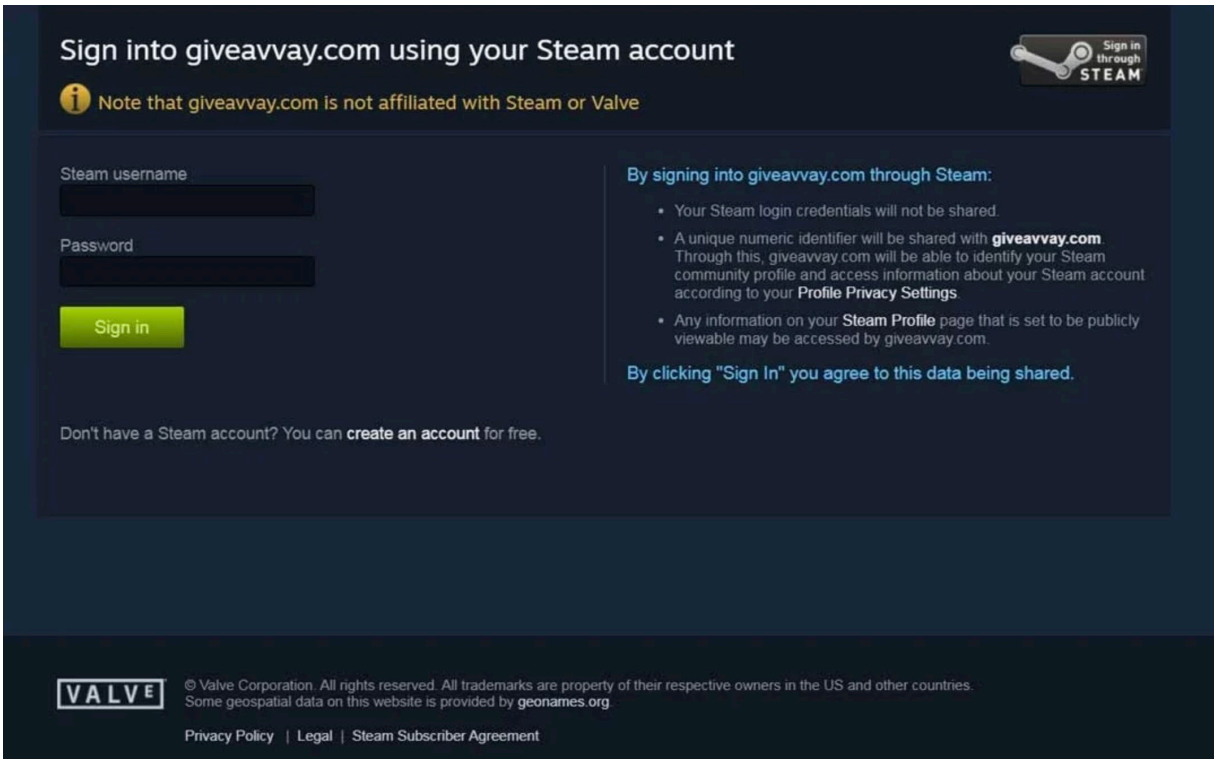
_____

_____

_____

_____

Det här är ett exempel på en bluffhemsida



3. Vad är det som känns konstigt eller misstänkt med det här meddelandet? Vilka varningssignaler hittar ni?

_____

_____

_____

_____

_____

_____

4. Vad tror ni kan hända om man klickar på länken eller lämnar ut uppgifter här?

_____

_____

_____

_____

_____

Till höger är ett exempel på ett videobedrägeri

Ni kan se videon genom att följa länken eller QR-koden nedan, eller bara svara utifrån bilden.

5. Vad är det som känns konstigt eller misstänkt med det här meddelandet? Vilka varningssignaler hittar ni?

_____

_____

_____

_____

_____

_____

_____

_____

6. Vad tror ni kan hända om man klickar på länken eller lämnar ut uppgifter här?

_____

_____

_____

_____

_____

Videon går att se på: https://x.com/MrBeast/status/1709046466629554577

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/

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.