STUDIEMATERIALEFTERLEKTION5AV6

Digital säkerhet och bedrägerier

FRAMTAGENFÖR

Digitala seniorer, Studieförbundet Vuxenskolan i samarbete med SPF Seniorerna

LEKTIONENHÖLLS

Måndag 16 november 2026

NÄSTALEKTION

Måndag 23 november 2026, kl. 13.30: **AI för föreningsarbete**

Tack för en engagerad lektion! Chatten gick varm med frågor från hela landet, och många grupper bestämde sig för att införa ett kodord i familjen. Den här lathunden är den största hittills. Den går igenom allt från lektionen, och dessutom tvåstegsverifiering, BankID, lösenord, ansiktsigenkänning och hur du gör dina konton i sociala medier privata. Svaren på alla frågor från chatten finns inbakade i texten.

Läs den gärna i omgångar. Börja med avsnitt 2 om social manipulering och avsnitt 5 om skyddsreglerna. De är viktigast.

Det här materialet är skapat av Gabriel Eliasson för Digitala seniorer. Det är fritt att skriva ut, spara och dela vidare till andra i din förening och familj.

Uppgifterna gäller i november 2026. Appar och tjänster ändras ofta, så knappar och menynamn kan se lite annorlunda ut hos dig.

Innehåll

1. Därför är det här viktigt
2. Social manipulering, grunden för alla bedrägerier
3. Nya bedrägerier med AI
4. Du kan inte se skillnad, använd sunt förnuft
5. Fem skyddsregler och fler enkla knep
6. BankID, SverigeID och e-legitimation
7. Tvåstegsverifiering och passkeys
8. Ansiktsigenkänning och fingeravtryck
9. Lösenord som håller
10. Gör dina konton i sociala medier privata
11. Länkar, appar och smarta prylar
12. Om du ändå blir lurad
13. Frågor om AI från chatten
14. Det här tar grupperna med sig
15. Gör det här i veckan
16. Länkar från lektionen
17. Ordlista

1. Därför är det här viktigt

Bedrägerier är i dag ett av de vanligaste brotten i Sverige, och bedragarna riktar sig ofta mot äldre. Enligt Polisen gav bedrägerierna kriminella nätverk miljarder kronor bara under 2025. Brå har visat att bedrägerier mot äldre kvinnor har mer än fördubblats på sex år.

Bedragarna är organiserade, skickliga och arbetar som ett yrke. De sitter i callcenter, följer manus och övar på att låta trovärdiga. Nu har de dessutom fått hjälp av AI, som kan härma röster, skapa falska filmer och skriva felfri svenska.

> **Viktigt:** Vem som helst kan bli lurad. Det handlar inte om att vara dum eller godtrogen. Den som blir lurad har inget att skämmas över, det är bedragaren som har gjort fel.

Vi började med ett aktuellt inslag

Lektionen inleddes med ett inslag från TV4 där bankerna varnar för tre bedrägerier inför julhandeln:

> **Falska webbutiker och sms om paketavgifter.** Butiker som ser äkta ut men aldrig skickar något, och sms som påstår att ditt paket väntar på en avgift.
> **Investeringar i påhittade AI-bolag.** Löften om snabba vinster på AI, ofta i annonser med kända ansikten.
> **Uppmaningar att öppna konto i en annan bank.** Bedragaren säger att dina pengar måste flyttas till ett ”säkert konto”.

Alla tre bygger på samma sak: social manipulering. Därför är det där vi börjar.

2. Social manipulering, grunden för alla bedrägerier

Social manipulering betyder att bedragaren lurar **människan**, inte datorn. Med ord och känslor får bedragaren dig att **själv** föra över pengar, logga in med BankID eller lämna ut uppgifter. Ingen behöver hacka något.

Tekniken byts ut hela tiden: telefon, sms, mejl, AI-röster, deepfakes och hembesök. Men knepen är desamma som de alltid har varit. **Förstår du knepen kan du nästan alltid avslöja bedragaren**, oavsett vilken teknik som används.

Sex knep som bedragarna använder

Knep	Så kan det låta	Därför fungerar det
Brådska	”Du måste göra det nu, annars är pengarna borta!”	Stress gör att vi slutar tänka efter.
Rädsla	”Ditt konto är hackat.” ”Någon har tagit lån i ditt namn.”	Oro får oss att lyda utan att ifrågasätta.
Auktoritet	”Hej, det är polisen. Vi behöver din hjälp.”	Vi är vana att lita på polis, bank och myndigheter.
Medkänsla	”Mamma, jag har hamnat i trubbel.”	Vi vill hjälpa dem vi älskar.
Lockelse	”Garanterad vinst, men bara i dag.” ”Du har vunnit!”	Drömmen om snabba pengar.
Förtroende	”Jag har aldrig träffat någon som dig.”	Smicker och kärlek sänker garden.

Ofta används flera knep samtidigt. Den falska polisen använder auktoritet, rädsla och brådska i samma samtal. Den falska dottern använder medkänsla och brådska. Romansbedragaren bygger förtroende i veckor innan lockelsen kommer.

Så går en manipulation till

Steg	Vad som händer
1. Kontakt	Ett samtal, ett sms, ett mejl, en annons eller en knackning på dörren.
2. Förtroende	Bedragaren låter trovärdig och vet ofta saker om dig, som namn, adress och vilken bank du har.
3. Känsla	Rädsla, oro eller hopp väcks.
4. Brådska och hemlighet	”Gör det nu, och berätta inte för någon, inte ens banken.”
5. Handling	Du betalar, loggar in med BankID eller lämnar ut kort och koder.

Varning: Känner du en stark känsla och stress på samma gång? Då ska du stanna upp. Lägg på och ring någon du litar på. Ingen seriös bank, myndighet eller anhörig ber dig att hålla något hemligt.

Tips: Deltagarna i Köping gav ett bra råd i chatten: **ställ flera kritiska frågor**. Fråga vad personen heter, vilken avdelning hen ringer från och vad ditt ärende gäller. En bedragare blir ofta stressad, irriterad eller lägger på.

3. Nya bedrägerier med AI

AI har inte skapat några nya knep. Den har gjort de gamla knepen mycket mer övertygande. Här är de vanligaste metoderna just nu.

Röstkloning

Med röstkloning kan en bedragare härma en verklig persons röst. Rösten kan sedan säga vad som helst, i realtid eller som inspelning.

Hur mycket ljud behövs för att kopiera en röst?

Det räcker med några sekunder, och ju längre inspelning, desto bättre blir kopian. Ljudet kan komma från en video i sociala medier, en hälsning på röstbrevlådan eller ett kort telefonsamtal där bedragaren får dig att prata.

Så kan det gå till: Du blir uppringd och hör ditt barnbarns röst. Hen gråter, har varit med om en olycka och behöver pengar direkt. Ann-Lis, 76, i Malmö fick precis ett sådant samtal, där rösten lät som hennes dotter.

GÖRSÅHÄR

Så skyddar du dig mot röstkloning

1. Bestäm ett **kodord** i familjen. Mer om det i avsnitt 5.
2. Lägg på och ring tillbaka på det nummer du redan har sparat.
3. Använd **standardhälsningen** på din röstbrevlåda i stället för en egen inspelning, så finns din röst inte där att kopiera.
4. Var försiktig med att prata länge med okända som ringer. Svara gärna kort tills du vet vem det är.

Deepfakes och falska annonser

En deepfake är en falsk video eller bild där en verklig person ser ut att säga eller göra något hen aldrig har gjort. Bedragare använder kända ansikten för att väcka förtroende.

Kända ansikten: Anders Tegnell, programledare och läkare ”tipsar” om investeringar eller mirakelkurer.
Falska myndigheter: videor där ”polisen” eller ”banken” varnar dig och ber dig agera snabbt.
Falska nyhetssidor: annonsen leder till en sida som ser ut som SVT, TV4 eller Aftonbladet.

Tips: Kändisar tipsar inte om investeringar i annonser på Facebook och Instagram. Klicka inte. Tryck på de tre prickarna vid annonsen och välj **Anmäl annons**.

AI-skrivna sms och mejl

Förr kunde man ofta känna igen en bluff på dålig svenska. Nu skriver AI felfritt och personligt. Felfri svenska betyder inte längre att något är äkta.

Kan man se på en mejladress att den inte kommer från banken eller Skatteverket?

Ibland. Titta på hela adressen, inte bara namnet som visas. Det som står efter @ ska vara företagets riktiga adress, till exempel @skatteverket.se. Bedragare använder ofta adresser som liknar den riktiga, som @skatteverket-info.com.

Kan en bedragare skicka mejl från en riktig adress?

Det går att förfalska avsändaren så att den ser riktig ut, men banker och myndigheter har skydd som gör att sådana mejl oftast stoppas. Lita ändå aldrig på avsändaren ensam. Det säkraste är att aldrig klicka på länkar i mejl och sms, utan själv gå till bankens app eller webbplats.

Sms om tull och paket inför julen

När vi handlar mycket på nätet kommer också många falska sms om tullavgifter och paket som väntar. Så avslöjar du dem:

> Fundera på om du verkligen väntar ett paket, och från vem.
> Klicka aldrig på länken i sms:et. Öppna i stället PostNords, DHL:s eller butikens egen app och skriv in spårningsnumret själv.
> Tull betalas bara på varor från länder utanför EU, och beloppet är aldrig några få kronor för att ”frigöra” ett paket.
> Vidarebefordra bluff-sms till numret **7726**. Det är gratis och hjälper operatörerna att stoppa liknande sms. Grattis Strömsund, som lärde sig det under lektionen!

Romansbedrägerier

AI hjälper bedragaren att föra långa, varma och kärleksfulla samtal med många personer samtidigt, ofta med falska bilder. Efter veckor eller månader kommer frågan om pengar: en biljett, en sjukdom, en tullavgift. Den som aldrig har träffats på riktigt och ber om pengar är nästan alltid en bedragare.

Bedragare som kommer hem till dig

En växande trend är att bedragarna inte nöjer sig med telefonen. De ringer först som ”polis” eller ”bank” och säger att dina pengar, kort eller smycken är i fara. Sedan kommer ett ”bud” eller en ”polis” hem och hämtar dina värdesaker för att ”säkra” dem.

> **Varning:** Polisen och banken hämtar aldrig kort, kontanter eller smycken hemma hos dig. Släpp inte in någon du inte väntat dig, även om personen visar en legitimation. Ring 112 om någon står utanför dörren och du känner dig hotad.

4. Du kan inte se skillnad, använd sunt förnuft

Det här var lektionens viktigaste budskap. **Försök inte avgöra om en bild, film eller röst är gjord med AI.** Redan i dag är det mycket svårt, och snart går det inte alls. I ett av inslagen vi tittade på blev till och med en bildexpert lurad av AI-bilder.

Använd i stället sunt förnuft och var sunt misstänksam. Ställ tre frågor:

Fråga	Tänk så här
1. Är det rimligt?	Skulle min bank, mitt barnbarn eller polisen verkligen göra så här?
2. Vill någon att jag gör något snabbt?	Brådska är bedragarens viktigaste verktyg.
3. Kan jag kontrollera det på annat sätt?	Ring själv upp, på ett nummer du redan har.

Det är alltid rätt att stanna upp. Ingen seriös person blir arg för att du dubbelkollar.

Låt AI hjälpa dig att granska

Kan jag låta AI avgöra om ett sms, ett mejl eller ett samtal kommer från en bedragare?

Sms och mejl, ja. Kopiera texten, klistra in den i ChatGPT, Gemini eller Claude och skriv: *Kan det här vara ett bedrägeri? Vilka varningstecken ser du?* AI:n är ofta bra på att peka ut varningstecknen. Ta bort ditt namn och personliga uppgifter innan du klistrar in. Samtal är svårare att granska, eftersom de sker i realtid. Där gäller kodord och att lägga på och ringa upp.

> **Bra att veta:** AI kan också ha fel. Se svaret som en andra åsikt, inte som en garanti. Är du osäker, ring din bank eller en anhörig.

5. Fem skyddsregler och fler enkla knep

Regel	Så gör du
1. Bestäm ett kodord	Ett hemligt ord som familjen alltid säger i en nödsituation.
2. Lägg på och ring upp	Ring själv, på ett nummer du redan har.
3. Brådska är en varningssignal	Ingen seriös bank eller myndighet kräver svar inom minuter.
4. BankID och koder är dina	Logga aldrig in eller signera för att någon annan ber dig.
5. Tala om det	Berätta för någon du litar på innan du betalar.

STEGFÖRSTEG

Så inför ni ett kodord i familjen

1. Samla familjen, gärna vid ett middagsbord eller i ett videosamtal.
2. Välj ett ord som är lätt att komma ihåg men som ingen utomstående kan gissa. Undvik husdjurets namn eller annat som syns i sociala medier.
3. Bestäm regeln: **ber någon om pengar eller hjälp i panik, fråga efter kodordet.** Kan personen inte säga det, lägg på.
4. Skriv inte kodordet i sms eller mejl. Berätta det muntligt.
5. Påminn varandra om ordet någon gång om året. Deltagarna i Strömsund vittnade om att det är lätt att glömma!

Fler enkla knep

Våga vara otrevlig. Det är helt okej att lägga på mitt i ett samtal. Polisens kampanj heter just så.
Ring inte numret i ett sms. Leta själv upp numret på bankens webbplats eller på ditt bankkort.
Använd standardhälsningen på röstbrevlådan, så finns din röst inte inspelad där.
Skicka ett sms innan du ringer till någon som inte har ditt nummer. Många svarar inte på okända nummer i dag, av rädsla för bedrägerier. Tack Vendelsö-Brandbergen för tipset!
Svara på ett annat språk. Deltagarna i Arvidsjaur föreslog med glimten i ögat att svara på finska. Det förvirrar åtminstone bedragarens manus.

Är det säkrare om jag själv ringer upp?

Ja, om du ringer ett nummer du själv har letat upp, till exempel på baksidan av ditt bankkort, i bankens app eller på bankens officiella webbplats. Ringer du ett nummer som någon har gett dig i ett samtal eller sms kan det gå direkt till bedragaren. Flera banker låter dig dessutom ringa kundtjänst direkt från appen, så att banken vet att det är du.

114 14 har alltid lång kö. Vad gör jag om jag behöver hjälp snabbt?

114 14 är till för att anmäla brott och ställa frågor som inte är akuta, och där är det tyvärr ofta kö. Pågår ett brott just nu, eller står någon utanför din dörr, ring **112**. Har du förlorat pengar är det viktigaste att ringa **banken först**, eftersom bankens spärrtjänst är öppen dygnet runt. Polisanmälan kan du även göra på polisen.se.

6. BankID, SverigeID och e-legitimation

BankID är nyckeln till din ekonomi och till de flesta myndigheter. Därför är det också det bedragarna helst vill komma åt. Här är svaren på de många frågor om BankID som kom i chatten.

Så fungerar BankID

När du skaffade BankID kontrollerade banken din identitet. Sedan skapades ett unikt, krypterat certifikat som bara finns i din telefon och som skyddas av din säkerhetskod, ditt ansikte eller ditt fingeravtryck. När du legitimerar dig skickar BankID en bekräftelse till företaget om att det verkligen är du. Din kod lämnar aldrig telefonen.

Vad ser mottagaren när jag legitimerar mig?

När du **legitimerar** dig får företaget eller myndigheten ditt namn och ditt personnummer, samt tekniska uppgifter som vilken internetuppkoppling du använde. När du **skriver under** får de dessutom veta vad du har skrivit under. De ser dig inte i bild och kommer inte åt något annat i din telefon.

Kan vilket företag som helst be mig om BankID?

Nej. Företaget måste ha ett avtal med en bank för att få använda BankID. Även små företag kan ha det, men inte privatpersoner. Tänk ändå på att även en bedragare kan ha startat en BankID-förfrågan, till exempel för att logga in på *din* bank från sin dator.

En bedragare ber mig legitimera mig med BankID. Vad får hen veta?

I bästa fall bara ditt namn och personnummer. Men det verkliga syftet är oftast ett annat: bedragaren har själv startat en inloggning på din bank, och när du godkänner kommer hen in på ditt konto. Läs därför alltid vad som står i BankID-appen innan du godkänner. Har du inte själv startat inloggningen, avbryt.

> **Varning:** Godkänn aldrig BankID för att någon ringer och ber dig. Skanna aldrig en QR-kod för BankID som någon har skickat till dig, och läs alltid texten i appen innan du godkänner.

Finns det risker med att legitimera sig med BankID i telefonsamtal till olika företag?

Om **du själv ringer** till ett nummer du vet är rätt, och företaget ber dig legitimera dig, är det tryggt. Det är ett sätt för dem att veta att det verkligen är du. Risken finns när **någon ringer dig** och ber dig använda BankID. Då ska du lägga på.

Kan man stjäla ett BankID?

BankID går inte att kopiera från din telefon. Men bedragare kan lura dig att själv ge dem tillgång, antingen genom att du godkänner deras inloggning eller genom att de får dig att beställa ett nytt BankID till deras telefon. Det är därför reglerna ovan är så viktiga.

Kan någon som går förbi mitt hus komma åt det jag gör med BankID?

Nej. Kommunikationen är krypterad, och ingen utanför kan se eller ta över din BankID-inloggning.

SverigeID, den nya statliga e-legitimationen

Den 1 december 2026 lanserar Polisen **SverigeID**, en statlig e-legitimation som är kopplad till det nationella id-kortet. Du ansöker när du skaffar ett nytt id-kort på polisstationen och använder den sedan via en app. SverigeID har den högsta säkerhetsnivån och ska kunna användas inom hela EU.

> Från start fungerar SverigeID för att logga in på Polisens Mina sidor. Fler myndigheter läggs till stegvis.
> SverigeID ersätter inte BankID, utan är ett komplement. Bankerna och Swish använder i dag bara BankID.
> Id-kort som utfärdats före den 1 december 2026 kan inte användas för SverigeID.

Är det säkrare att använda en annan e-legitimation än BankID?

Båda är säkra. SverigeID har en högre teknisk säkerhetsklass, men det som skyddar dig mest är ändå hur du använder legitimationen: godkänn aldrig något du inte själv har startat.

7. Tvåstegsverifiering och passkeys

Det bästa du kan göra för att skydda dina konton på nätet är att slå på tvåstegsverifiering. Ännu bättre är att börja använda passkeys där det går.

Vad är tvåstegsverifiering?

Tvåstegsverifiering, som ibland kallas tvåfaktorsautentisering, betyder att du behöver två saker för att logga in: något du **vet**, ditt lösenord, och något du **har**, oftast din telefon. Även om en bedragare skulle få tag på ditt lösenord kommer hen inte in utan din telefon.

Det andra steget kan vara en kod i ett sms, en kod i en app eller att du godkänner inloggningen i en app på telefonen.

Varning: Koden från tvåstegsverifieringen är lika hemlig som en PIN-kod. Bedragare ringer ibland och ber dig läsa upp ”koden du just fick”. Gör aldrig det.

STEGFÖRSTEG

Slå på tvåstegsverifiering i ditt Google-konto

1. Gå till **myaccount.google.com** och logga in.
2. Välj **Säkerhet**.
3. Tryck på **Tvåstegsverifiering** och följ instruktionerna.

STEGFÖRSTEG

Slå på tvåstegsverifiering på Facebook och Instagram

1. Gå till **Inställningar** och välj **Kontocenter**.
2. Välj **Lösenord och säkerhet** och sedan **Tvåfaktorsautentisering**.
3. Välj ditt konto och följ instruktionerna. Välj gärna **Autentiseringsapp** eller sms.

Bra att veta: Har du en iPhone har ditt Apple-konto redan tvåstegsverifiering påslagen. Det är därför du ibland får en kod på telefonen när du loggar in på en ny enhet.

Vad är en passkey?

En passkey, som på svenska ibland kallas **nyckel** eller **inloggningsnyckel**, ersätter lösenordet helt. I stället för att skriva ett lösenord låser du upp med ansiktet, fingret eller telefonens PIN-kod, precis som när du låser upp telefonen.

> **Inget att glömma:** du behöver inte komma ihåg något lösenord.
> **Inget att stjäla:** passkeyn finns bara i dina enheter och fungerar bara på rätt webbplats. Den kan inte lockas fram av en falsk inloggningssida.
> **Finns redan hos många:** Google, Apple, Microsoft, Facebook och flera andra stöder passkeys.

STEGFÖRSTEG

Skapa en passkey för ditt Google-konto

1. Gå till **myaccount.google.com** och välj **Säkerhet**.
2. Välj **Nycklar** (kan heta *Lösennycklar och säkerhetsnycklar*).
3. Tryck på **Skapa en nyckel** och bekräfta med ansikte, finger eller PIN-kod.

8. Ansiktsigenkänning och fingeravtryck

De flesta telefoner kan låsas upp med ansiktet eller fingret. Det kallas biometri. Det är både bekvämt och säkert, så länge du vet hur det fungerar.

Metod	Hur det fungerar	Hur säkert
Face ID (iPhone)	Telefonen gör en 3D-karta av ansiktet med osynligt ljus.	Mycket säkert. Risken att en främling låser upp är ungefär en på en miljon.
Fingeravtryck	Telefonen läser av fingrets unika mönster.	Mycket säkert. Risken är ungefär en på femtio tusen.
Ansiktsupplåsning på vissa Android	Använder den vanliga kameran, alltså en platt 2D-bild.	Mindre säkert. Kan på vissa modeller luras av ett foto.
PIN-kod	Sex siffror eller fler.	Säkert, om koden inte är 123456 eller ditt födelseår.

Kan man låsa upp telefonen med ett foto av mig?

Inte en iPhone med Face ID, eftersom den mäter ansiktets form i 3D. På vissa Android-telefoner som bara använder framkameran kan det gå. De telefonerna varnar ofta själva för att ansiktsupplåsningen är mindre säker. Använd då hellre fingeravtryck eller PIN-kod. Bankappar och BankID godkänner oftast inte den enklare ansiktsupplåsningen.

Hur säkert är det att använda ansikte eller fingeravtryck?

Mycket säkert. Bilden av ditt ansikte eller fingeravtryck sparas krypterad i telefonen och skickas aldrig till Apple, Google eller banken. Det är dessutom säkrare än att skriva in en kod som någon kan titta över axeln på.

> **Tips:** Tänk på var du skriver din PIN-kod. Skärma av med handen i butiken och vid bankomaten. Ett sekretessfilter till mobilskärmen, som gör att den bara syns rakt framifrån, kostar några hundralappar och finns i de flesta mobilbutiker.

9. Lösenord som håller

Ett starkt lösenord är långt och unikt. Det viktigaste är att du **inte använder samma lösenord på flera ställen**. Läcker ett lösenord från en webbutik provar bedragare det automatiskt på din e-post, Facebook och andra tjänster.

Gör en lösenfras

Ett bra knep är att sätta ihop fyra slumpmässiga ord, till exempel **Kaffe Cykel Moln Hallon**. Det är lätt att komma ihåg men nästan omöjligt att gissa. Längd är viktigare än konstiga tecken.

Hur sparar man bäst sina olika lösenord?

Med en lösenordshanterare. Det är ett digitalt kassaskåp som kommer ihåg alla dina lösenord och fyller i dem åt dig. Du har troligen redan en: **Lösenord** på iPhone och **Googles lösenordshanterare** på Android och i Chrome. Fristående alternativ är till exempel Bitwarden och 1Password. En anteckningsbok hemma i en låda är också okej, så länge den aldrig följer med ut.

Hur säkert är Google? Kan någon få reda på mitt lösenord där?

Google hör till de säkraste tjänsterna som finns, särskilt om du slår på tvåstegsverifiering eller använder en passkey. Googles lösenordshanterare varnar dessutom om något av dina lösenord har läckt. Kontrollera dina lösenord på **passwords.google.com** under **Lösenordskontroll**.

Är det en bra idé att klicka på ”Glömt lösenord” varje gång man loggar in?

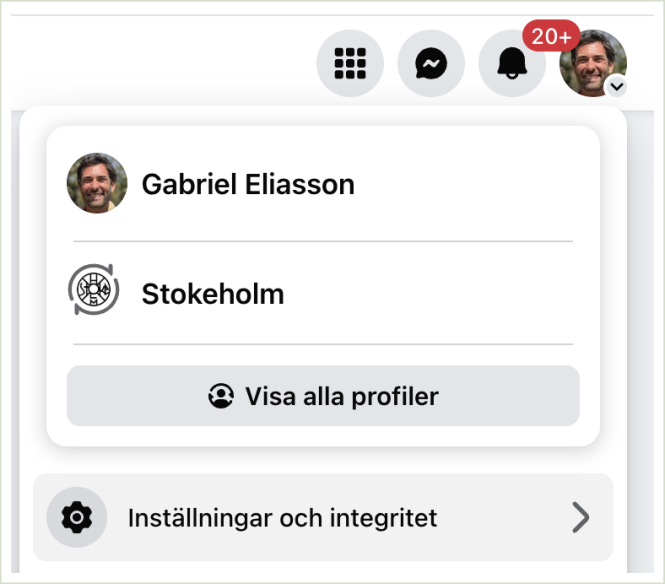
En deltagare i Blekinge tipsade om det, och det fungerar faktiskt, eftersom du får ett nytt lösenord varje gång. Det kräver dock att din e-post är väl skyddad, eftersom den då blir nyckeln till allt. En lösenordshanterare eller passkeys är enklare i längden.

10. Gör dina konton i sociala medier privata

Allt du delar öppet i sociala medier kan användas av bedragare: namn på barnbarn, var du bor, när du är på semester, din röst i videor och bilder på ditt ansikte. Genom att göra kontona privata ser bara de du själv har godkänt vad du delar.

Facebook: gör integritetskontrollen

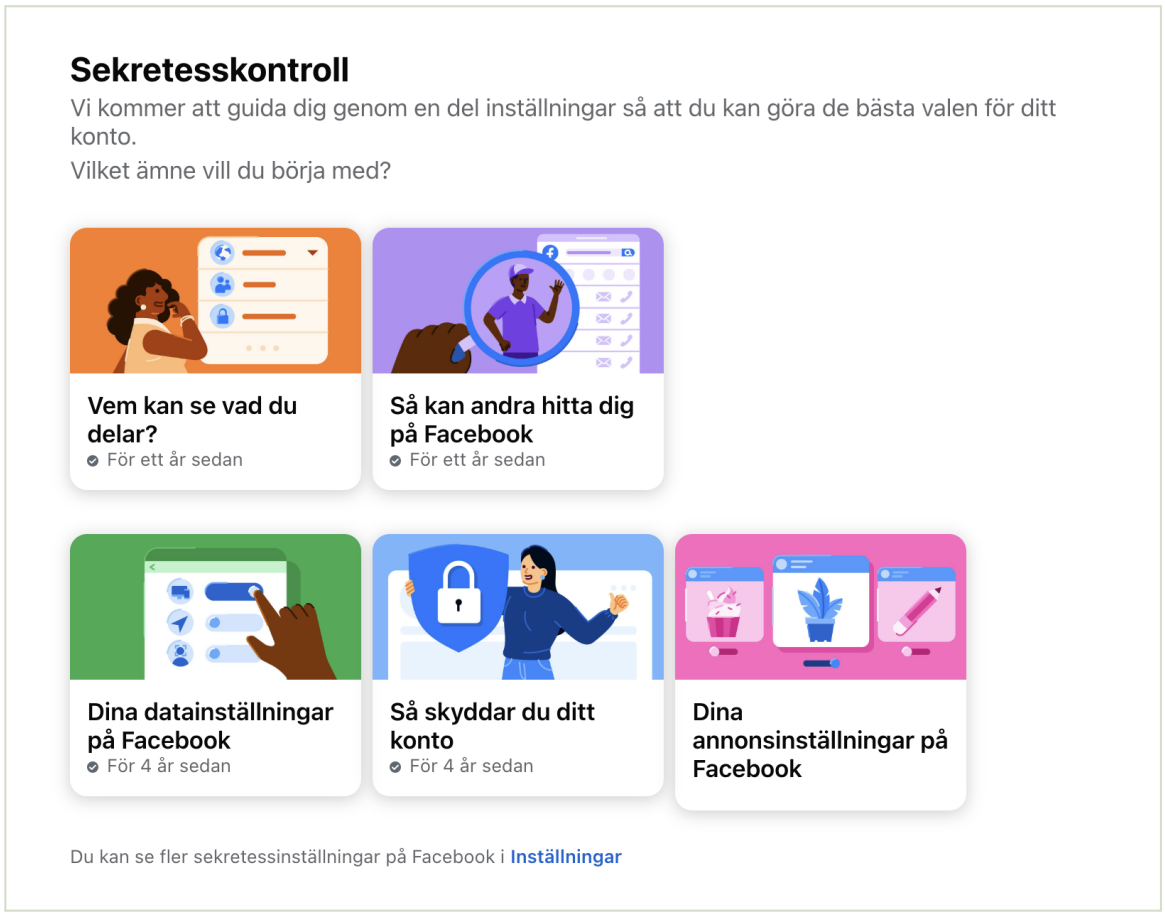
Facebook har en inbyggd guide som går igenom de viktigaste inställningarna. Bilderna nedan visar hur det ser ut på datorn. I mobilen hittar du samma sak under menyn med tre streck och kugghjulet.



Steg 1: Klicka på din profilbild uppe till höger och välj Inställningar och integritet.



Steg 2: Välj Integritetskontroll.

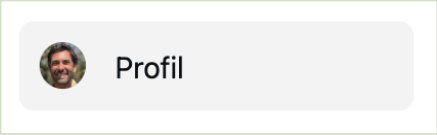


Steg 3: Sekretesskontrollen guidar dig genom inställningarna, ett ämne i taget.

Facebook använder både orden integritetskontroll och sekretesskontroll. Det är samma sak. Gå igenom ämnena så här:

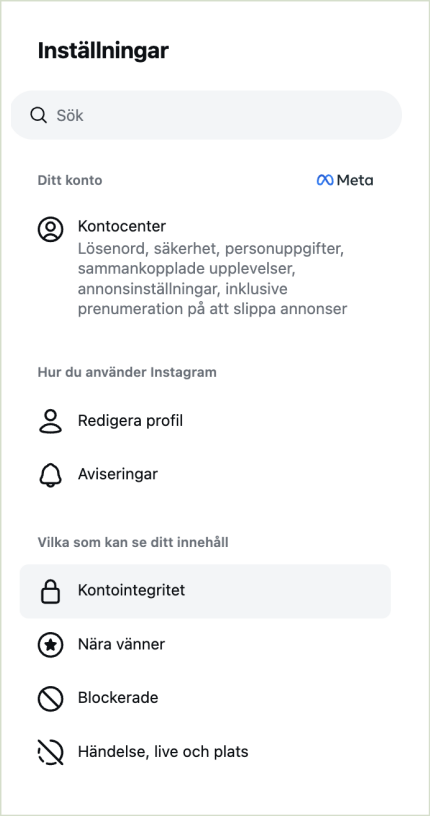
Ämne	Gör så här
Vem kan se vad du delar?	Välj **Vänner** för framtida inlägg. Välj **Begränsa tidigare inlägg**, så blir även gamla öppna inlägg synliga bara för vänner. Sätt telefonnummer, e-post och födelsedag till **Endast jag**.
Så kan andra hitta dig på Facebook	Låt bara **Vänners vänner** skicka vänförfrågningar. Välj **Endast jag** för vem som kan söka upp dig med telefonnummer och e-post. Stäng av att sökmotorer utanför Facebook länkar till din profil.
Så skyddar du ditt konto	Slå på tvåfaktorsautentisering och få varningar om okända inloggningar.
Dina datainställningar	Se vilka appar och webbplatser som är kopplade till ditt konto, och ta bort dem du inte använder.
Dina annonsinställningar	Styr vilka uppgifter som används för att visa annonser för dig.

Instagram: slå på privat konto

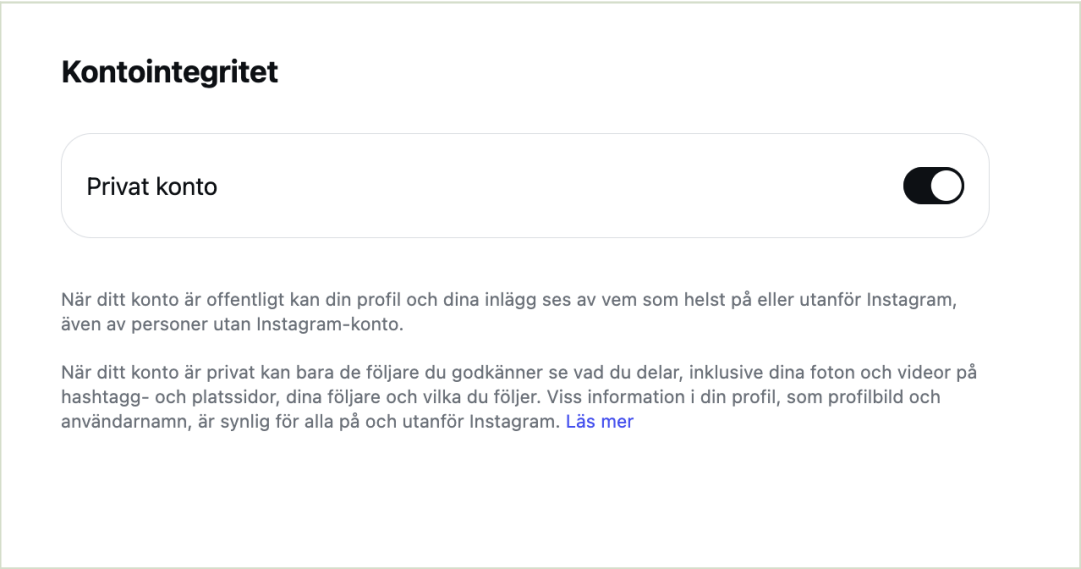


Steg 1: Klicka på Profil. På datorn finns den i menyn till vänster, i mobilen nere till höger.

Klicka sedan på kugghjulet på datorn, eller på de tre strecken uppe till höger i mobilen, för att komma till **Inställningar**.



Steg 2: Under rubriken Vilka som kan se ditt innehåll, välj Kontointegritet.



Steg 3: Slå på Privat konto. Reglaget blir mörkt när det är påslaget.

Bra att veta: Med ett privat konto ser bara de följare du har godkänt dina bilder och inlägg. Din profilbild och ditt användarnamn syns ändå för alla. Välj därför en profilbild som du är bekväm med att främlingar ser.

WhatsApp

Är WhatsApp lika öppet som Facebook?

Nej. WhatsApp är en meddelandeapp, inte ett socialt nätverk, och alla meddelanden är krypterade så att bara du och mottagaren kan läsa dem. Men den som har ditt telefonnummer kan beroende på dina inställningar se din profilbild, ditt namn och när du senast var aktiv. Ändra det så här:

STEGFÖRSTEG

Skydda din profil i WhatsApp

1. Öppna **Inställningar** och välj **Integritet**.
2. Sätt **Profilbild**, **Om** och **Senast sedd och online** till **Mina kontakter**.
3. Under **Grupper**, välj **Mina kontakter**, så kan inte främlingar lägga till dig i grupper.
4. Under **Samtal**, slå på **Tysta okända uppringare**.

Facebookgrupper och vänförfrågningar

Om jag går med i en grupp på Facebook, kan alla i gruppen se min privata sida?

Nej. Gruppmedlemmarna kan se att du är med i gruppen, ditt namn och din profilbild, och det du själv skriver i gruppen. Det du har gjort privat på din egen sida kan de inte se. Tänk på att det du skriver i en **offentlig** grupp kan läsas av vem som helst.

Vad kan en bedragare komma åt om jag accepterar en falsk vänförfrågan eller klickar på ett falskt inlägg?

En falsk vän kommer inte åt din dator eller telefon. Däremot kan hen se allt du delar med dina vänner, och använda det för att lura dig eller dina vänner. Att bara klicka på ett inlägg är oftast inte farligt i sig. Risken uppstår om du sedan loggar in, lämnar ut uppgifter eller laddar ned något.

Tips: Får du en vänförfrågan från någon du redan är vän med? Då är det troligen en kopia av din väns konto. Tacka nej och säg till din vän, gärna via telefon.

Bilder på nära och kära

Vad ska man tänka på när man laddar upp bilder på nära och kära?

Fråga först om personen vill vara med. Dela helst bara med vänner, inte öppet. Undvik att skriva ut barnbarnens fullständiga namn, skola eller var ni befinner er just nu. Tänk också på att videor där någon pratar kan användas för röstkloning, och att öppna bilder ger bedragare information de kan använda för att låta trovärdiga.

11. Länkar, appar och smarta prylar

Om du råkar klicka på en länk

Vad händer om jag råkar klicka på en länk, till exempel i en falsk annons? Kan man stoppa det?

Oftast händer ingenting direkt. Länken öppnar en webbsida, och det farliga är det som kommer sedan: att du loggar in, fyller i kortuppgifter, godkänner BankID eller laddar ned något. Stäng sidan direkt, så är du oftast säker.

GÖRSÅHÄR

Har du lämnat ut uppgifter på en falsk sida?

1. Har du lämnat ut kortuppgifter eller godkänt BankID: **ring banken direkt** och spärra.
2. Har du skrivit in ett lösenord: byt lösenordet på riktiga sidan, och på alla andra ställen där du använder samma.
3. Har du laddat ned något: ta bort appen eller filen, och kör en uppdatering av telefonen eller datorn.

Om telefonen har blivit hackad

Tecken på att ett konto eller en telefon har blivit hackad: meddelanden skickas som du inte har skrivit, du får varningar om inloggningar du inte känner igen, ditt lösenord har ändrats utan att du gjort det, eller okända appar har dykt upp.

STEGFÖRSTEG

Om din telefon eller ditt konto skickar meddelanden du inte skrivit

1. Byt lösenord på det konto som har drabbats, till exempel Facebook eller e-posten, från en annan enhet om du kan.
2. Logga ut alla andra enheter. På Facebook finns det under **Kontocenter**, **Lösenord och säkerhet**, **Var du är inloggad**.
3. Slå på tvåstegsverifiering.
4. Varna dina vänner så att de inte svarar på meddelandena.
5. Hjälper inget av detta: kontakta butiken eller din operatör och återställ telefonen till fabriksinställningar. Se till att du har en säkerhetskopia av bilderna först.

Uppdateringar och falska varningar

På Facebook sprids varningar om att man inte ska uppdatera telefonen till en viss version. Stämmer det?

Nästan alltid är det kedjebrev som saknar grund. Uppdateringar från Apple och Google täpper till säkerhetshål och är bland det viktigaste du kan göra för din säkerhet. Uppdatera alltid via telefonens egna inställningar: **Inställningar, Allmänt, Programuppdatering** på iPhone, och **Inställningar, System, Systemuppdatering** på Android. Klicka aldrig på uppdateringslänkar i meddelanden.

Lyssnar telefonen eller tv:n på oss?

Spelar telefoner och tv-apparater in det vi säger för att visa riktad reklam?

Det finns inga bevis för att mobiltelefoner i hemlighet lyssnar för att visa reklam, och det vore olagligt. Annonserna bygger i stället på vad du söker, klickar på och var du befinner dig, vilket kan kännas som att telefonen har lyssnat. Däremot finns det smarta tv-apparater som registrerar **vad du tittar på** för att anpassa reklam. Den funktionen går att stänga av i tv:ns inställningar, ofta under namn som tittarinformation eller ACR.

Tips: Se vilka appar som får använda mikrofonen. På iPhone: **Inställningar, Integritet och säkerhet, Mikrofon**. På Android: **Inställningar, Säkerhet och integritet, Behörighetshanterare, Mikrofon**. En liten orange eller grön prick i skärmens hörn visar när mikrofonen eller kameran används.

Robotdammsugare och andra smarta prylar

Finns det risker med en robotdammsugare med kamera som är uppkopplad till hemmets nätverk?

Ja, en viss risk finns, som med alla uppkopplade prylar. Välj kända märken, uppdatera appen och prylen regelbundet, och ha ett starkt lösenord på ditt wifi. Behöver du inte kamerafunktionen, stäng av den i appen. Har din router ett gästnätverk kan du koppla smarta prylar dit, så hålls de åtskilda från datorn och telefonen.

Kan någon skimma mitt kontokort?

Skimning vid bankomater har blivit ovanligt, men titta efter lösa delar och skärma alltid av med handen när du slår koden. Kontaktlös betalning kräver att kortet hålls mycket nära en terminal, och beloppen är begränsade. Slå på notiser i bankappen, så ser du direkt om något dras från kortet.

12. Om du ändå blir lurad

Det finns ingenting att skämmas över. Skammen hjälper bara bedragarna. Den som berättar kan få hjälp snabbare och varnar dessutom andra.

GÖRSÅHÄRDIREKT

Om du misstänker att du har blivit lurad

1. **Ring banken direkt** och spärra kort, konton och BankID. Numret finns på kortet och på bankens webbplats. Spärrtjänsten är öppen dygnet runt.
2. **Polisanmäl** på 114 14 eller polisen.se. Ring 112 om brottet pågår.
3. **Byt lösenord**, börja med e-post och bank.
4. **Berätta för någon** du litar på. Brottsofferjouren svarar på 116 006.

Nummer	Till vem	När
Bankens spärrtjänst	Din bank	Först av allt, om pengar, kort eller BankID är inblandade
112	Polis, ambulans, räddningstjänst	När brottet pågår eller någon står vid din dörr
114 14	Polisen	För att anmäla brott som inte pågår
116 006	Brottsofferjouren	För stöd och någon att prata med
7726	Din mobiloperatör	Vidarebefordra bluff-sms, gratis

När är lurendrejeri ett brott?

Enligt brottsbalken är det bedrägeri när någon medvetet vilseleder en annan person att göra något, till exempel betala eller lämna ut uppgifter, som ger bedragaren en vinning och den lurade en skada. Det är alltså brottsligt så fort någon luras på pengar eller värden. Även försök till bedrägeri är brottsligt, så anmäl gärna även de försök som du har genomskådat.

Personuppgifter på nätet

Hur tar jag bort mina uppgifter från sajter som Hitta, Ratsit och Mrkoll?

Sajterna hämtar uppgifterna från offentliga register, men de flesta låter dig dölja dig. Leta efter länkar som **Ta bort mina uppgifter** eller **Dölj mig**, ofta längst ned på sidan, och identifiera dig med BankID. Varje sajt fungerar lite olika, och uppgifterna kan dyka upp igen efter en tid. Fråga gärna en AI-tjänst, till exempel: *Hur tar jag bort mina uppgifter från Mrkoll? Förklara steg för steg*.

Är det farligt att lämna ut de fyra sista siffrorna i personnumret?

Ditt personnummer är en offentlig uppgift i Sverige och går att få fram av vem som helst. Därför är siffrorna i sig inte så hemliga som många tror. Lämna ändå inte ut dem i onödan, eftersom bedragare använder dem för att låta trovärdiga. Det som verkligen ska skyddas är BankID, koder och lösenord.

Säljare ringer och vill sälja id-skydd. Är det seriöst?

Sådana samtal är fortfarande vanliga. Det finns seriösa id-skyddstjänster, och de ingår ibland redan i din hemförsäkring eller i bankens tjänster. Men köp aldrig något i ett samtal som du inte själv har tagit initiativ till. Be om information skriftligt och jämför i lugn och ro.

13. Frågor om AI från chatten

Under lektionen kom också många frågor om AI i allmänhet. Här är svaren.

Appar och verktyg

Kan man ha NotebookLM i datorn?

Ja. Gå till **notebooklm.google.com** i webbläsaren och logga in med ditt Google-konto. Det fungerar på samma sätt som i appen.

Jag har hittat appen Perplexity på min nya Samsung. Är den tillförlitlig?

Ja, Perplexity är en seriös AI-tjänst och finns förinstallerad på vissa nya Samsung-telefoner. Den fungerar som en sökmotor där du får ett samlat svar i stället för en lista med länkar, och den kan använda flera olika AI-modeller. En stor fördel är att den visar **vilka källor** svaret bygger på. Klicka gärna på källorna och kontrollera viktiga uppgifter, eftersom även Perplexity kan ha fel.

Vad är Claude bra på?

Claude är en AI-assistent från företaget Anthropic, och finns på claude.ai och som app. Den är särskilt bra på att skriva och bearbeta text, sammanfatta långa dokument, resonera kring svåra frågor och skapa små verktyg och webbsidor. Den skapar inte bilder på samma sätt som ChatGPT och Gemini.

Finns det fler verktyg än Gemini och Suno för att skapa musik?

Ja, till exempel **Udio**, som liknar Suno. Utbudet ändras snabbt, så fråga gärna en AI-tjänst vilka musikverktyg som finns just nu.

Vad är fördelen med den tillfälliga chatten i ChatGPT?

En tillfällig chatt sparas inte i din historik, påverkar inte ChatGPT:s minne om dig och används inte för att träna AI:n. Den passar när du vill fråga om något personligt, eller testa något utan att det sparas. Du hittar den uppe till höger i en ny chatt.

AI, el och samhälle

Hur mycket el drar det att skapa en bild med AI? Och jämfört med ett vanligt foto?

En studie från Hugging Face och Carnegie Mellon University visade att det i genomsnitt gick åt ungefär 3 kilowattimmar el för att skapa tusen AI-bilder. Det blir ungefär 3 wattimmar per bild, vilket motsvarar en stor del av en mobilladdning. Nyare modeller är ofta effektivare, så se det som en grov uppskattning. Ett vanligt foto med mobilkameran drar så lite el att det knappt märks på batteriet, i storleksordningen tusen gånger mindre.

Vem styr utvecklingen av AI? Och ska vi lägga vår energi på AI?

I dag styrs utvecklingen främst av stora teknikföretag i USA och Kina, som OpenAI, Google, Meta, Microsoft och Anthropic. Inom EU finns sedan 2024 en AI-förordning som sätter regler för hur AI får användas. AI kan skapa stora vinster för samhället, till exempel inom vården, men förbrukar också mycket el och vatten. Mitt svar är: ja, men med eftertanke. Vi bör satsa på AI som gör nytta för människor, inte utveckla AI till varje pris. Deltagarna i Nivren sammanfattade det bra: granska utvecklingen kritiskt.

Vad kommer härnäst efter AI?

Ingen vet säkert, men mycket pekar på att AI blir mer självständig. AI-agenter som utför uppgifter åt oss, robotar i hemmet och vården, och AI som är inbyggd i allt från glasögon till bilar. Grunden från den här kursen, att vara nyfiken och sunt misstänksam, kommer att gälla även då.

14. Det här tar grupperna med sig

Efter gruppsamtalen skrev cirkelledarna vad grupperna tar med sig. Här är ett urval från hela landet:

Grupp	Det här tar vi med oss
Lund	Vi börjar med att införa ett kodord i våra familjer.
Mönsterås	Kodord i familjen är en bra idé. Vi funderar också på digital dubbelattest i föreningen.
Norsjö	Vi använder kodord, dubbelkollar vem som ringer, lämnar inte ut uppgifter och klickar inte på okända länkar.
Eksjö	Vi kommer att lägga på luren och vara mer otrevliga i telefon.
Ystad	Vi ska prata om kodord med våra familjer och tänka en gång till innan vi lämnar ut uppgifter.
Kalmar	Vi behöver vara mer observanta i alla möjliga sammanhang.
Jönköpings län	Vi har lärt oss att vara lite mer misstänksamma.
Tavelsjö	Vi har lärt oss att vi kan bli lurade.
Strömsund	Vi har lärt oss om 7726, och försöker minnas de kodord vi redan har bestämt.
Robertsfors, Tranås, Hammarstrand, Blekinge, Sölvesborg	Kodord i familjen!

Digital dubbelattest i föreningen

Gruppen i Mönsterås tog upp något viktigt inför nästa lektion. Föreningar är också måltavlor. Ett vanligt bedrägeri är att kassören får ett mejl som ser ut att komma från ordföranden, med en brådskande begäran om att betala en faktura. Med **dubbelattest** i internetbanken måste två personer godkänna varje betalning med BankID. Det gör att en enskild person inte kan luras att betala. Fråga föreningens bank hur ni slår på det.

15. Gör det här i veckan

- [ ] Bestäm ett kodord med din familj.
- [ ] Byt hälsningen på röstbrevlådan till standardhälsningen.
- [ ] Gör integritetskontrollen på Facebook och slå på privat konto på Instagram.
- [ ] Ställ in WhatsApp så att bara dina kontakter ser din profilbild.
- [ ] Slå på tvåstegsverifiering på ditt Google-konto och på Facebook.
- [ ] Prova att skapa en passkey för ditt Google-konto.
- [ ] Uppdatera telefonen via inställningarna.
- [ ] Spara bankens spärrnummer i telefonen, så har du det när det behövs.
- [ ] Klistra in ett misstänkt sms i en AI-tjänst och fråga om det kan vara ett bedrägeri.
- [ ] Berätta för en vän eller granne vad du har lärt dig i dag.

Det här har du lärt dig

> Social manipulering spelar på känslor som brådska, rädsla och medkänsla. AI gör bedrägerierna svårare att upptäcka, men knepen är desamma.
> Röster, filmer och meddelanden kan vara falska även om de verkar äkta. Försök inte avgöra om något är AI, använd sunt förnuft.
> Kodord, att lägga på och ringa upp, och att aldrig godkänna BankID åt någon annan skyddar dig mot de flesta bedrägerier.
> Tvåstegsverifiering, passkeys och privata konton i sociala medier gör det mycket svårare för bedragare.
> Den som blir lurad har inget att skämmas över. Ring banken först, sedan polisen.

Nästa lektion: AI för föreningsarbete

Måndag 23 november 2026, kl. 13.30. Sista lektionen i serien handlar om hur AI kan hjälpa till i föreningen: att skriva inbjudningar och protokoll, planera aktiviteter och göra affischer. Det blir även då en praktisk övning, kopplad till föreningsarbetet. Bjud gärna in föreningens styrelse, som SV Mora redan har gjort!

Har du frågor eller vill dela något från veckan? Mejla mig gärna på **hej@gabrieleliasson.se**.

16. Länkar från lektionen

Alla länkar vi visade under lektionen, samlade på ett ställe. Klicka på länkarna i pdf:en eller skriv in adressen i webbläsaren.

Källa	Rubrik och länk
TV4	Bedrägerierna att se upp med just nu https://www.tv4.se/artikel/1jjy0KM3UrDselq8WznU7c/trippelvarnar-bedraegerierna-att-se-upp-med-just-nu
TV4	Polisen varnar för AI-klonade röster https://www.tv4.se/artikel/6I17x4luQZ6OJR9qxkIPZL/varnar-bedraegerier-med-ai-klonade-roester-sker-redan-i-sverige
TV4	Ann-Lis, 76, hörde sin dotters röst https://www.tv4.se/artikel/u0C79WoRKH2DTrjFboGrL/ann-lis-76-blev-uppringd-av-bedragare-hoer-min-dotters-roest
TV4	Steffo uppringd av AI förklädd till kollegan https://www.tv4.se/artikel/1C613rziJuenczTYiQ9bxC/steffo-uppringd-av-ai-foerklaedd-till-kollegan-aer-det-verkligen-du-jenny
SVT	Så lätt kan din röst stjälas https://www.svt.se/nyheter/utrikes/ai-klonade-roster-anvands-i-bedragerier-roststolder-artificiell-intelligens
SVT	AI-Tegnell i falsk reklam https://www.svt.se/nyheter/inrikes/bedragare-anvander-ai-tegnell-i-falsk-reklam
SVT	Svenska polisen deepfejkas i miljonbluff https://www.svt.se/nyheter/inrikes/har-deepfejkas-svenska-polisen-i-miljonbluff-polisanmaler-oerhort-allvarligt
SVT	Uppdrag granskning utnyttjas i bluffkampanj https://www.svt.se/nyheter/inrikes/uppdrag-granskning-utnyttjas-i-en-bluffkampanj-kanns-bedrovligt
SVT	Jenny Strömstedt och Olof Lundh gillrar en fälla för bedragaren https://www.svt.se/nyheter/granskning/ug/obs-embargo-630-har-gillrar-jenny-stromstedt-och-olof-lundh-en-falla-for-bedragaren
TV4	Bluffannonsörernas nya knep https://www.tv4.se/artikel/5eghzbvvTZi2XkX2cEC9Uz/bluffannonsoerernas-nya-knep-sa-luras-du-att-klicka
TV4	Här blir bildexperten lurad av AI https://www.tv4.se/klipp/va/28c563c92b24fda9a42f/har-blir-bildexperten-lurad-av-ai

Källa	Rubrik och länk
TV4	Polisen varnar för ny våg av guldbedrägerier https://www.tv4.se/artikel/3oTCM87V1sCWqJ3oh6Hb60/polisen-varnar-foer-ny-vag-av-guldbedraegerier
Polisen	Nya bedrägeriförsök mot äldre https://polisen.se/aktuellt/nyheter/bergslagen/2026/september/polisen-varnar-efter-nya-bedrageriforsok-mot-aldre/
Polisen	Lyssna på riktiga bedragarsamtal https://polisen.se/telefonbedragerier
Polisen	Prata om bedrägerier, korta filmer https://polisen.se/prata-bedragerier
Polisen	Våga vara otrevlig https://polisen.se/aktuellt/nyheter/nationell/2026/september/kraftsamlar-mot-bedragerier--fortsatt-vaga-vara-otrevlig/
Polisen	SverigeID, den statliga e-legitimationen https://polisen.se/tjanster-tillstand/pass-och-nationellt-id-kort/statlig-e-legitimation-sverigeid/
Dagens PS	Bedrägerier mot äldre kvinnor har fördubblats https://www.dagensps.se/privatekonomi/bra-bedragerier-mot-aldre-kvinnor-har-mer-an-fordubblats-pa-sex-ar/

17. Ordlista

Ord	Förklaring
BankID	Elektronisk legitimation från bankerna. Används för att logga in och skriva under digitalt.
Biometri	Att identifiera sig med kroppen, till exempel ansikte eller fingeravtryck.
Deepfake	En falsk video eller bild, skapad med AI, där en verklig person ser ut att säga eller göra något.
Dubbelattest	Att två personer måste godkänna en betalning.
Kodord	Ett hemligt ord som familjen använder för att bekräfta att det verkligen är rätt person.
Lösenordshanterare	Ett digitalt kassaskåp som sparar och fyller i dina lösenord.
Passkey	Inloggning utan lösenord, där du låser upp med ansikte, finger eller PIN-kod. Kallas även nyckel.
Phishing (nätfiske)	Falska mejl, sms eller webbsidor som försöker lura dig att lämna ut uppgifter.
Romansbedrägeri	Bedrägeri där bedragaren bygger upp en kärleksrelation för att till slut be om pengar.
Röstkloning	När AI härmar en verklig persons röst utifrån en kort inspelning.
Social manipulering	Att lura människor med hjälp av känslor, stress och förtroende i stället för teknik.
Spoofing	När bedragaren förfalskar avsändaren, så att ett samtal, sms eller mejl ser ut att komma från någon annan.
SverigeID	Statlig e-legitimation kopplad till det nationella id-kortet. Lanseras 1 december 2026.
Tvåstegsverifiering	Inloggning i två steg, med både lösenord och till exempel en kod i telefonen.
Vishing	Bedrägeri via telefonsamtal, där bedragaren ofta utger sig för att vara bank eller polis.