



Trygghet och säkerhet



# Agenda

- Inledning
- Skydda din personliga information
- Undvik bedrägerier och fällor
- Skapa säkra lösenord



# Inledning

I en värld där internet blir alltmer en del av vår vardag, är det viktigt att känna sig trygg och säker online.

Detta avsnitt är särskilt framtaget för att ge dig, som kanske inte växt upp med digital teknik, de verktyg och den kunskap du behöver för att navigera på nätet med självförtroende.



# Diskutera

- Varför tror ni att det är viktigt att förstå och känna sig trygg med internetanvändning, särskilt för de som inte växte upp med tekniken?
- Vilka är några av de största farhågorna ni har när det gäller att använda internet?



# Skydda din personliga information

# Skydda din personliga information

## 1. Användning av starka och unika lösenord

Starka och unika lösenord är viktiga för att skydda dina konton från obehörig åtkomst. Det minskar risken för identitetsstöld och andra former av cyberbrott.

## 2. Tvåfaktorsautentisering

Tvåfaktorsautentisering är en säkerhetsprocess där användaren måste tillhandahålla två olika sätt för att verifiera sin identitet.

## 3. Hantering av personlig information

Dela din personliga information med samma försiktighet som du skulle dela en familjehemlighet.





# Diskutera

- Hur kan betalningar på nätet göra livet enklare?
- Vad gör ni för att känna er trygga när ni betalar på nätet?



# Undvik bedrägerier och fällor





## Phishing

Phishing är ett försök att få känslig information såsom användarnamn, lösenord och kreditkortsdetaljer genom att utge sig för att vara en pålitlig avsändare i en elektronisk kommunikation.



### Tips!

- Var försiktig med e-postmeddelanden eller meddelanden som begär personlig information eller hänvisar till en webbplats med okända länkar.
- Kontrollera avsändarens e-postadress och var uppmärksam mot stavfel eller konstiga formuleringar.



## Spoofing

Spoofing är en metod där bedragare förfalskar identiteter- som telefonnummer eller e-postadresser - för att få det att verka som om de är någon du känner och litar på.



### Tips!

- Om du får ett oväntat samtal eller meddelande som ber om personlig information eller uppmanar dig att vidta åtgärder, var skeptisk.
- Kom ihåg att ingen legitim organisation kommer att be dig om dina lösenord eller PIN-koder via telefon eller e-post.

## Onlinebedrägerier

Det finns flera sätt som bedragare kan försöka lura dig på nätet, några vanliga är:

- Lotteribedrägerier
- Förmånstagarbedrägerier
- Nätdejtingbedrägerier
- Välgörenhetsbedrägeri
- Reparationsbedrägerier



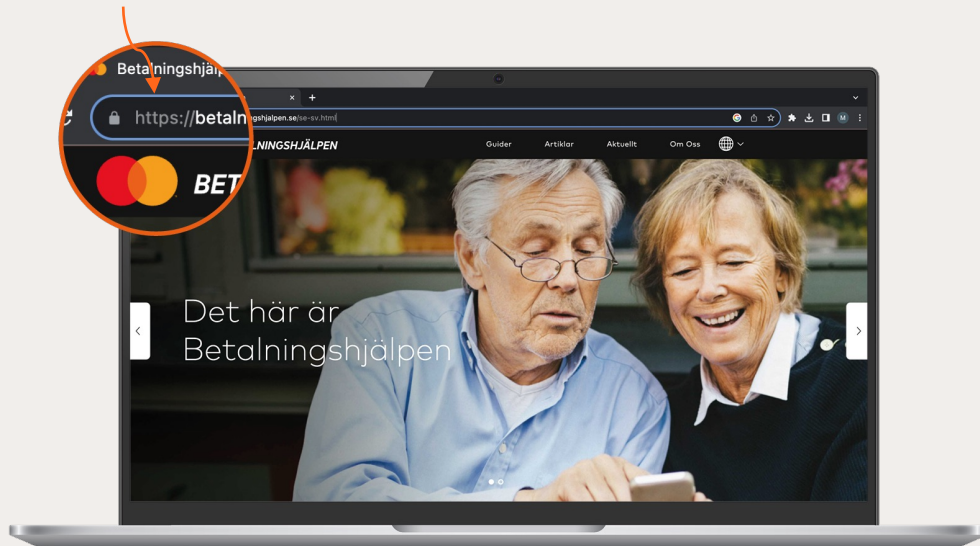


Ett enkelt sätt att se att webbplatsen är säker att kolla om webbadressen börjar med "https".

## Säker handel på nätet

När du handlar online, se till att webbplatsen är säker.

Kontrollera också att webbplatsen har goda recensioner och goda omdömen. Hör gärna med vänner och bekanta om de känner till hemsidan du vill handla från.





# Diskutera

- Har någon av er någonsin stött på ett phishing-försök?  
Hur kände ni igen det?
- Vilka är några varningssignaler ni letar efter för att identifiera en potentiell bluffwebbplats?
- Hur kan man bäst utbilda andra om riskerna med onlinebedrägerier?



**Säkra lösenord**



## Mer om säkra lösenord

### 1. Skapa starka lösenord

Skapa lösenord som är minst 12 tecken långa och innehåller en blandning av bokstäver, siffror och specialtecken.

### 2. Använd en lösenordshanterare

En lösenordshanterare är ett program som skapar, lagrar och hanterar dina lösenord för olika webbplatser och appar.

### 3. Uppdatera lösenord löpande

Genom att regelbundet uppdatera dina lösenord minskar du risken för att någon ska få obehörig åtkomst till dina konton.

För bästa säkerhet rekommenderas det att du ändrar dina lösenord var tredje till sjätte månad.

### 4. Användning av biometrisk säkerhet

Biometrisk säkerhet handlar om att använda dina unika kännetecken, som ditt fingeravtryck eller ditt ansikte, för att bekräfta din identitet.



# Diskutera

- Hur ofta ändrar ni era lösenord? Använder ni samma lösenord för flera konton?
- Vad tycker ni om idén att använda en lösenordshanterare? Ser ni några potentiella risker med det?
- Hur känner ni för att använda biometrisk säkerhet, som fingeravtryck eller ansiktsgenkänning, för att skydda era enheter och konton?



## Sammanfattning

- När vi navigerar på internet, lämnar vi spår bakom oss som tillsammans bildar vårt "digitala fottryck".
- Det är viktigt att vara medveten om vilken typ av information vi delar online.
- Håll dig uppdaterad med de senaste säkerhetstipsen för att skydda din personliga information.
- Internet är en plattform där du kan upptäcka, skapa och hålla kontakten med nära och kära.





# Diskutera

- Vad menas med ett "digitalt fotavtryck"? Hur kan vi bäst hantera och skydda vårt digitala fotavtryck?
- Vilka steg kommer ni att ta efter den här sessionen för att förbättra er online-säkerhet?



## Testa dina kunskaper!

Du har nu gått igenom vår utbildning på temat Trygghet och säkerhet  
– vill du testa dina kunskaper, scanna QR-koden för att ta dig till quizet.



Scanna QR-koden  
med din mobilkamera



# Tack!

Det finns fortfarande mycket att lära sig.  
Gå in på **betalningshjälpen.se** för att se våra övriga utbildningar.