



BETALINGSHJÆLPEN

Tryghed og sikkerhed



Program

- Indledning
- Beskyt dine personlige oplysninger
- Undgå svindel og fælder
- Opret stærke adgangskoder



Indledning

Internettet bliver en stadig større del af vores hverdag, og det er derfor vigtigt at føle sig tryk og sikker online.

Her bliver du introduceret til værktøjer og viden, du måske har brug for, så du kan navigere på nettet med selvtillid – også selvom du er helt ny på området.



Spørgsmål

- Hvorfor tror I, det er vigtigt at forstå og føle sig tryk ved internetbrug, især for dem der ikke er vokset op med teknologien?
- Hvilke er nogle af de største bekymringer, I har, når det gælder brug af internettet?



Beskyt dine personlige oplysninger

Beskyt dine personlige oplysninger

- 1. Brug stærke adgangskoder**
Gode og sikre adgangskoder er vigtige for at beskytte dine konti mod uautoriseret adgang. Det reducerer risikoen for identitetstyveri og andre former for cyberkriminalitet.
- 2. To-faktor-godkendelse**
To-faktor-godkendelse er en sikkerhedsproces, hvor brugeren skal bekræfte sin identitet på to forskellige måder
- 3. Håndtering af personlige oplysninger**
Del dine personlige oplysninger med samme omtanke, som du ville dele en familiehemmelighed.





Spørgsmål

- Hvilke typer personlige oplysninger synes du er okay at dele online – og hvilke bør man altid holde private? Hvor går grænsen for dig?
- Udover de tips, vi har talt om her, gør du så selv noget særligt for at beskytte dine personlige oplysninger online? Hvorfor eller hvorfor ikke?



Undgå svindel og fælder

Phishing

Phishing er et forsøg på at få følsomme oplysninger som brugernavne, adgangskoder og kortdetaljer ved at udgive sig for at være en pålidelig afsender i elektronisk kommunikation.



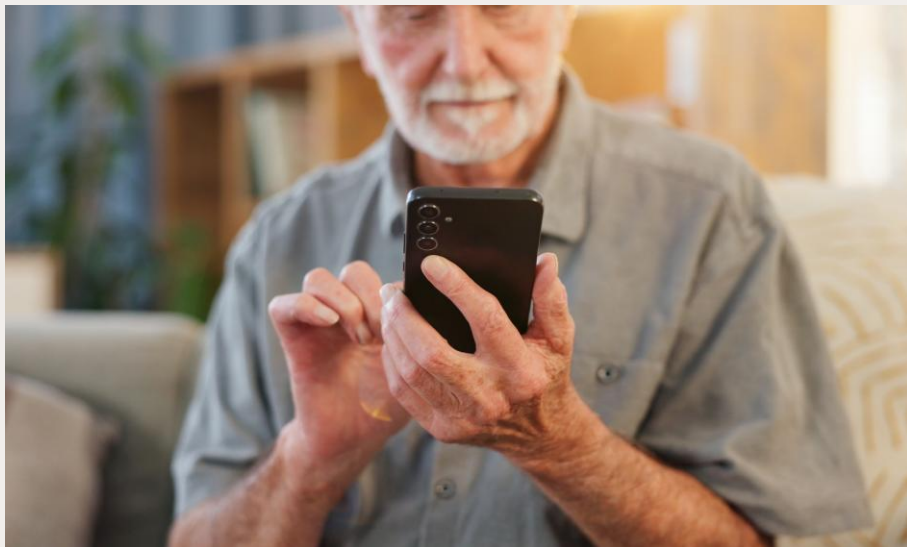
Tips!

- Vær forsigtig med e-mails eller beskeder, der beder om personlige oplysninger eller henviser til ukendte links.
- Tjek afsenderens e-mailadresse, og vær opmærksom på stavefejl eller mærkelige formuleringer.



Spoofing

Spoofing er en metode, hvor svindlere forfalsker identiteter – som telefonnumre eller e-mailadresser – for at få det til at se ud, som om de er en, du kender og stoler på.



Tips!

- Hvis du modtager et uventet opkald eller en besked, hvor du bliver bedt om at afgive personlige oplysninger eller som kræver handling, så vær skeptisk.
- Husk, ingen legitim organisation vil bede dig om adgangskoder eller PIN-kode via telefon eller e-mail.

Digital svindel

Der er flere måder, svindlere kan forsøge at narre dig på nettet. Nogle af de almindelige er:

- Lottosvindel
- Arvesvindel
- Dating-svindel
- Velgørenhedssvindel
- Teknisk support-svindel



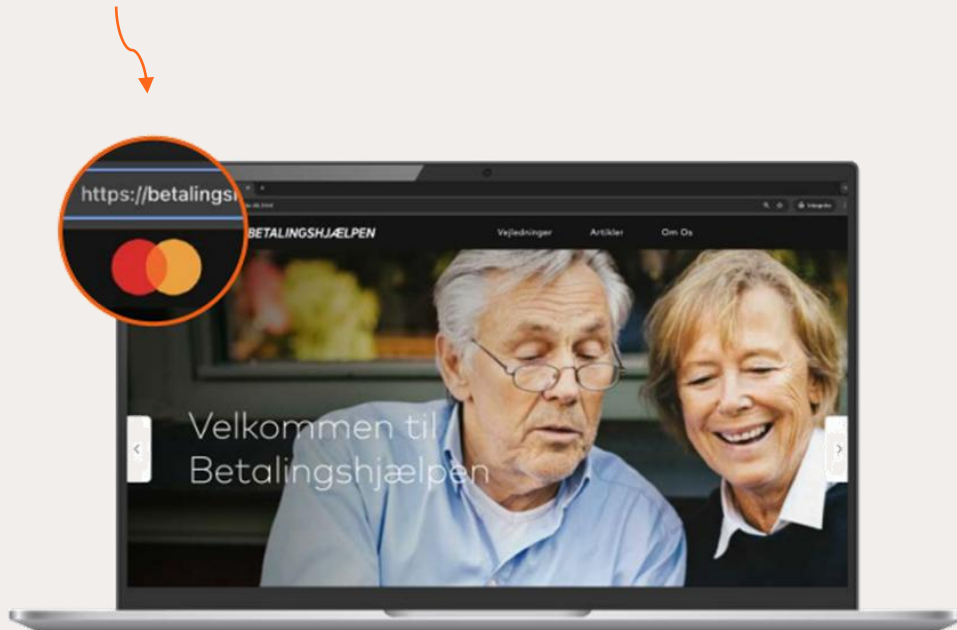


En nem måde at tjekke sikkerhed på er, at se om webadressen starter med "https".

Sikker handel på internettet

Når du handler online, skal du sikre dig, at hjemmesiden er sikker.

Tjek, at siden har gode anmeldelser og god omtale. Spørg gerne venner eller familie, om de kender siden.





Spørgsmål

- Har nogen af jer nogensinde været udsat for et phishing-forsøg? Hvordan genkendte I det?
- Hvad er de advarselstegn, I ser efter for at identificere en potentiel svindelhjemmeside?
- Hvordan kan man bedst fortælle andre om risiciene ved digital svindel?



Sikre adgangskoder



Sikre adgangskoder

1. Opret stærke adgangskoder

Vælg adgangskoder, der er på mindst 12 tegn og indeholder en blanding af bogstaver, tal og specialtegn.

2. Brug en 'password manager'

En password manager er et program, der kan oprette, gemme og håndtere dine adgangskoder til forskellige hjemmesider og apps.

3. Opdater adgangskoder regelmæssigt

Ved at ændre dine adgangskoder med jævne mellemrum mindsker du risikoen for, at uvedkommende får adgang til dine konti.

For optimal sikkerhed anbefales det, at du ændrer dine adgangskoder hver tredje til sjette måned.

4. Brug af biometrisk sikkerhed

Biometrisk sikkerhed handler om at bruge dine unikke kendetegn – som dit fingeraftryk eller ansigt – til at bekræfte din identitet.

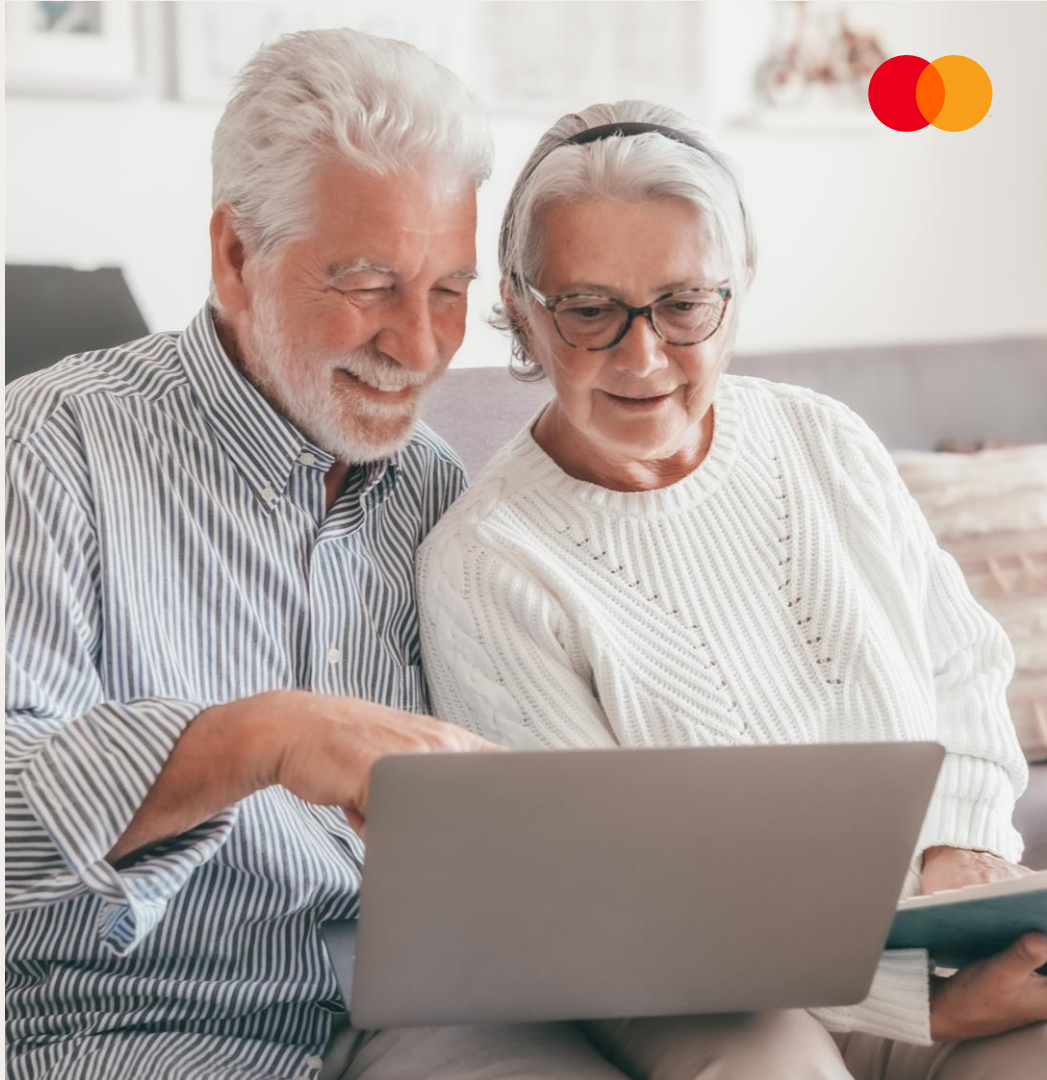


Spørgsmål

- Hvor ofte ændrer I jeres adgangskoder? Bruger I den samme adgangskode til flere konti?
- Hvad synes I om ideen om at bruge en 'password manager' (et program, der hjælper dig med at håndtere dine adgangskoder)? Ser I nogen potentielle risici ved det?
- Hvad synes I om at bruge biometrisk sikkerhed – såsom fingeraftryk eller ansigtsgenkendelse – for at beskytte jeres enheder og konti?

Opsummering

- Når vi bevæger os rundt på internettet, efterlader vi spor, som tilsammen danner vores "digitale fodaftryk".
- Det er vigtigt at være opmærksom på, hvilken type information vi deler online.
- Hold dig opdateret med de nyeste sikkerhedstips for at beskytte dine personlige oplysninger.
- Internettet er en platform, hvor du kan opdage, skabe og holde kontakt med dine kære.





Spørgsmål

- Hvad menes med et digitalt fodaftryk? Hvordan kan vi bedst håndtere og beskytte vores digitale fodaftryk?
- Hvilke skridt vil I nu tage for at forbedre jeres digitale sikkerhed?



Test din viden

Du har nu gennemgået emnet "Tryghed og sikkerhed"
– vil du teste din viden, så scan QR-koden for at tage testen.



Scan QR-koden med
kameraet i din
smartphone.



Tak!

Der er stadig meget at lære.
Gå ind på **betalingshjælpen.dk** for at se
de fem andre emner, du kan dykke ned i.