



BETALINGSHJÆLPEN

Tryghed og
sikkerhed

Indledning

Internettet er blevet en central del af vores hverdag – en ressource, der tilbyder en uendelig mængde information og muligheder for kommunikation og læring. For dem, der ikke er født ind i den digitale æra, kan det godt være en udfordring at navigere i den digitale verden. Derfor har vi skabt dette undervisningsmateriale, så du kan få mere viden om, hvordan du trygt og sikkert kan bruge internettet.

Vi starter med at tale lidt om, hvor vigtigt det er at beskytte dine personlige oplysninger – en ressource, der er lige så værdifuld digitalt som i den fysiske verden.

Derefter vil vi udforske forskellige typer digitalt bedrageri og give dig gode råd til, hvordan du kan genkende og undgå dem. Det er en vigtig færdighed både i den fysiske og digitale verden.

Vi vil give dig gode råd til, hvordan du gennemfører sikre køb, så du trygt kan handle og agere på internettet.

Til sidst går vi ind i, hvordan du skaber og vedligeholder stærke adgangskoder, der er afgørende for at beskytte din digitale identitet. Vi vil give dig råd til, hvordan du kan bruge moderne teknologi – f.eks. biometrisk sikkerhed – for at styrke din sikkerhed på internettet.

Undervisningsmaterialet giver dig et godt grundlag for at begynde at navigere trygt og sikkert på internettet. Husk dog, at den digitale verden er i konstant forandring, og at der hele tiden kommer nye teknologier, tjenester og trusler. Derfor er det vigtigt ikke kun at ruste dig med viden og værktøjer lige nu, men også at fortsætte med at holde dig opdateret. Betalingshjælpen er her for at støtte dig på din digitale rejse og opfordrer dig til regelmæssigt at opdatere din viden på området. På den måde kan du fortsætte med at være tryg og sikker, når du bruger digitale platforme.

Spørgsmål til dig
og dine venner

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 internet-tet?



Beskyt dine personlige oplysninger

1. Brug stærke adgangskoder (passwords)

Gode og sikre adgangskoder er vigtige for at beskytte dine konti mod uautoriseret adgang. Det reducerer risikoen for identitetstyveri og andre former for cyberkriminalitet. På side 8 får du tips til, hvordan du vælger en stærk og god adgangskode.

Forestil dig: Tænk på din adgangskode som en nøgle til et sikkert pengeskab, hvor du opbevarer dine mest værdifulde ejendele. Hver nøgle bør være unik og kompleks for at forhindre uautoriseret adgang.

2. To-faktor-godkendelse

To-faktor-godkendelse er en sikkerhedsproces, hvor brugeren skal bekræfte sin identitet på to forskellige måder. En almindelig metode er at bruge SMS som et supplement til navn og adgangskode. Når du logger ind på en tjeneste, sendes der en engangskode via SMS til din smartphone, og du skal indtaste koden for at fuldføre login. Det bruges f.eks. ved banktjenester, e-mail, sociale medier og offentlige tjenester.

Forestil dig: Det er som at have dobbeltlås på din dør; selvom nogen har den ene nøgle, kan de ikke komme ind uden den anden.

3. Håndtering af personlige oplysninger

Vær forsigtig med, hvilke informationer du deler digitalt. I Danmark er nogle personlige oplysninger såsom adresse og telefonnummer offentlige. Alligevel er det vigtigt at være opmærksom på, hvilken information du deler på sociale medier og andre offentlige fora.

Undgå altid at dele f.eks. personnummer, bankoplysninger eller billeder og statusopdateringer, der afslører, at du er på ferie.

Forestil dig: Hvem ville du dele dine familiehemmeligheder med? Pas på dine informationer på samme måde på internettet.

Spørgsmål til dig
og dine venner

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



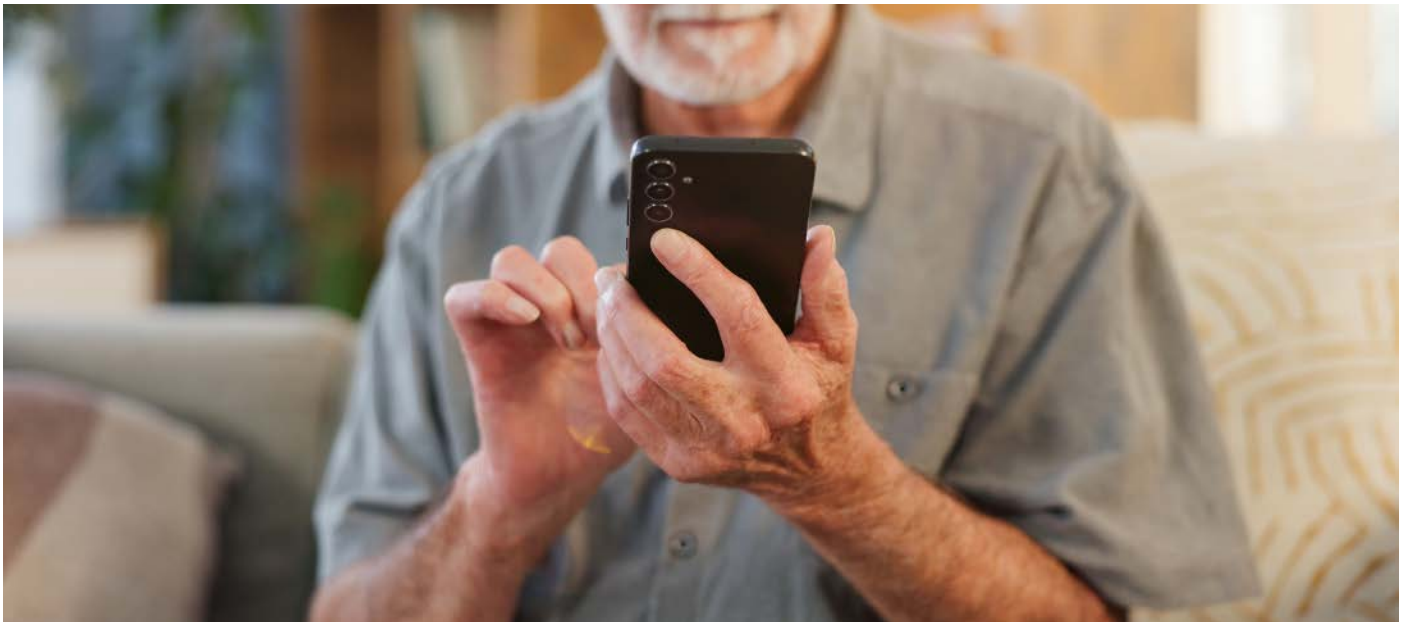
1. Phishing

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.

Forestil dig: Phishing-forsøg er som falske sælgere, der prøver at narre dig til at købe noget, du ikke har brug for eller ønsker.

Gode råd:

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



2. 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.

Forestil dig: Tænk på spoofing som en svindler, der klæder sig ud som en ven eller en officiel person for at vinde din tillid og derefter udnytte den.

Gode råd:

Hvis du modtager et uventet opkald eller besked, der beder om personlige oplysninger eller opfordrer dig til at tage handling, så vær skeptisk.

En effektiv måde at afsløre et spoofing-forsøg på er at tilbyde at ringe personen eller organisationen op direkte. Læg på først, og ring derefter tilbage til et nummer, du ved er korrekt. Det sikrer, at du faktisk taler med den rette person og ikke en svindler, der forsøger at narre dig.

Husk, at ingen legitim organisation vil bede dig om dine adgangs- eller pinkoder via telefon eller e-mail.

3. Digital svindel

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

Lottosvindel: Du modtager en e-mail om, at du har vundet i et ukendt lotteri og bedes betale et gebyr. Dette er ofte svindel – har du ikke købt en kupon, har du ikke vundet.

Modtager-svindel: Du modtager en e-mail fra nogen, der ønsker at flytte et stort beløb og har brug for din hjælp. De beder dig betale et lille gebyr med løftet om, at du derefter vil få meget mere tilbage.

Dating-svindel på internettet: Du møder nogen på en digital platform, som hurtigt udtrykker stærke følelser og beder om penge. Giv aldrig penge til nogen, du aldrig har mødt i virkeligheden.

Velgørenhedssvindel: Efter store naturkatastrofer og lignende skaber svindlere falske hjemmesider, hvor du kan blive opfordret til at donere penge. Kontroller altid hjemmesidens ægthed, før du donerer.

Reparationssvindel: Du får et opkald fra nogen, der påstår at kunne hjælpe med din computer. De tager derefter kontrol over din computer med skadelig kode. Vær forsigtig med uopfordrede opkald med påstået teknikhjælp.

Forestil dig: Digital svindel er ganske enkelt moderne versioner af svindlere, der bruger digitale midler til at narre dig.

Gode råd:

Hvis du mistænker svindel, skal du rapportere det til de lokale myndigheder og advare dine venner og familie for at forhindre, at de også bliver narret.



4. Sikker handel på nettet

Når du handler på internettet, skal du sikre dig, at hjemmesiden er sikker (adressen bør begynde med "https"). Tjek også, at hjemmesiden har gode anmeldelser og vurderinger. Spørg gerne venner og bekendte, om de kender til hjemmesiden, du vil handle fra.

Forestil dig: Tænk på sikker digital handel som at handle i en velrenommeret butik i stedet for på en tvivlsom markedsplads.

Gode råd:

Vær forsigtig med at dele dit kortnummer og andre personlige oplysninger på hjemmesider, der virker useriøse. Brug altid sikre, afprøvede betalingsmetoder.

En enkel måde at se, om en hjemmeside er sikker på, er at tjekke, om webadressen begynder med "https".



Spørgsmål til dig
og dine venner

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?



Mere om sikre adgangskoder

Saker-81!losen

Niklas74

Hvilken af de to adgangskoder er stærkest?

1. Opret stærke adgangskoder

Opret adgangskoder, der er mindst 12 tegn lange og indeholder en blanding af bogstaver, tal og specialtegn. Undgå at bruge åbenlyse ord eller sætninger som dit navn, det år du er født og lignende.

2. Brug en 'password manager'

En 'password manager' er et program, der opretter, gemmer og administrerer dine adgangskoder til forskellige websites og apps. Tænk på det som et digitalt pengeskab, hvor dine adgangskoder er sikkert opbevaret bag én vigtig adgangskode – den eneste, du skal huske. 'Password manageren' hjælper også med at få stærke og unikke adgangskoder til hver konto, hvilket væsentligt mindsker risikoen for at andre får adgang til dine konti. I en 'password manager' er dine adgangskoder krypteret for maksimal sikkerhed. Populære eksempler er NordPass, 1Password og Bitwarden. Du får dem nemmest ved at hente dem fra de respektive hjemmesider.

3. Opdater adgangskoder regelmæssigt

Ved at opdatere dine adgangskoder regelmæssigt mindsker du risikoen for, at nogen får uautoriseret adgang til dine konti. For bedst sikkerhed anbefales det, at du ændrer dine adgangskoder hver tredje til sjette måned. Desuden er det vigtigt, at du ikke genbruger gamle adgangskoder. Sikkerhed bør altid være en prioritet, og med disse enkle trin kan du holde dine digitale døre låst og sikre.

4. Brug af biometrisk sikkerhed

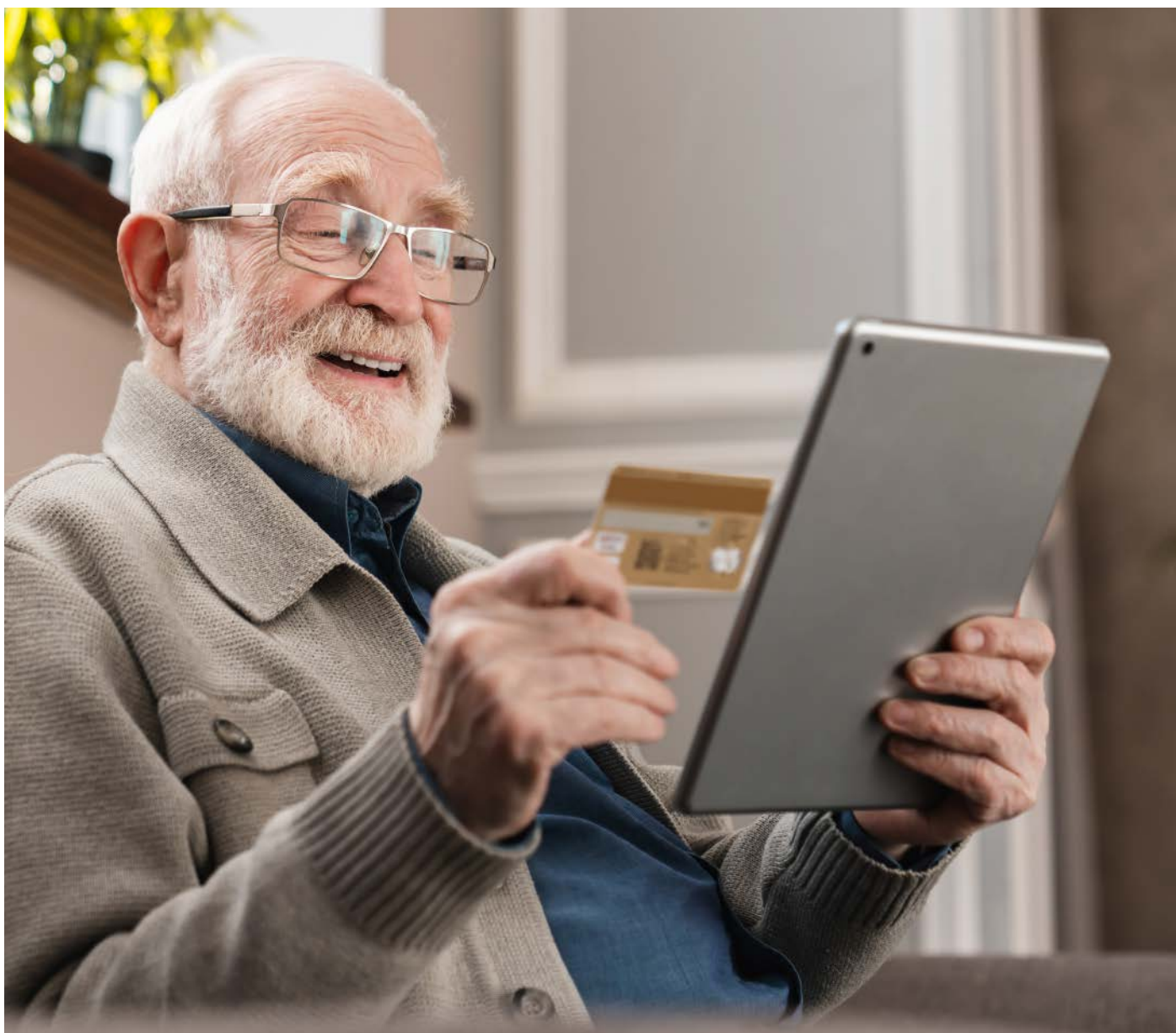
Biometrisk sikkerhed handler om at bruge dine unikke kendetegn – såsom dit fingeraftryk eller dit ansigt – til at bekræfte din identitet. Mange moderne enheder tilbyder den funktion. Tænk på biometrisk sikkerhed som en personlig nøgle, der kun fungerer for dig, hvilket gør det både nemt og sikkert at beskytte dine oplysninger.



Det anbefales, at du ændrer dine adgangskoder hver tredje til sjette måned.

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 navigerer på internettet, efterlader vi spor – det er vores "digitale fodaftryk" og kan inkludere information, som vi bevidst deler; opslag på sociale medier, data der indsamles af de hjemmesider, vi besøger, vores placering eller søgehistorik. Det er vigtigt at være opmærksom på, hvilken type information vi deler på digitale platforme, og at håndtere vores digitale fodaftryk på en sikker og ansvarlig måde.

Husk altid at være opmærksom og tage de nødvendige forholdsregler for at beskytte dig selv på digitale platforme. Det er vigtigt at holde dig opdateret i henhold til de seneste sikkerhedsråd og være proaktiv i at beskytte dine personlige oplysninger.

Men når du deler, interagerer og lærer på digitale platforme, så gør det med glæde og nysgerrighed. Internettet er en platform, hvor du kan opdage, skabe og holde forbindelsen på måder, der var utænkelige for kun få årtier siden. Så brug mulighederne, og lad din digitale rejse give dig store oplevelser og nye opdagelser.



Spørgsmål til dig
og dine venner

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?

