



Hvad er Cybersvindel?

Temadag Distrikt 4 – 16. januar 2024

Hvad er svindel?

- Svindlere, er personer, der forsøger at narre et offer til at oplyse personlige oplysninger eller overføre penge. Svindel kan opstå gennem forskellige kanaler, herunder telefonopkald, e-mails, SMS'er besøg af ukendte personer, onlineplatforme og falske annoncer.
- Andre svindeltyper:
 - Ved **kærlighedssvindel** kontakter en svindler en person online og starter en samtale med det formål at indlede et kærlighedsforhold. Kærlighedssvindlere lader ofte til at være reelle personer (ved brug af manipulerede eller stjalne billeder), som er både følsomme og meget omsorgsfulde.
 - Ved **investeringssvindel** får man løfte om lukrative investeringer med lav risiko i aktier, obligationer, kryptovalutaer eller andet. Svindlerne kontakter typisk deres offer via falske kampagner, telefonopkald, e-mail, sms eller de sociale medier.

Hvilke svindelmetoder ser vi typisk?



Falske telefonopkald

Smæk røret på, hvis samtalen føles utryg eller virker forhastet



Falske e-mails og SMS'er

Klik aldrig på et link eller en fil, som du ikke har bedt om

Andre typiske svindeltyper



Kærlighedssvindel

Vær opmærksom på pengeanmodninger – også mindre beløb. Send aldrig penge, kortoplysninger, kontooplysninger eller kopier af personlige dokumenter.



Investeringsvindel

Hvis du vil begynde at investere, bør du tale med dit netværk, venner og bekendte, så du kan opsøge den rette rådgivning.

Du vil typisk få at vide, at svindleren vil...

- ! Hjælpe dig med at **stoppe noget igangværende svindel** på din konto eller dit kort
- ! Hjælpe med at **erstatte/returnere penge som du har tabt** ved en anden svindelsag, mod et mindre gebyr.
- ! Fortælle at du har **vundet penge eller anden præmie**
- ! Hjælpe med **teknisk support** eller at din **computer eller telefon har fået en virus** som de kan hjælpe dig med at løse
- ! Hjælpe dig ved at få dig til at **downloade en software eller app, (som kan styre din skærm)** for at afhjælpe en et angreb på din enhed
- ! Udgive sig for at være et familie medlem (oftest søn/datter) i økonomisk krise, i forsøget på at franarre dig penge.

Hvordan forebygger vi sammen mere svindel?

1 Din bank, politiet eller anden betroet myndighed vil **aldrig** bede dig dele MitID oplysninger og kodeord, ej heller overføre penge til andre konti, samt anmode om kontrol over din computer eller mobilenhed.

2 Åbn **aldrig** links eller filer i en SMS eller e-mail, du ikke har bedt om. Din bank, det offentlige eller politiet vil aldrig sende SMS'er eller e-mails indeholdende links.

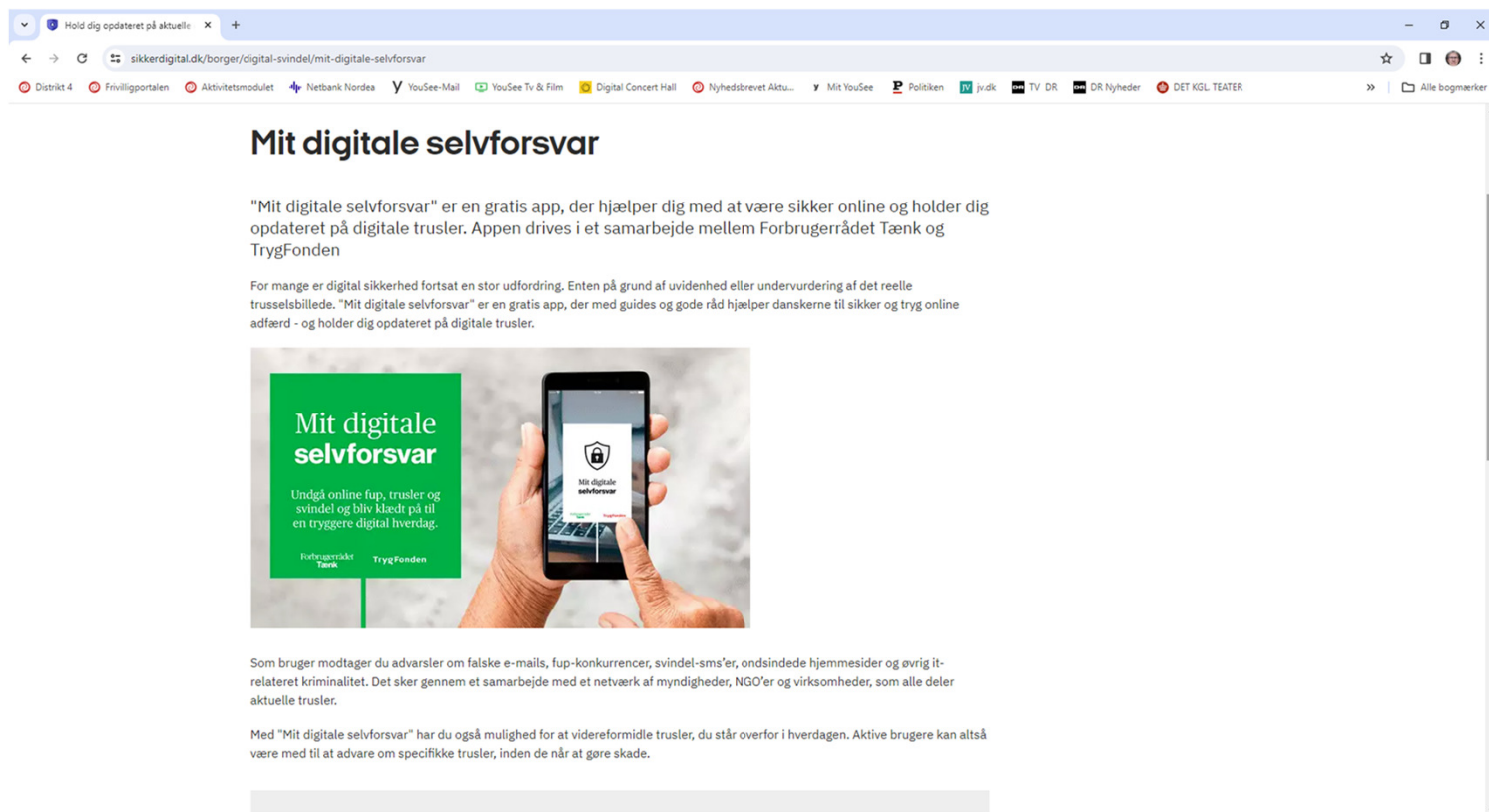
3 Læs **altid** teksten i MitID app en ekstra gang, inden du bekræfter. Hvis du stadigvæk er i tvivl om ægtheden, så kontakt afsender af beskeden – **men på den adresse/telefonnummer, du kender i forvejen!!**

Kontakt dit netværk
om dine digitale
beslutninger.

Tag dig altid god
tid og foretag
aldrig
forhastede
beslutninger.

**Lyt til din
mavefornemmelse.**
Lyder det for godt til at
være sandt?
Så er det det for det
meste også.

App'en - også når du vil hjælpe andre!



Hold dig opdateret på aktuelle x +

sikkerdigital.dk/borger/digital-svindel/mit-digitale-selvforvar

District 4 Frivilligportalen Aktivitetsmodulet Netbank Nordea YouSee-Mail YouSee Tv & Film Digital Concert Hall Nyhedsbrevet Aktu... Mit YouSee Politiken Jv.dk TV DR DR Nyheder DET KGL TEATER Alle bogmærker

Mit digitale selvforsvar


"Mit digitale selvforsvar" er en gratis app, der hjælper dig med at være sikker online og holder dig opdateret på digitale trusler. Appen drives i et samarbejde mellem Forbrugerrådet Tænk og TrygFonden

For mange er digital sikkerhed fortsat en stor udfordring. Enten på grund af uvidenhed eller undervurdering af det reelle trusselsbillede. "Mit digitale selvforsvar" er en gratis app, der med guides og gode råd hjælper danskerne til sikker og tryk online adfærd - og holder dig opdateret på digitale trusler.

Mit digitale selvforsvar

Undgå online fup, trusler og svindel og bliv klædt på til en trygkere digital hverdag.

Forbrugerrådet Tænk TrygFonden



Som bruger modtager du advarset om falske e-mails, fup-konkurrencer, svindel-sms'er, ondsindede hjemmesider og øvrig it-relateret kriminalitet. Det sker gennem et samarbejde med et netværk af myndigheder, NGO'er og virksomheder, som alle deler aktuelle trusler.

Med "Mit digitale selvforsvar" har du også mulighed for at viderefordre trusler, du står overfor i hverdagen. Aktive brugere kan altså være med til at advare om specifikke trusler, inden de når at gøre skade.

https://sikkerdigital.dk/

The screenshot shows the homepage of sikkerdigital.dk. At the top, there is a navigation bar with the logo 'sikker digital' and a search bar labeled 'Indtast søgeord'. Below the navigation bar, there are three main categories: 'Borger', 'Virksomhed', and 'Myndighed'. The main content area features a section titled 'GODE RÅD TIL BEDRE SIKKERHED' with a list of links: 'Hvordan spotter du svindel', '5 sikre råd til din digitale hverdag', 'Dit tekniske setup', 'Når du shopper på nettet', 'Når du er på sociale medier', 'Sådan bliver familien digital sikker', and 'Bliv klogere på digital svindel'. A dark button with white text says 'Få hjælp, hvis skaden er sket'. Below this is a large image of a crowd of people. To the right of the image, the heading 'Din guide til en sikker digital hverdag' is displayed, followed by a short paragraph: 'På sikkerdigital.dk har Digitaliseringsstyrelsen samlet vigtig viden om informationssikkerhed. Du finder råd og vejledning, hvad enten du er borger, virksomhed eller myndighed.' At the bottom, there are three buttons labeled 'Borger', 'Virksomhed', and 'Myndighed'.

KOM SIKKERT VIDERE

Er dit CPR-nummer faldet i de forkerte hænder?

I denne guide får du hjælp til, hvad du bør gøre, hvis du har været udsat for identitetstyveri eller forsøg herpå. Guiden er til dig, der har fået kompromitteret dit CPR-nummer. Guiden hjælper dig med, hvordan du sikrer dit CPR-nummer og din identitet mod misbrug.

[Gå til guiden](#)



NY CYBERHOTLINE

Ring til Cyberhotline for digital sikkerhed

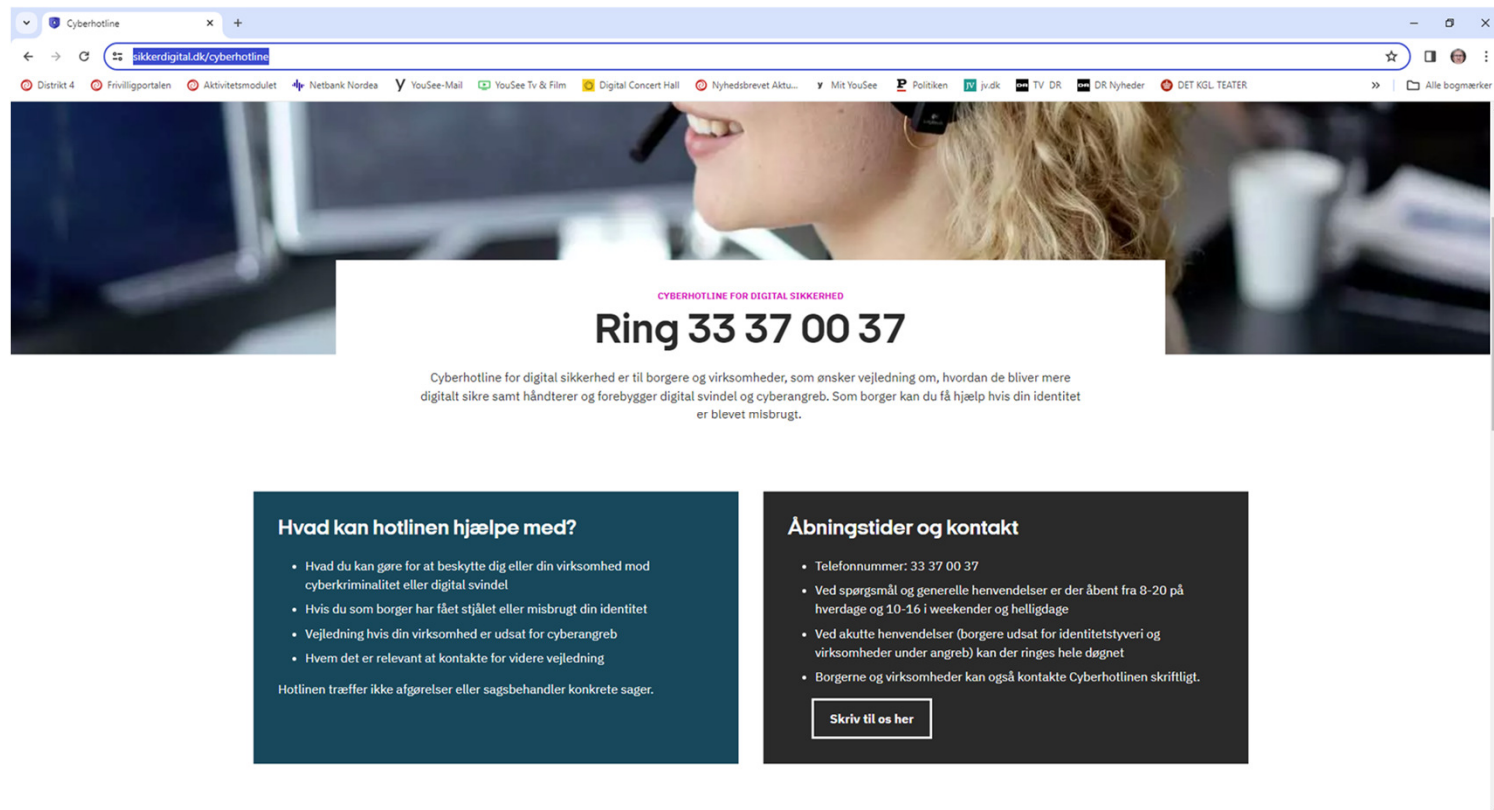
Det kan være svært at vide, hvordan man beskytter sig mod cybertrusler, og hvad man gør, hvis uheldet er ude. Her kan Cyberhotline og digital sikkerhed hjælpe borgere og virksomheder, hvis de er udsat for eller har brug for vejledning til at beskytte sig mod it

[Gå til Cyberhotline](#)

Følg guiden på en computer eller tablet for bedste visning.

På mobilen fungerer guiden bedst i landscape-visning.

https://sikkerdigital.dk/cyberhotline



The screenshot shows a web browser window with the URL sikkerdigital.dk/cyberhotline. The page features a background image of a smiling woman wearing a headset. A white text box in the center contains the following information:

CYBERHOTLINE FOR DIGITAL SIKKERHED
Ring 33 37 00 37

Cyberhotline for digital sikkerhed er til borgere og virksomheder, som ønsker vejledning om, hvordan de bliver mere digitalt sikre samt håndterer og forebygger digital svindel og cyberangreb. Som borger kan du få hjælp hvis din identitet er blevet misbrugt.

Below this, there are two dark blue boxes with white text:

Hvad kan hotlinen hjælpe med?

- Hvad du kan gøre for at beskytte dig eller din virksomhed mod cyberkriminalitet eller digital svindel
- Hvis du som borger har fået stjålet eller misbrugt din identitet
- Vejledning hvis din virksomhed er udsat for cyberangreb
- Hvem det er relevant at kontakte for videre vejledning

Hotlinen træffer ikke afgørelser eller sagsbehandler konkrete sager.

Åbningstider og kontakt

- Telefonnummer: 33 37 00 37
- Ved spørgsmål og generelle henvendelser er der åbent fra 8-20 på hverdage og 10-16 i weekender og helligdage
- Ved akutte henvendelser (borgere udsat for identitetstyveri og virksomheder under angreb) kan der ringes hele døgnet
- Borgerne og virksomheder kan også kontakte Cyberhotlinen skriftligt.

[Skriv til os her](#)

Flere gode råd til din digitale sikkerhed



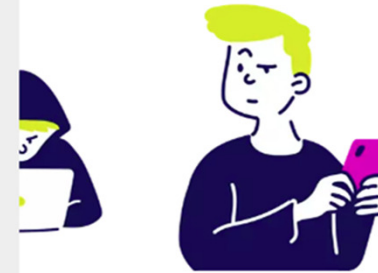
› Sådan spotter du: Falske mails

Du kan - via mail eller sms - blive bedt om at udlevere personlige oplysninger. Her er, hvad du skal være opmærksom på.



› Beskyt dine personlige oplysninger

Du beskytter dine personlige oplysninger bedst, hvis du undgår at dele dem. Her er nogle gode råd.



› Sådan spotter du: Falske beskeder

Du kan - via mail eller sms - blive bedt om at udlevere personlige oplysninger. Her er, hvad du skal være opmærksom på.



På sikkerdigital.dk har vi samlet vigtig viden om informationssikkerhed til dig som er borger, virksomhed eller myndighed.

Du bliver klogere på digitale trusler, og får konkrete råd og vejledninger til en mere sikker digital adfærd.

FØLG OS

- Sikkerdigital
- Sikkerdigital
- Digitaliseringsstyrelsen

SAMARBEJDSPARTNERE



<https://sikkerdigital.dk/cyberhotline/guides-ved-identitetstyveri>

Guides ved identitetstyveri

sikkerdigital.dk/cyberhotline/guides-ved-identitetstyveri

District 4 Frivilligportalen Aktivitetsmodulet Netbank Nordea YouSee-Mail YouSee Tv & Film Digital Concert Hall Nyhedsbrevet Aktu... Mit YouSee Politiken Jv.dk TV DR DR Nyheder DET KGL TEATER Alle bogmærker

GODT I GANG!

Sådan bruger du vores guides

- Du kan bruge guiden på flere måder: Du kan følge den fra start til slut, men du kan også klikke dig frem til de emner, som er vigtigst for dig.
- Følg guiden på en computer eller tablet for bedste visning. På mobilen fungerer guiden bedst i landscape-visning.

Hvis dit CPR-nummer er blevet kompromitteret, så følg nedenstående guide, der giver dig et trinvis overblik over de handlinger, du skal foretage dig for at komme sikkert videre.

Kom sikkert videre:


Er dit CPR-nummer faldet i de forkerte hænder?

I denne guide får du hjælp til, hvad du bør gøre, når du har været udsat for identitetstyveri eller forsøg herpå. Guiden er til dig, der har fået kompromitteret dit CPR-nummer.

Guiden hjælper dig med, hvordan du sikrer dit CPR-nummer og din identitet mod misbrug.

Hvis dit MitID er blevet kompromitteret, så se i stedet guiden for sikring af MitID.

Klik dig gennem siderne med pilene ▶



Er dit CPR-nummer blevet 1 / 15

Reuse

<https://sikkerdigital.dk/cyberhotline/guides-ved-identitetstyveri>

Guides ved identitetstyveri

sikkerdigital.dk/cyberhotline/guides-ved-identitetstyveri

Distrikt 4 Frivilligportalen Aktivitetsmodulet Netbank Nordea YouSee-Mail YouSee Tv & Film Digital Concert Hall Nyhedsbrevet Aktu... Mit YouSee Politiken Jv.dk TV DR DR Nyheder DET KGL TEATER

Alle bogmærker

Hvis dit MitID er blevet kompromitteret, så følg nedenstående guide, der giver dig et trinvis overblik over de handlinger, du skal foretage dig for at komme sikkert videre.

Kom sikkert videre:
Er dit MitID blevet forsøgt svindlet?

I denne guide får du hjælp til, hvad du bør gøre, når du har været udsat for identitetstyveri eller forsøg herpå. Guiden er til dig, der har fået kompromitteret dine MitID-oplysninger.




Guiden hjælper dig med, hvordan du sikrer dit MitID og din identitet mod misbrug.

Klik dig gennem siderne med pilene ▶

Er dit MitID blevet kompromitteret? 1 / 18 ▶

Reuse

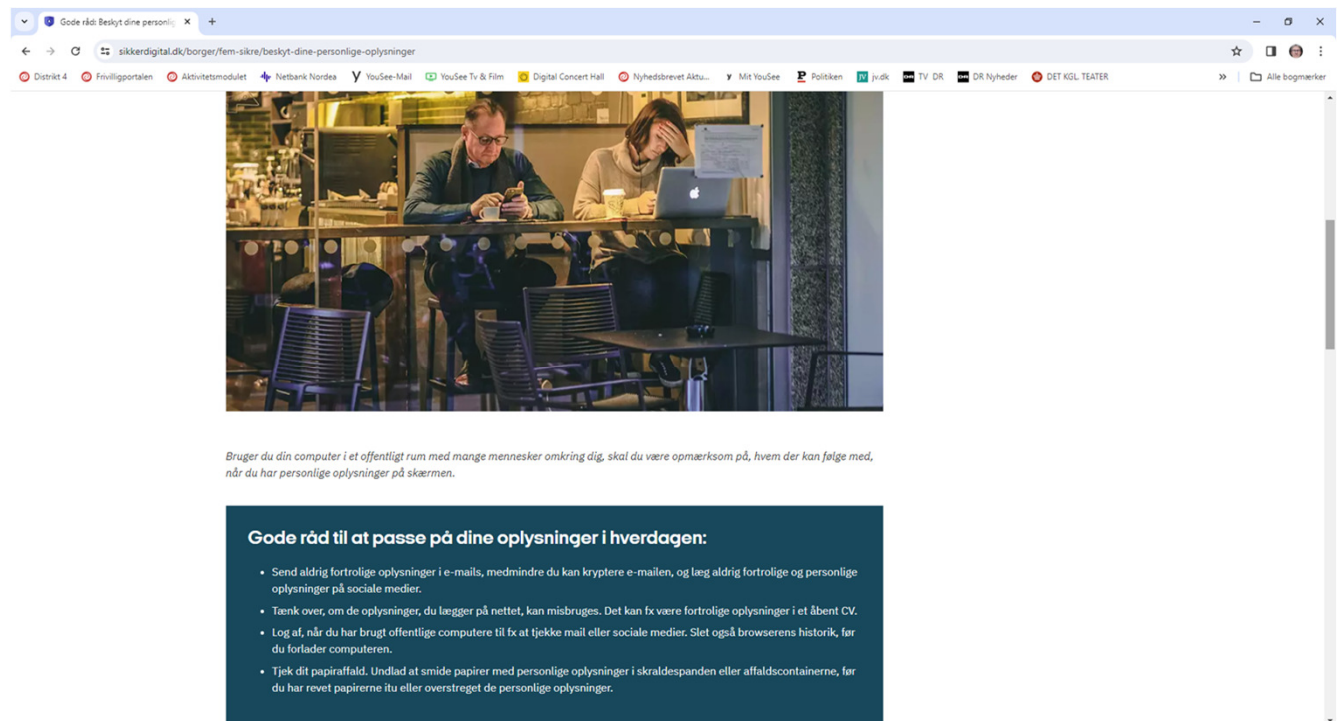
Flere gode råd til din digitale sikkerhed



Video: Spot falske beskeder (mail og SMS)

The screenshot shows a web browser window with the URL sikkerdigital.dk/borger/spot-svindel/laadan-spotter-du-falske-mails. The page title is "Hold øje med, hvad du godkender". Below the title, there is a short paragraph: "Tjek altid, hvad du bliver bedt om, og vær opmærksom på, hvad du godkender i for eksempel MitID-appen og bekræftelses-sms'er." To the right of this text is a dark box with the text "57 pct." in large yellow font, followed by "af danskerne har været udsat for phishing-forsøg over mail, besked eller opkald. Kilde: Analyse 'Danskerne informationsikkerhed 2022'." Below this is a video player. The video player has a dark background with a woman in a white shirt. On the left side of the video, there is a list of five points: "1. Kig på afsenderadressen", "2. Har du en relation til afsenderen?", "3. Pas på mistænkelige links", "4. Send ikke personlige oplysninger", and "5. Tjek for sprog- eller stavefejl". On the right side of the video, there is a logo for "postnord-mail@jogascozinhar.co" and a graphic of a hand pointing to a screen. At the bottom of the video, there is a caption: "Så er det tegn på svindel. To: Har du en relation til afsenderen?". Below the video player, there is a small caption: "Se videoen, der forklarer, hvordan du spotter falske mails og sms'ere."


Pas på dine
oplysninger!



Gode råd: Beslyt dine personlige oplysninger

sikkerdigital.dk/borger/fem-sikre/beslyt-dine-personlige-oplysninger

Distrakt 4 Frivilligportalen Aktivitetsmodul Netbank Nordea YouSee-Mail YouSee Tv & Film Digital Concert Hall Nyhedsbrevet Aktu... Mit YouSee Politiken jvdk TV DR DR Nyheder DET KGL. TEATER Alle bogmærker



Bruger du din computer i et offentligt rum med mange mennesker omkring dig, skal du være opmærksom på, hvem der kan følge med, når du har personlige oplysninger på skærmen.

Gode råd til at passe på dine oplysninger i hverdagen:

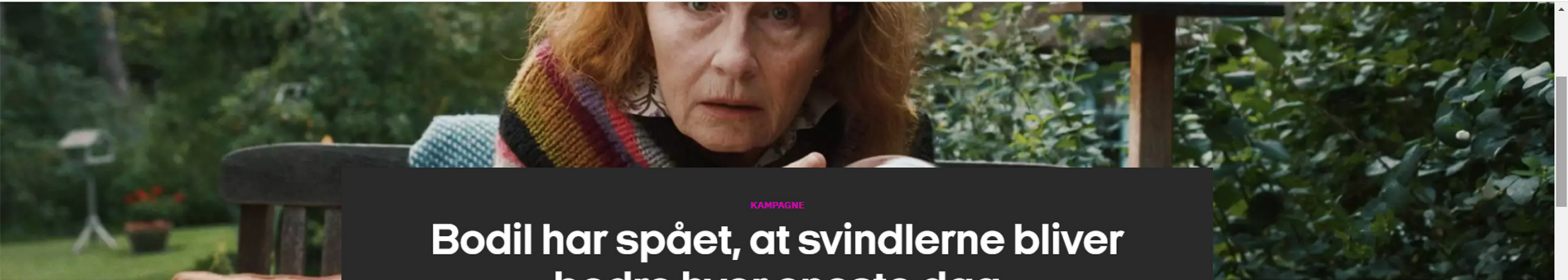
- Send aldrig fortrolige oplysninger i e-mails, medmindre du kan kryptere e-mailen, og læg aldrig fortrolige og personlige oplysninger på sociale medier.
- Tænk over, om de oplysninger, du lægger på nettet, kan misbruges. Det kan fx være fortrolige oplysninger i et åbent CV.
- Log af, når du har brugt offentlige computere til fx at tjekke mail eller sociale medier. Slet også browserens historik, før du forlader computeren.
- Tjek dit papiraffald. Undlad at smide papirer med personlige oplysninger i skraldespanden eller affaldscontainerne, før du har revet papirerne itu eller overstreget de personlige oplysninger.



Test

Svindel-sms'er, phishing mails og phishing-sider. Digitale tricktyve har mange metoder til at svindle og stjæle. **TESTEN** og se, om du hopper i fælderne.

Start test



KAMPAGNE

Bodil har spået, at svindlerne bliver bedre hver eneste dag

Banker og offentlige myndigheder vil ikke uopfordret bede dig om at overføre penge eller om dine personlige oplysninger på mail, SMS eller opkald

BODIL SPÅR OM FREMTIDEN

Vær opmærksom på digital svindel

Digitaliseringsstyrelsen lancerer, i samarbejde med Finans Danmark, Politiet, KL og Danske Regioner, en kampagne, der skal hjælpe borgere til bedre at kunne passe på deres personlige oplysninger og undgå identitetstyveri.

Vigtig huskeregel som hovedbudskab

Banker og offentlige myndigheder vil ikke uopfordret bede dig om at overføre penge eller om dine personlige oplysninger over mail, SMS eller opkald.

Sådan lyder kampagnens hovedbudskab. Digitale svindlere udgiver sig ofte for at være fra banken eller en myndighed, når de forsøger at lokke personlige oplysninger ud af borgere. Svindlerne kan virke troværdige og være svære at gennemskue. Derfor er budskabet en god huskeregel, der kan hjælpe borgere med at undgå at få stjålet og misbrugt deres digitale identitet.

Hvis banker og offentlige myndigheder har brug for dine personlige oplysninger, vil de kontakte dig gennem Digital Post eller din netbank og henvise til selvbetjeningsløsninger. De vil altså ikke række ud til dig uopfordret over mail, SMS eller opkald med det formål at bede dig om at overføre penge eller om dine personlige oplysninger.