



Styrelsen for
Samfundssikkerhed



Digital svindel

30. maj 2025

Progr am

- **Introduktion – Hvem er vi?**
- **Hvad er digital svindel og identitetstyveri?**
- **Udviklingen af digital svindel i tal**
- **Hvordan foregår digital svindel?**
Eksempler på:
 - **Opkald**
 - **SMS'er**
 - **Mails**

- **Forebyggende indsatser**
 - **Kreditadvarsel**
 - **Stærke kodeord**
 - **To-trins login**
 - **Sikkerpånettet.dk**
 - **Mit Digitale**

Selvforsvar

Hvis skaden er sket?

- **Cyberhotline for digital sikkerhed**
- **Guides på Sikkerdigital.dk**

- **Spørgsmål og afrunding**





**Styrelsen for
Samfundssikkerhed**



**sikker
digital^{DK}**

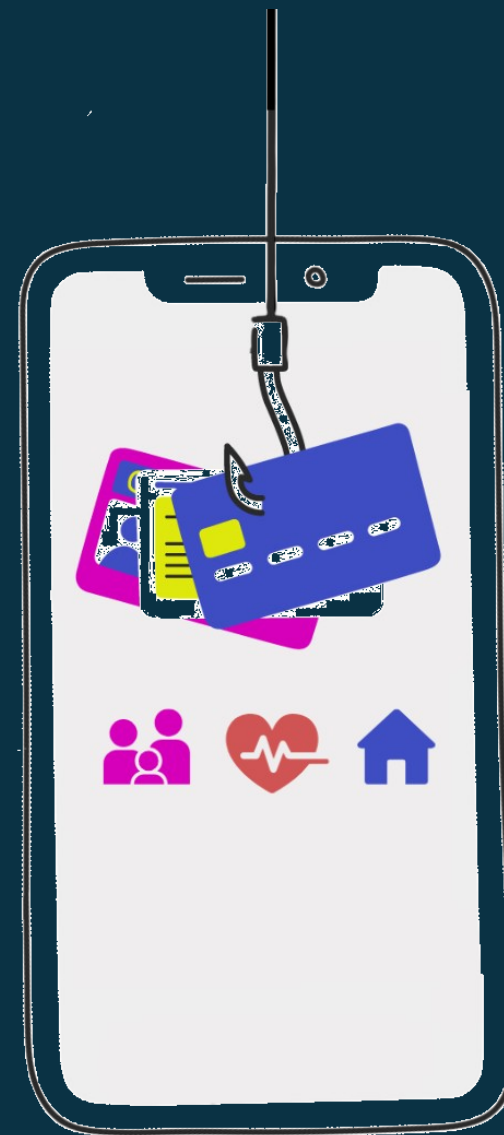
- Sikkerdigital.dk – borger, virksomhed og myndighed
- Forebyggende kommunikationsindsatser – fx kampagner
- Råd og vejledninger, som hjælper borgere, virksomheder og myndigheder med at ruste sig mod cyberangreb og få en mere sikker digital adfærd
- Cyberhotline for digital sikkerhed



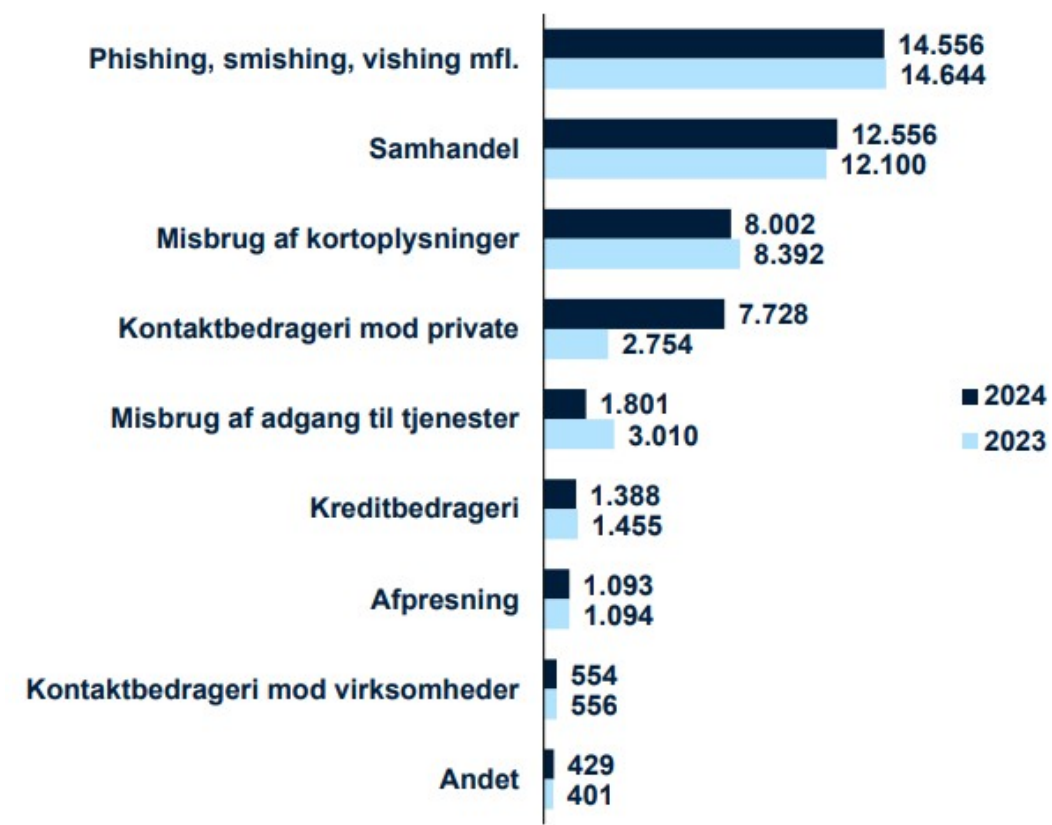
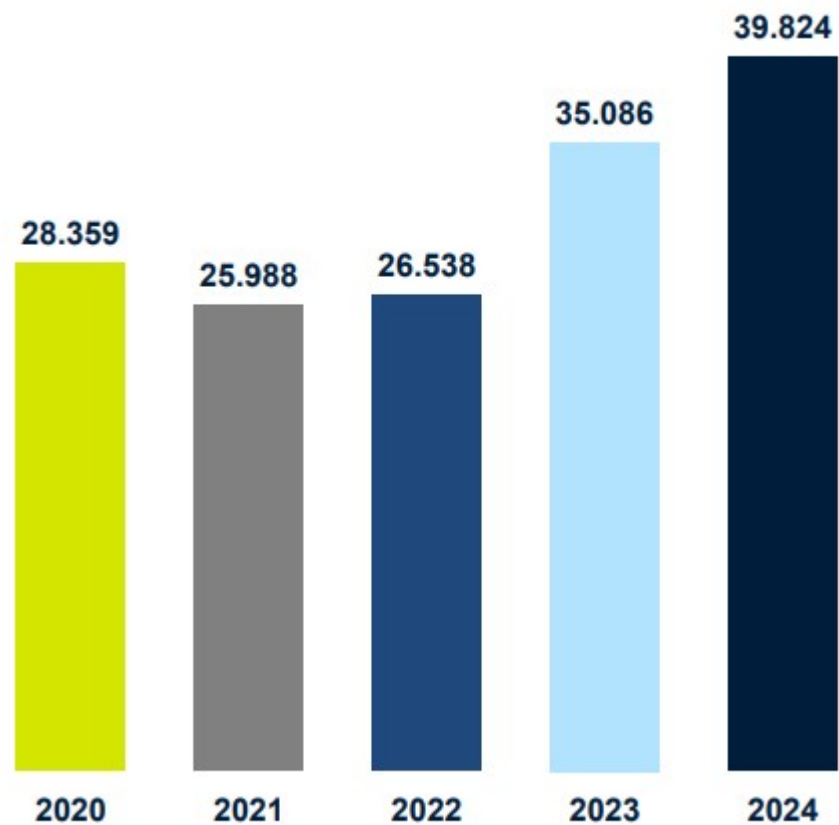
Hvad er digital svindel?

Digital svindel kan mødes på mange måder:

- Identitetstyveri
- Phishing, smishing og vishing
- Online afpresning (ransomware)
- Datingsvindel
- Bekendt i knibe-svindel

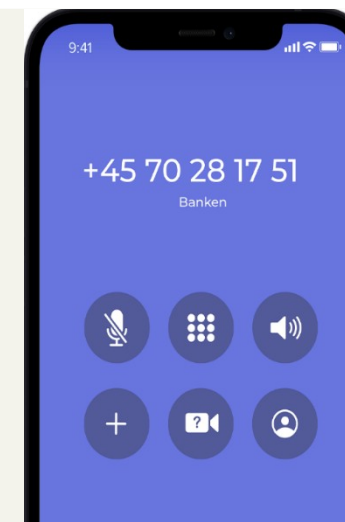
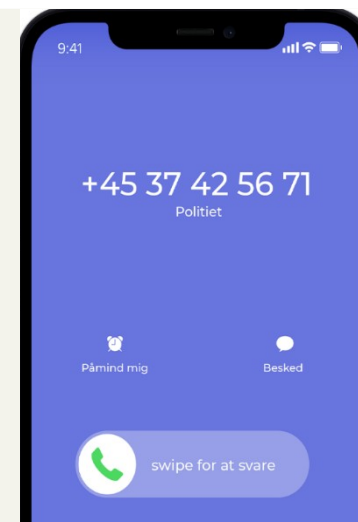


Udviklingen i tal



Falske opkald (vishing)

- Typiske dæksnavne: Politiet, banken, anden myndighed
- Tegn på fupopkald
 - Personlige oplysninger kræves udleveret, eller du skal overføre penge.
 - Du skal handle med det samme.
 - Skjult eller udenlandsk nummer (OBS på spoofing)
- Hvilke oplysninger skal de bruge?
 - MitID-godkendelse (op til flere gange)
 - Skift til engangskode fra QR-kode
 - Skærmoptagelse af QR-kode
 - Overførsel til en "sikkerhedskonto"



57 pct.

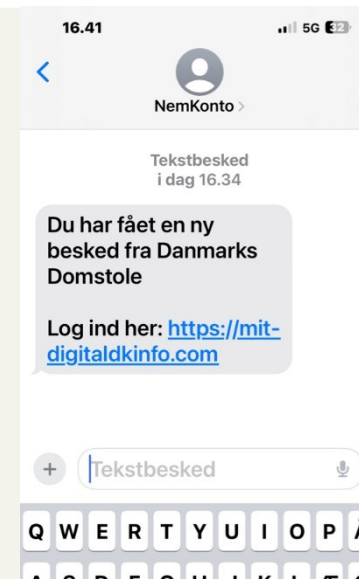
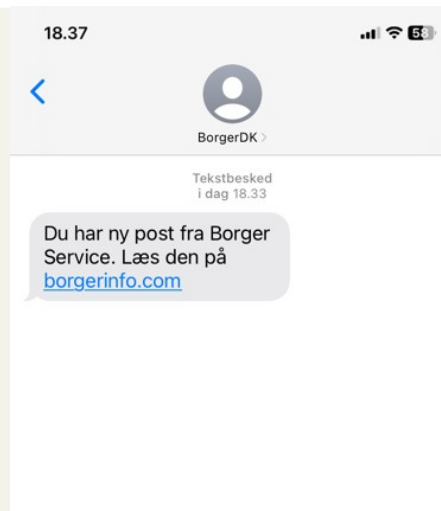
af danskerne har været udsat for svindelforsøg over opkald, mail eller sms, hvor svindleren forsøgte at franske dem personlige oplysninger.

Kilde: Rapport "Danskernes informationssikkerhed 2022"

Falske SMS'er (smishing)

Seks tegn, du skal være opmærksomme på:

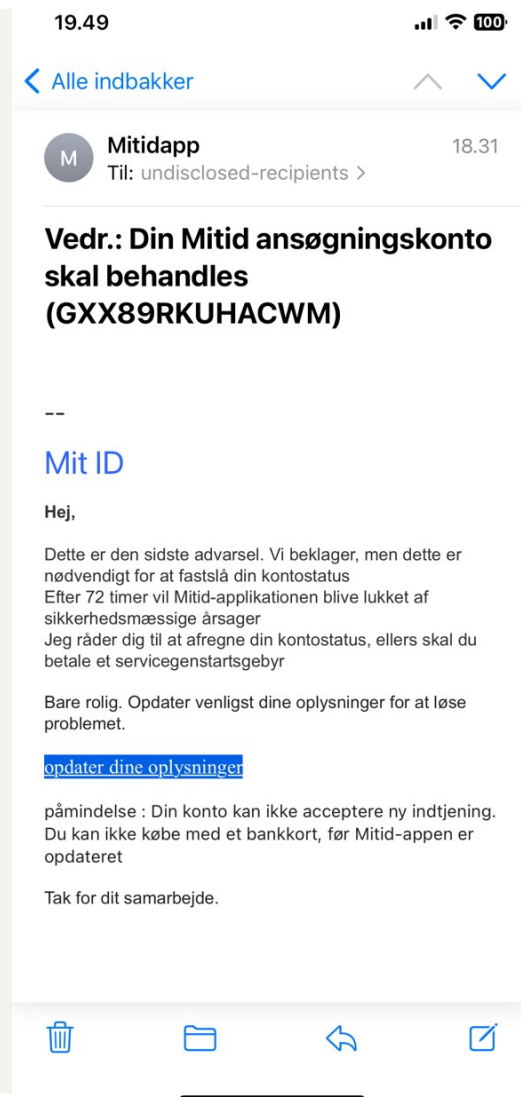
- Kræves der, at du sender dine personlige oplysninger?
- Er der mistænkelige eller direkte links?
- Insisterer afsenderen på, at du skal handle med det samme?
- Er beskeden fra en virksomhed, du ikke har en relation til?
- Vær opmærksom på at svindlere kan ændre visningen af et telefonnummer – spoofing
- Er der sprog- og stavefejl?



Falske e-mails (phishing)

Seks tegn, du skal være opmærksomme på:

- Tjek altid afsenderadresse
- Kræves der, at du sender dine personlige oplysninger?
- Er der mistænkelige eller direkte links?
- Insisterer afsenderen på, at du skal handle med det samme?
- Er beskeden fra en virksomhed, du ikke har en relation til?
- Er der sprog- og stavefejl?



Du har en vigtig besked

borger.dk

Velkommen;

Du skal opdatere dine betalingsoplysninger og identifikationsnummer for at få adgang til vores platform, som giver dig mulighed for at drage fordel af mange tjenester.

Du vil ikke kunne få adgang til platformen, før du opdaterer dine personlige oplysninger.

<https://www.borger.dk/opdatere>

Bemærk: alle konti, der ikke opdateres, vil blive suspenderet ved udgangen af august.

[Borger.dk-2024.](#)

X Luk Du er berettiget til skatterefusion

Skatteforvaltningen <danmarkskatresiluz@telefonica.net>
Til: Skatteforvaltningen

Hej
Du har modtaget en skatterefusionsudbetaling på 6.120,00 kr. fra Skat.dk.

Bekræft venligst anmodningen om skatterefusion.
Pengene går ind på din bankkonto om 1-2 dage.

[>> Klik her og indsend din ansøgning om skatterefusion.](#)

Denne e-mail blev sendt fra en e-mailadresse, der ikke kan modtage e-mails. Besvar venligst ikke denne e-mail.

Hvis du har spørgsmål, så brug vores kontaktformular.

Venlig hilsen,
Skat.dk



Styrelsen for
Samfundssikkerhed

Fem gode råd: Beskyt dig mod falske opkald, mails og SMS'er



1. Udlever aldrig personlige oplysninger, hvis nogen uopfordret beder dig om det over mail eller SMS.



2. Stol ikke på visningen af et opkalds telefonnummer. Svindlere kan ændre visningen af nummeret, de ringer fra, så det er identisk med fx bankens eller politiets.



3. Indtast aldrig oplysninger i forbindelse med links, der fører dig direkte til en loginside. Åbn i stedet en internetside, og søg den officielle hjemmeside frem, fx MitID.dk eller borger.dk



4. Stop op, og lad dig ikke presse, selvom du får indtryk af, at det haster. Svindlere forsøger ofte at give indtryk af, at du skal handle med det samme.



5. Hvis en mail eller SMS kommer fra en virksomhed, du ikke har en relation til, kan det være et tegn på svindel.

Fem konkrete råd til at undgå digital svindel



Opret en kreditadvarsel



Lav et stærkt kodeord



Anvend to-trins-login



Sæt beløbsgrænsen
ned for overførsler



Få udeladt
telefonnummer



Kreditadvarsel

- Forebyg identitetstyveri med en kreditadvarsel
- anbefales i forbindelse med lækket CPR-nummer
- Et signal til banken/virksomheden om at være særlig opmærksom med identitetskontrol, inden der ydes lån eller kredit
- Er dog ikke 100 % sikker, da det ikke er obligatorisk for banker og virksomheder at tjekke op i CPR-registret

borger.dk

 Digital Post

 Mit Overblik

 Menu

Forside / Internet og sikkerhed / Digitale trusler / Kreditadvarsel

› Gode råd til en sikker digital hverdag

› Digital selvbetjening

› Sikker forbruger på nettet

✓ Digitale trusler

- Hvad er identitetstyveri?
- Offer for identitetstyveri
- Spot falske e-mails, beskeder og opkald
- **Kreditadvarsel**

› Privatliv online

Kreditadvarsel

Markering om kreditadvarsel i CPR kan være med til at sikre dig mod identitetsmisbrug



+ Indsæt eller fjern markering om kreditadvarsel i CPR

Start →

+ Hvad er kreditadvarsel?

+ Hvornår skal jeg indsætte kreditadvarsel?

+ Problemer med at få lån eller kredit

+ Digital Fuldmagt: Hvis du skal hjælpe en anden

Bestil tid i borgerservice

Start →

+ Lovgivning

+ Læs også

Skrevet af CPR-Kontoret



Stærke kodeord

Et stærkt kodeord er kendetegnet ved:

- 1. At være minimum **15 tegn**
- 2. At benytte både store og små bogstaver, men gerne en blanding af bogstaver, tal og/eller specialtegn
- 3. At være usædvanligt og svært at gætte for andre.

Gode råd til kodeord:

- Brug ikke samme kodeord flere steder
- Del aldrig kodeord med andre
- Brug en sangtekst/sætning/billede som huskeregel

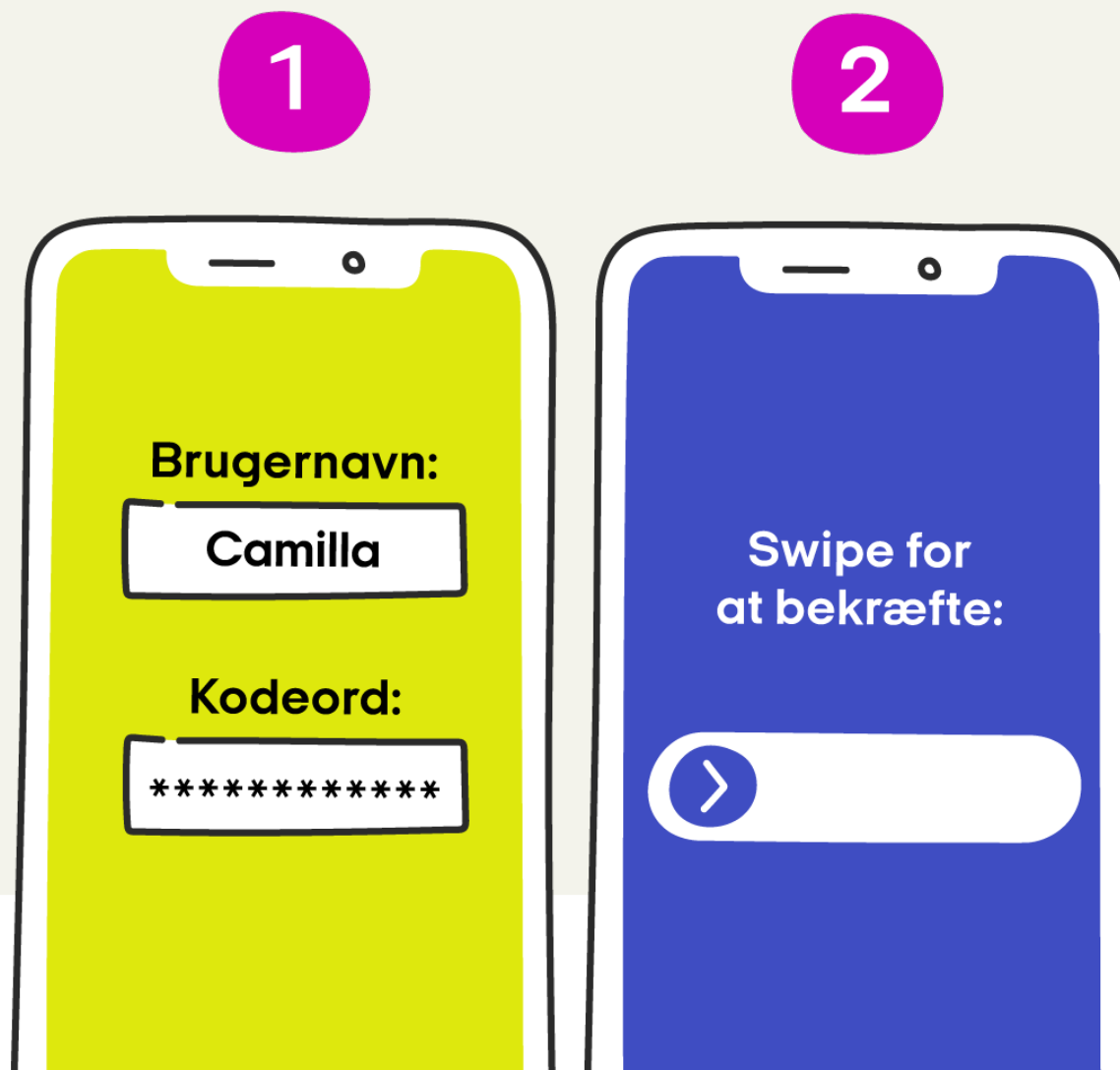
36 pct.

af danskere genbruger ofte eller i
nogen grad kodeord til
forskellige digitale tjenester.
Kilde: Analyse "Danskernes
informationssikkerhed 2022".



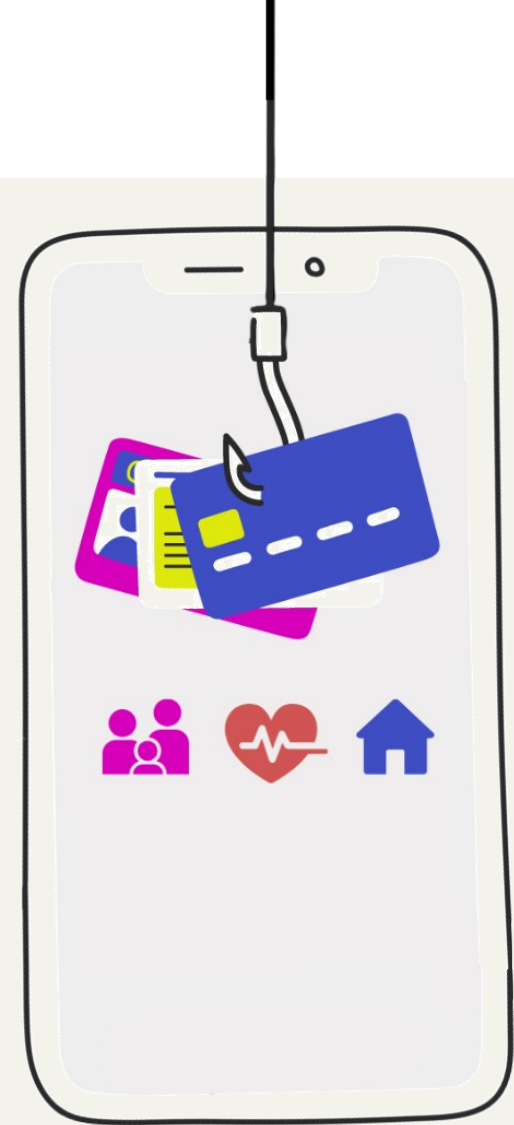
To-trins-login

- To-trins-login betyder, at borgeren skal igennem to trin for at logge ind
- Fx kode på sms udover det normale kodeord eller godkendelse via en app
- MitID er et eksempel på to-trins-login



Sæt beløbsgrænsen ned for overførsler

- Sæt beløbsgrænsen for overførsler ned i din netbank, så svindlere ikke kan overføre et stort beløb, hvis uheldet er ude.
- Beløbet er hos de fleste banker automatisk sat til 50.000 kr.
- Det er forskelligt fra bank til bank, hvor i netbanken det ændres. Kontakt derfor din bank og bed dem om hjælp til at sætte beløbsgrænsen ned



Få udeladt nummer

- Politiet anbefaler, at man kontakter sit teleselskab med henblik på at "få udeladt nummer", således at nummer (navn og adresse) ikke kan fremsøges via fx 118.dk eller krak.dk
- Samtidig anbefales det at gøre ens Facebook-profil (og ens andre sociale medie-profiler) mere private

FOREBYG SVINDEL

Du kan selv gøre meget for at undgå at blive udsat for svindel. Du kan...



... gøre din Facebook-profil mere privat

- Gå ind på din Facebook-profil - gå til 'Indstillinger' og klik på 'Kontrol af privatindstillinger'
- Klik på 'Hvem kan se det, du deler' og klik 'Fortsæt'
- Rediger, hvem der kan se din profiloplysninger
- Vælg 'Kun mig' om dine kontaktoplysninger og venneliste - så kan svindlerne ikke se dine kontaktoplysninger eller dine venne- og familierelationer



... få udeladt nummer

- Kontakt din teleudbyder for at få udeladt nummer (Ring til dem eller gå ind på din profil på deres hjemmeside)
- Udeladt nummer er IKKE det samme som hemmeligt nummer
- Med udeladt nummer kan svindlerne ikke finde dit telefonnummer, og det bliver sværere for dem at ringe til dig
- Alle dine venner kan stadig ringe til dig, og de kan se, at det er dig, der ringer, selvom du har udeladt nummer



Nyttige sider og apps



Styrelsen for
Samfundssikkerhed

 Tjek på nettet.dk

MENU DK

Tjek på nettet.dk:

Tjek om du kan stole på et link.

Indtast det link, du vil tjekke... 

RapportérOm Tjekpånettet.dkDisclaimer

Vi gør alt for at give dig et nøjagtigt resultat, men ingen er perfekte. Brug altid selv din sunde fornuft, hvis du besøger en hjemmeside. Hvis vi har lavet en fejl, vil vi gerne høre fra dig. Oplysningerne i denne tjeneste er til generelle information og kan ikke bruges til eventuelle skader eller andre negative konsekvenser.

For vores fulde disclaimer, [klik her](#).

Vi står bag Tjekpånettet

 Digital

DanskEnglish

ForsideVidensdatabaseOm initiativet

HVOR SÅRBART ER DIT WEBSITE?

Internetkriminalitet er blevet en del af vores hverdag. Beskyt dit website og dine brugere.

Test dit domæne

Vi tester, om dit domæne har en moderne IPv6-adresse, er DNSSEC-signeret, om forbindelsen er sikret med HTTPS-indstillinger og hvilke sikkerhedsindstillinger, der aktiveres i browseren hos besøgende på dit website.

[Klik her for at læse om testen.](#)

Dit domænenavn:

Start test

Test din e-mail

Vi tester, om din e-mailserver har en moderne IPv6-adresse, er DNSSEC-signeret, hvilke antiphishingindstillinger der er aktiveret, og om forbindelsen er sikret med SSL/TLS-indstillinger.

[Klik her for at læse om testen.](#)

Din e-mailadresse:

Start test

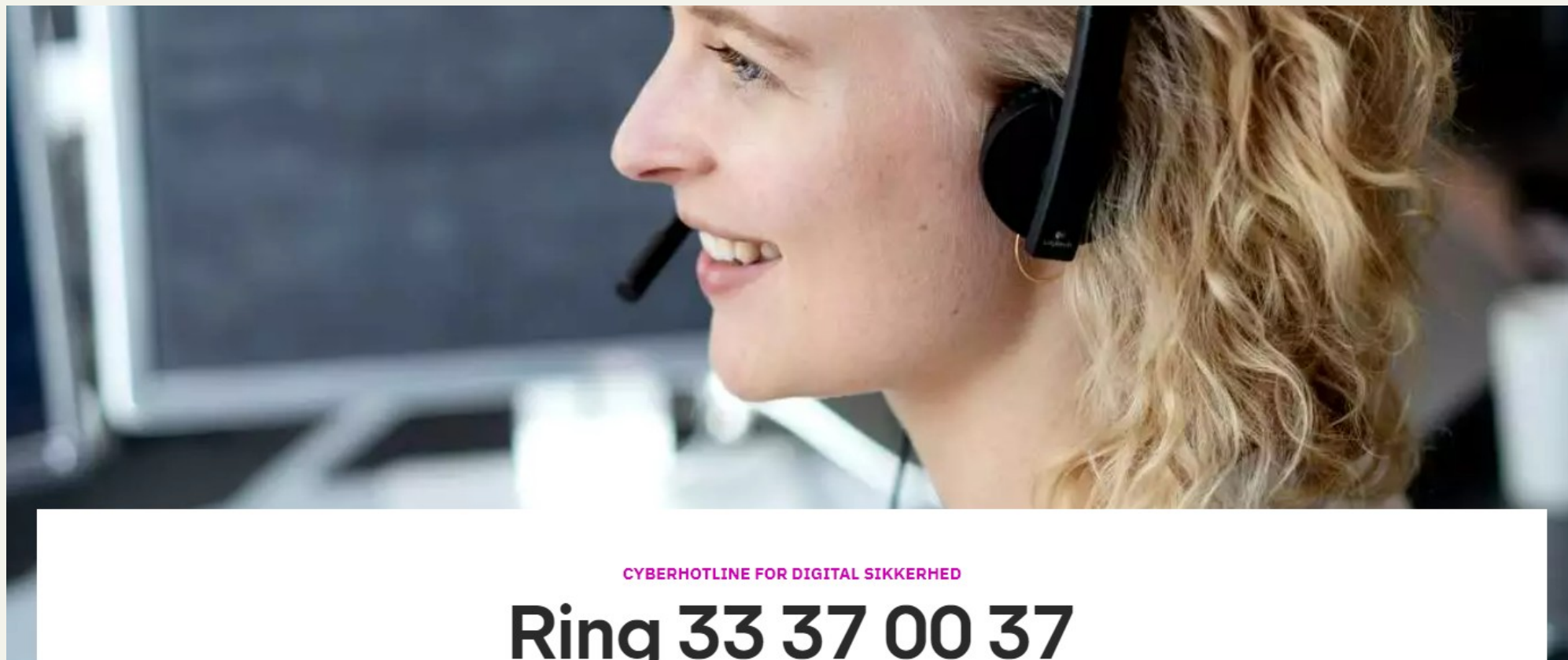
Test din forbindelse

Vi tester, om du kan tilgå internettet med en moderne IPv6-adresse, og om din internetudbyder tilbyder et DNSSEC-signeret domæne.

[Klik her for at læse om testen.](#)

Start test

Hvis skaden er sket – og allerhelst før..



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 angreb.



Styrelsen for
Samfundssikkerhed

Flere forebyggende råd på Sikkerdigital.dk



QUIZZER OG TEST

› Lær, hvordan du spotter falske mails, SMS'er og opkald

Det kan være svært at gennemskue, hvornår der er tale om svindel. Tag quizzen her og bliv klogere på, hvad du skal være særligt opmærksom på for at passe på dine oplysninger.



QUIZZER OG TEST

› Test dig selv: Kan du spotte de digitale fælder?

Kan du spotte fælder og svindel? Tag testen og bliv klogere på de digitale fælder.



QUIZZER OG TEST

› Handler I på nettet?

Prøv en test, tag en challenge og få gode råd om svindel, når I handler på nettet. Her bliver hele familien klogere på handel.

Gode råd til bedre sikkerhed

Find gode råd, vejledninger og værktøjer, som hjælper dig til en mere sikker digital hverdag.

Hvordan spotter du svindel?

Svindel på nettet er udbredt. Heldigvis findes der en række råd, der gør det lettere for dig at spotte svindel.



Bliv klogere på stærke kodeord

Dine kodeord skal beskytte dig mod, at digitale svindlere får adgang til dine mest private oplysninger. Men det gør kodeordene kun, hvis de er stærke.

Her kan du lære, hvad et stærkt kodeord er, hvordan du laver og husker stærke kodeord, og hvordan du passer på dem i hverdagen.

Du kan teste din viden undervejs. Klik dig gennem siderne med pilene. ▶



Styrelsen for
Samfundssikkerhed



Styrelsen for
Samfundssikkerhed



sikker
digital^{DK}

**Spørgsmål og
afrunding**

Tak for i dag



samsik.dk



Styrelsen for Samfundssikkerhed



@samfundssikker