

DEL IKKE DINE PERSONLIGE OPLYSNINGER





DU KAN TRYGT BRUGE DINE PERSONLIGE KODER

Det er trygt at bruge dit NemID eller indtaste dine personlige oplysninger. Skulle du alligevel være så uheldig, at en bedrager prøver at snyde dig, er det godt at være forberedt.

SPOT ET FUP-OPKALD

Et fup-opkald vil typisk prøve at lokke dine personlige oplysninger ud af dig eller få dig til at ringe op til et dyrt udenlandsk nummer.

1. Svindleren prøver at lokke oplysninger ud af dig

Vær på vagt, hvis du bliver ringet op, og den anden person hurtigt begynder at spørge efter personlige oplysninger.

2. Du bliver tilbudt hjælp, du ikke har brug for

Modtager du et opkald fra et it-firma, kan det være en svindler som påstår, at du har brug for teknisk support, fordi din computer, tablet eller smartphone har fået en virus eller lignende. Svindleren kan også hævde at være ansat hos en virksomhed, hvor du er kunde – fx din bank eller teleudbyder. De prøver at overbevise dig om, at der er sket en fejl, og at de har brug for dine oplysninger fx adgang til din netbank for at udbedre den.

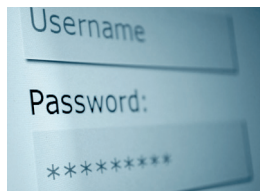
3. Lad dig ikke narre af dansk tale

Vær på vagt, når du kan se, at du modtager et opkald fra et udenlandsk nummer – også selv om personen taler dansk.

4. Ring ikke tilbage

Hvis et ukendt udenlandsk nummer har ringet til dig, så lad være med at ringe tilbage. Det kan være et betalingsnummer med meget høje takster.

**Gem dine koder i
hukommelsen
- ikke på telefonen**



SPOT EN FUP E-MAIL ELLER SMS

1. Vær skeptisk

Banker, virksomheder og offentlige myndigheder som fx SKAT vil aldrig bede dig om personlige oplysninger som kontooplysninger, kodeord og CPR-nummer via sms eller mail.

Del derfor aldrig personlige oplysninger via sms eller mail.

2. Stol ikke på links

Links i falske sms'er eller e-mails har enten til formål at installere virus på din telefon eller at lokke personlige oplysninger ud af dig.

De lokker fx med en præmie eller andet, men lad være med at trykke på linket. Linksene er ofte forkortede, så du ikke kan se, hvad der gemmer sig bagved.

De kan se ud som på billedet her:

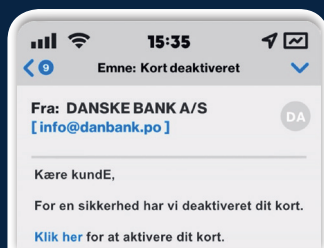
Vil du gerne tjekke om sms'en eller e-mailen er falsk, så kontakt afsenderen på en anden måde end via oplysningerne i beskeden.



3. Tjek afsendernavnet

Du kan tjekke om e-mailadressen eller telefonnummeret stemmer overens med afsender-navnet. Ser mailadressen mærkelig ud eller passer den ikke med afsendernavnet, er der tale om en falsk henvendelse.

Gå ind på virksomhedens officielle hjemmeside og tjek kontaktoplysninger, dog uden at bruge linket i e-mailen.



**VÆR SKEPTISK OVER FOR,
HVEM DU TALER MED
- DU SKAL IKKE STOLE PÅ ALLE**

PAS GODT PÅ DINE PERSONLIGE OPLYSNINGER

- Vær skeptisk, når du, uden du har bedt om det, bliver kontaktet enten via e-mail, SMS eller telefonisk
- Banker, virksomheder og offentlige myndigheder vil aldrig bede dig om at oplyse NemID koder eller andre adgangskoder, som giver adgang til fx din bankkonto
- Download gratis app'en "Mit Digitale Selvforvar", som hjælper dig til en sikker og tryk afdærd på nettet



Har du mistanke om, at dine oplysninger er faldet i de forkerte hænder, skal du:

- Kontakte politiet hurtigst muligt på 114 eller anmeld det på www.politi.dk/anmeld
- Kontakte din bank, hvis du har delt dine bankoplysninger
- Spærre dit NemID nøglekort på www.nemid.nu

Har du mistanke om, at dit CPR-nummer eller NemID er misbrugt, kan du oprette en kreditadvarsel via borger.dk, så andre ikke kan optage lån mv. i dit navn

Det er grænseoverskridende at skulle indrømme over for sig selv, at man er faldet i klørne på en bedrager, men hurtig reaktion efterfølgende kan være med til at mindske omfanget af bedraget.