Nordea

1.
Lad dig ikke overtale til at lave en overførsel – og **udlevér aldrig MitID- eller kortoplysninger** over telefonen.

2.
Læs altid teksten i MitID-appen eller i en SMS, **inden du bekræfter.**

3.
Klik ikke på et link i en SMS eller e-mail, du ikke har bedt om.

4.
Stol på din sunde fornuft. Det gælder især, når du handler med andre private, skriver med fremmede på nettet/datingplatforme eller overvejer et investeringstilbud, der lover høje afkast.

5.
Tal med dine nærmeste om digital svindel, og hold dig opdateret via appen "**Mit digitale selvforsvar**".

Har du mistanke om svindel?
Kontakt os straks på **70 33 33 33**.

Vi svarer døgnet rundt alle årets dage.
Læs mere på nordea.dk/**svindel**

Nordea

Undgå svindel

Hyppigste svindelnumre og vores bedste råd til at undgå dem

Kære kunde

Tak fordi du læser med.

At blive svindlet er en yderst ubehagelig og grænseoverskridende oplevelse, som desværre rammer flere og flere danskere i alle aldre.

De kriminelle finder hele tiden nye, digitale veje. I 2022 lykkedes det dem at slippe afsted med hele 425 mio. kr. (ifølge Finans Danmark).

Med denne lille bog håber vi at hjælpe dig med at spotte og stoppe svindlen, så du eller dine kære ikke bliver de næste ofre.

Venlig hilsen
Alle os i Nordea

I dag går svindlere ikke længere efter at hacke din telefon eller computer, men forsøger i stedet at hacke dig som person.

Svindlerne udgiver sig typisk for at være fra banken eller fra politiet. Det gør de for at manipulere deres ofre til at give dem fortrolige oplysninger eller for at få offeret til at overføre penge.

Dennis Schytt Haahr
Ekspert i svindelforebyggelse
hos Nordea

De 5 hyppigste svindelnumre

Sådan arbejder svindlerne

På de følgende sider får du en gennemgang af de mest udbredte måder, der bliver svindlet på:

- Telefonsvindel
- Falske e-mails og SMS'er
- Køb/salg af brugte varer
- Investeringssvindel
- Kærlighedssvindel

Svindelmetode 1: Telefonsvindel

Telefonsvindel går ud på at manipulere og snyde dig gennem et telefonopkald. Svindleren ringer og udgiver sig ofte for at være fra en autoritet, fx din bank, politiet eller en anden myndighed.

Svindlerne er trænet i at være utroligt overbevisende og komme med gode begrundelser for, hvorfor du skal overføre penge eller udlevere dine personlige oplysninger og godkende ting med dit MitID.

De kan fx finde på at sige, at din konto er ved at blive hacket, og at du derfor skal flytte dine penge hurtigst muligt.

Sådan undgår du telefonsvindel

Lav aldrig en overførsel, fordi nogen forsøger at overtale dig til det. Udlevér aldrig MitID- eller kortoplysninger over telefonen. Er du i tvivl? Så afbryd opkaldet og ring selv op til det nummer, du ved tilhører fx banken eller politiet.

Og husk: Politiet eller din bank vil aldrig ringe og bede dig overføre penge.

Svindelmetode 2: E-mails og SMS'er

Svindlere sender ofte falske e-mails og SMS'er, som ser ud til at komme fra en organisation eller virksomhed, som du kender og stoler på. Det kan fx være en pakkeleverandør eller skattevæsnet.

I beskederne er der et link eller en knap, som de forsøger at lokke dig til at klikke på – typisk ved at sige, at noget skal løses og haster.

Klikker du på linket, bliver du ført videre til en falsk og meget vellignende login-side, der stjæler dine oplysninger.

Sådan undgår du denne type svindel

Klik aldrig på et link i en e-mail eller SMS, du ikke selv har bedt om at modtage.

Og husk: Du bør ikke stole på en virksomhed, der uopfordret beder om følsomme oplysninger via SMS eller e-mail.

NORDEA: Dit brugernavn skal aktiveres, ellers suspenderes din adgang til MitID : https://selvbetjening.nemiddkda.app/

FAKE

Svindelmetode 3:
Køb og salg af brugte varer

Hver dag køber og sælger danskere mobiltelefoner, tøj og meget andet af hinanden. Det sker på loppemarkeder, men det sker også på digitale platforme og hjemmesider.

Når du handler med private, skal du være opmærksom på, at der findes et hav af falske profiler og annoncer, som udnytter vores tiltro til andre mennesker.

Sæt derfor farten ned, når du falder over et godt tilbud. Er et tilbud for godt til at være sandt, er det desværre ofte svindel.

Dine alarmklokker bør ringe, hvis:

- Sælger har kreative undskyldninger for, hvorfor du ikke kan komme forbi og se varen.
- Varen sælges væsentligt billigere end andre steder.
- Sælgers profil ikke er valideret med MitID.
- Sælgers eller købers profil ikke ser troværdig ud.
- Køber sender et "bevis" på en betaling, men du ikke kan se pengene på din konto.

Svindelmetode 4: Investeringssvindel

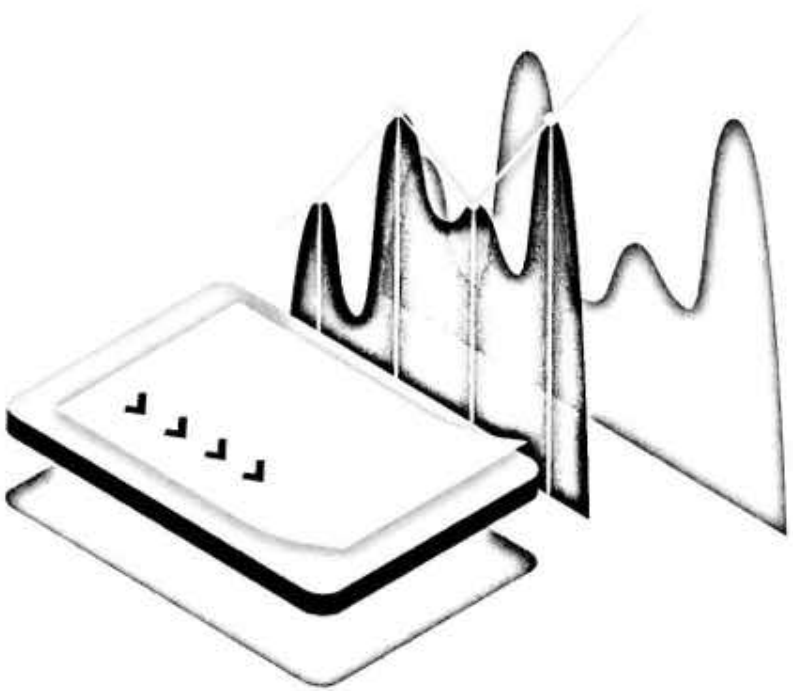
Mange drømmer om at blive rige ved at investere deres penge. Og det udnytter svindlerne. Med falske annoncer på sociale medier lokker svindlere med fantastiske afkast på investeringer. Ofte udnytter de kendte personer, som mod deres vilje bliver ansigt på reklamen.

Skriver du dig op til at høre mere, vil du få en veltrænet svindel-sælger i røret, en såkaldt "investeringsrådgiver". Svindlerens mål er at få dig til at smide flest muligt penge ind i svindelnummeret. Falder du i fælden, får du desværre hverken dine penge igen eller et fantastisk afkast.

Sådan undgår du denne type svindel

Stol på din sunde fornuft og undersøg troværdigheden.

Har du en lille tvivl eller en forkert fornemmelse, er det ofte fordi, der er noget galt.



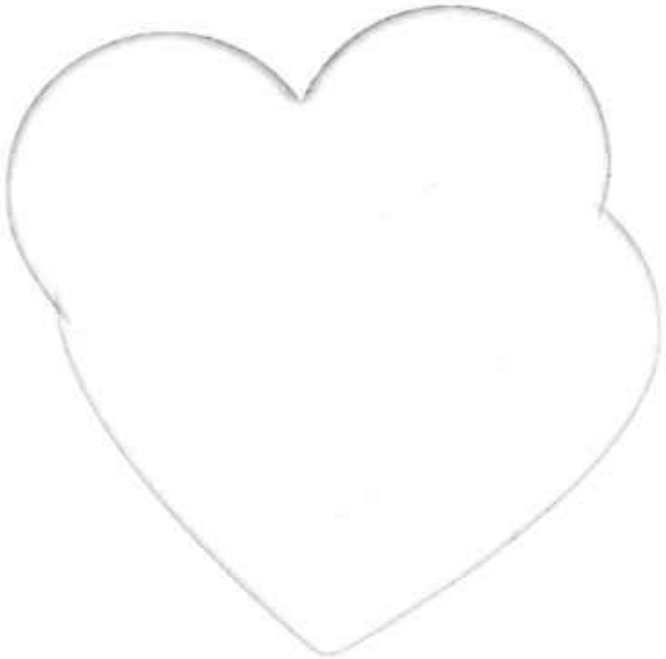
Svindelmetode 5:
Kærlighedssvindel

Kærlighedssvindel begynder typisk på nettet. Det kan være på sociale medier eller en datingside, hvor svindleren ofte udgiver sig for at være en "smuk kvinde" eller en "oberst på opgave i udlandet".

Kontakten udvikler sig hurtigt til også at foregå over telefon- eller videoopkald. Her erklærer svindleren sin kærlighed og begynder at tale om en fælles fremtid. Efter et stykke tid begynder svindleren at bede om penge til eksempelvis rejser eller hospitalsudgifter.

Sådan undgår du denne type svindel

Det kan være en god idé at tale med en, du stoler på, hvis du får en kæreste på nettet. Det kan nemlig være utroligt svært at se advarselstegnene, når man selv er forelsket.



I politiet oplever vi, at det er borgere i alle aldre, der udsættes for it-kriminalitet. Svindlerne fremstår ofte troværdige, og derfor er din kritiske sans det bedste våben mod svindel.

Sig nej, når du bliver bedt om at overføre penge via telefonen, udlevere dine MitID-oplysninger eller klikke på et link i en SMS eller mail. Tal også med din bank om muligheden for at beskytte din konto ved at sætte en beløbsgrænse for pengeoverførsler. Så er du på den sikre side.

Kresten Munksgaard
Sektionsleder hos politiets Nationale enhed for Særlig Kriminalitet

Tak fordi du læste med

Du kan holde dig opdateret om svindel og få vores bedste råd på **nordea.dk/svindel**.

Vi anbefaler også, at du henter en gratis app til din telefon, der hedder "Mit digitale selvforsvar". Det er Forbrugerrådet Tænk og Trygfonden, der står bag appen, og her kan du løbende få advarsler om de svindelnumre, der er i omløb.

Vi råder alle til at tale højt med hinanden om svindel, så vi sammen kan passe godt på os selv og vores kære.

Er du i tvivl?

Du kan altid ringe til os på
70 33 33 33