



Nordea

Idéen om en tryk hverdag

Velkommen til arrangement om svindelforebyggelse

Lasse Karner, Fraud Communication & Awareness Danmark
Oktober, 2025



Dagens agenda

- ⊕ Introduktion
- ⊕ Social manipulation
- ⊕ Svindelrends
- ⊕ Hjælpeværktøjer

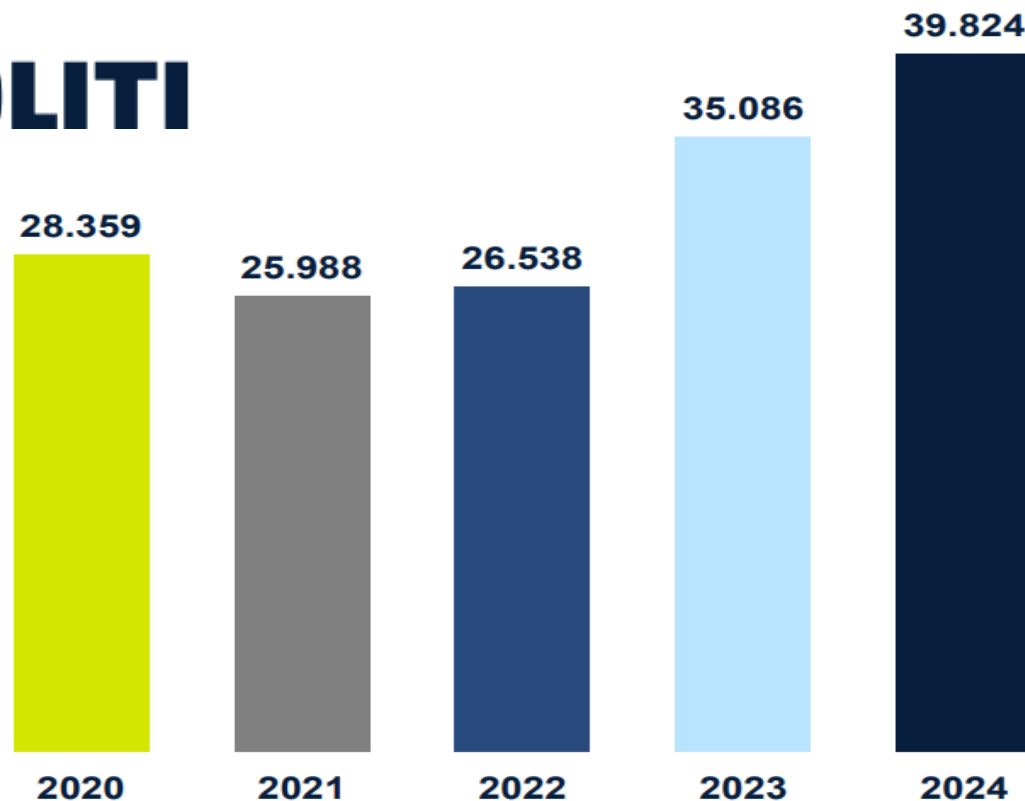
627

Millioner kroner

Det var, hvad de kriminelle svindlede sig til i 2023 ifølge Nationalbanken og Finans Danmark.

Rekordmange politianmeldelser i 2024

POLITI



Samfundet ændrer sig



Nordea

Nordea

Social manipulation

Svindlernes supervåben



Udviklingen af svindel

'Hacking' af mennesket

2010

2025

'Hacking' af teknologien

- Virus
- Malware
- ID theft
- Hacked Facebook profil
- Uautoriseret betalinger



Social Manipulation

- Telefonsvindel
- Falske SMS'er og mails
- Spoofing
- CEO svindel
- Autoriserede betalinger

Nordea

Svindeltyper



De mest brugte svindeltyper

1

Telefonsvindel



2

Falske mails og SMS'er



3

Investeringsvindel



4

Kærlighedssvindel



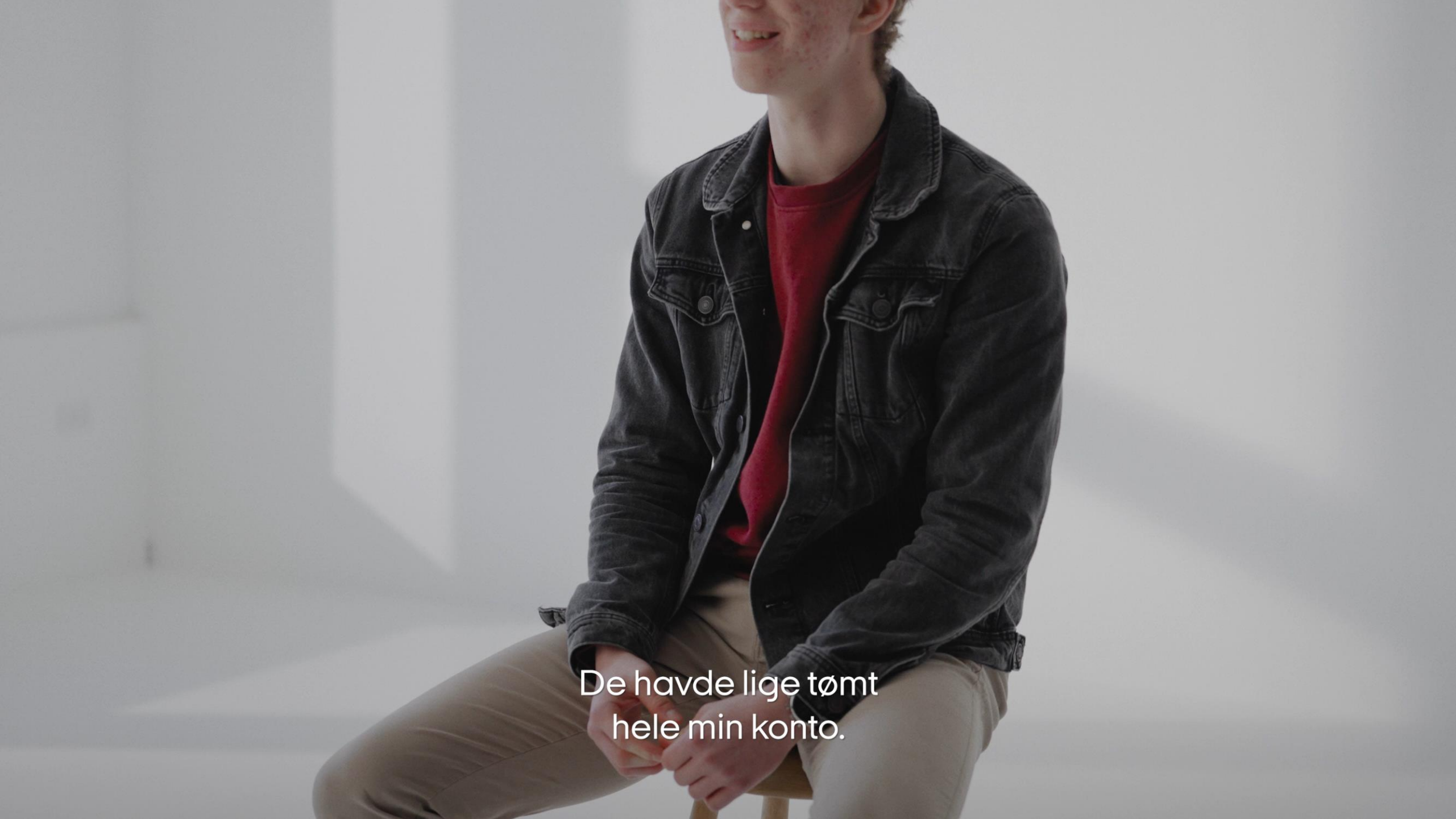
5

Køb på nettet



Telefonsvindel





De havde lige tømt
hele min konto.

Telefonsvindel

- 1 Du modtager et telefonopkald; der er sket noget!
- 2 Det kan ordnes! Du skal bare..
- 3 Svindlerne fisker efter de oplysninger, de har brug for..
- 4 .. eller lokker dig til at flytte penge til en såkaldt "sikkerhedskonto"

Svindlerne er trænet i at **manipulere** dig. De siger mange ting, der får kaldet til at virke troværdigt

Kombination af svindelmetoder gør forsøget mere **realistisk**.

Med "spoofing" får de telefonnummeret til at ligne et troværdigt nummer

Du kan få fjernet dit telefonnummer fra offentlige sider som krak, de gule sider og 118, ved at kontakte dit teleselskab.

Fra telefonsvindel til fysisk fremmøde

Svindel: Der stod en 'nydelig ung mand'

Svindlere og plattenslagere fortsætter deres bedrageri mod ældre

Falsk Nordea-medarbejder på spil

Borgere i Vordingborg er blevet kontaktet af en person, der forsøger at franarre dem deres betalingskort

Politiet advarer: Atter falsk bankmand på spil

Udgav sig for at være Emil fra banken og svindledede ældre for oplysninger

Kunder ringes op af en falsk bankmedarbejder, som melder om alarmerende aktivitet på ens betalingskort

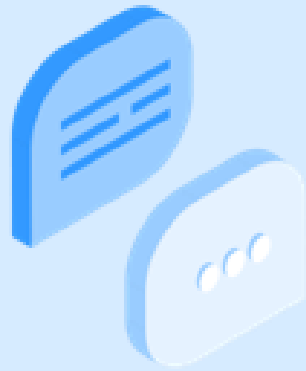
En "medarbejder" vil derfor komme ud på adressen efter kortet hurtigst muligt



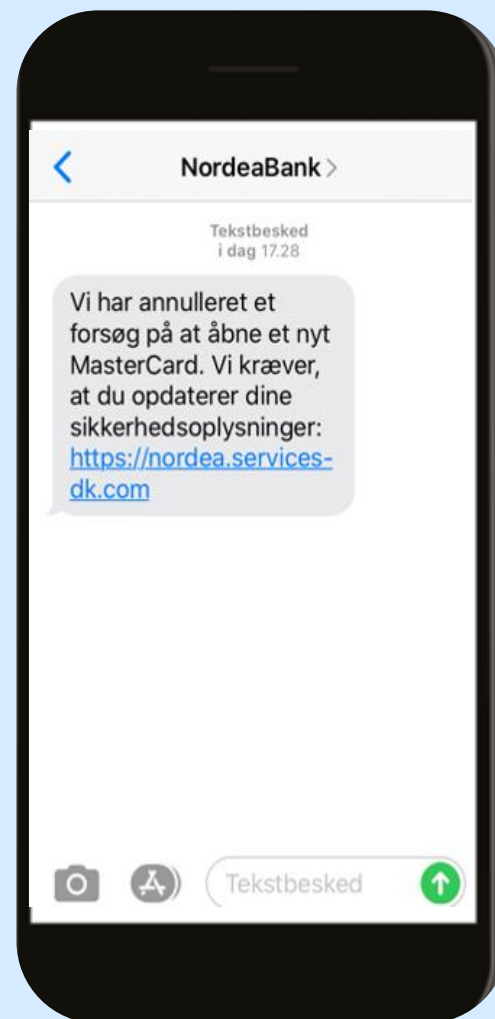
Lav aldrig en overførsel og udlever ikke personlige oplysninger, fordi nogen forsøger at overtale dig til det

Er du i tvivl? Smæk røret på og kontakt selv virksomheden vedkommende påstår at komme

Falske mails og SMS'er



- 1 Beskeden udgiver sig for at være en organisation eller virksomhed, som du kender og stoler på.
- 2 Indeholder altid et link eller en knap, som du skal klikke på
- 3 Beskeden siger ofte, at noget skal løses og det haster
- 4 Når du klikker på linket, kommer du ind på en veldisigneret hjemmeside, hvor du skal indtaste personlige oplysninger



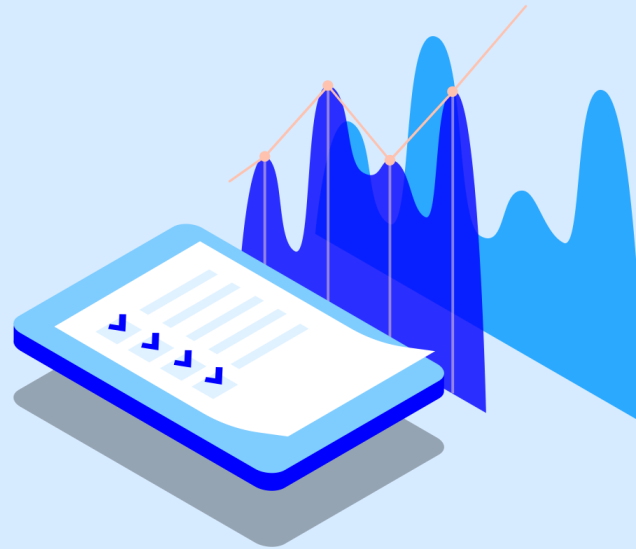
Falske mails og SMS'er



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

*Og læs altid teksten i MitID app og SMS,
inden du bekræfter.*

Investeringsvindel



Investeringsvindel

- Det starter med en annonce – typisk på sociale medier
- Du bliver lovet høje afkast og rigdom
- Investeringssiden ser professionel og troværdig ud og kan indeholde overbevisende videoer
- Du får din egen 'investeringsrådgiver' og adgang til en platform hvor du kan se dine investeringer i realtid
- Når du vil have pengene ud, finder ud af det, at det er svindel



Du kan blive kontaktet efterfølgende af et 'advokatfirma'

”

*Stol på din sunde skepsis
og undersøg troværdigheden.*

Kærlighedssvind





Kærlighedssvindel



- Kontakten opstår via sociale medier eller datingplatforme
- Relationen udvikler sig hurtigt og foregår på skrift, men også via telefon- eller videoopkald
- Romancen kan være flere måneder/år
- Når forelsket er fuldt indtruffet beder svindleren om økonomisk hjælp
- Svindleren vil også forsøge at isolere dig fra din omgangskreds

”

*Tal med en du stoler på,
inden du overfører penge til en,
du ikke har mødt*

Køb på internettet



Køb på nettet – pas på falske butikker

Dine alarmklokker
bør ringe hvis

Vær opmærksom på webshops og
lokkende annoncer på sociale medier.
Du risikerer:

- At købe noget, men aldrig modtage varen
- At modtage en kopivare eller et produkt langt under standard
- At dine kort- og kontooplysninger bliver misbrugt fx til at købe andre varer for eller bliver solgt til andre svindlere

Webadressen ser underlig ud

Der er ingen 'om os' side på hjemmesiden

Varen sælges væsentligt billigere end andre steder

Der er priser i skæve og underlige beløb

Beløb eller butiksnavn er ændret, når du skal godkende

Opsummering og råd



**Autoriserede
betalinger**

**Kunstig
Intelligens**

**Svindlerne
handler og deler
med hinanden**

**Men... også
positive
tendenser**

5 gode råd til at undgå digital svindel

1

Lav aldrig en overførsel, fordi nogen forsøger at overtale dig til det – og udlever aldrig MitID eller kortoplysninger til en i telefonen.

2

Læs altid teksten i MitID app og 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 skepsis og undersøg troværdigheden.

5

Tal med dine nærmeste om digital svindel og hold dig opdateret.



Her finder du hjælp

- [Mit Digitale Selvforvar app](#)
- [Nordea.dk](#) & [Facebook](#)
- [Sikkerdigital.dk](#)
- Brug banken

Hvis skaden er sket

- Kontakt banken hurtigst muligt
- Meld svindlen til politiet

Tak!