SVINDELVAGT · DANMARK · UGENTLIG UDGAVE · 24. november 2026

Er det svindel?

En letlæst guide til den svindel, der rammer danskere lige nu — på telefonen, i indbakken og på de sociale medier.

Udgivet af: **lennartandersen.xyz**

Hvis du lige har klikket, betalt eller godkendt i MitID

1. **Ring til din bank** på nummeret bag på dit kort, og bed dem stoppe betalingen — minutter tæller. Spær kortet, hvis du har givet kortoplysninger.
2. **Spær dit MitID** via Cyberhotline (33 37 00 37) eller mitid.dk, hvis du har godkendt noget, du ikke selv startede. Skift adgangskoder fra en anden enhed.
3. **Anmeld det til politiet** på politi.dk eller 114 — også selvom du ikke har mistet noget. Banken skal ofte bruge anmeldelsen.

Hvem du skal kontakte i Danmark

ANMELD DET

Politiet

114

Politiets servicenummer i hele landet. Mange former for svindel kan anmeldes digitalt på politi.dk. Akut fare: 112.

FÅ HJÆLP

Cyberhotline for digital sikkerhed

33 37 00 37

Råd ved svindel og identitetstyveri. Hverdage 8–20, weekend og helligdage 10–16. Uden for åbningstid: spærring af MitID.

RING NU

Spær dit kort — Nets

44 89 29 29

Dankort og Visa/Dankort, døgnet rundt. Visa og Mastercard: 44 89 27 50. Eller spær direkte i din mobilbank.

BESKYT DIN IDENTITET

Kreditadvarsel i CPR

borger.dk

Er dit CPR-nummer eller pas lækket, kan du selv sætte en kreditadvarsel, så långivere skal tjekke din identitet ekstra.

Seks regler, der beskytter dig online

- **En uventet SMS med et link er svindel, til det modsatte er bevist.** PostNord, Skattestyrelsen, MitID, din bank — gå selv ind i deres app eller på deres side, aldrig via linket.
- **Godkend kun i MitID, når du selv logger ind.** Læs teksten i appen. Beder nogen dig godkende, er det svindel.
- **Garanteret afkast er løgn.** Kendte danskere, der »anbefaler« krypto eller »AI-trading«, er falske reklamer — ofte deepfake-videoer. Tjek firmaet hos Finanstilsynet.
- **Slå automatiske opdateringer til** på telefon, computer og browser. De fleste hackerangreb udnytter fejl, der allerede er rettet.
- **Brug totrinsbekræftelse og en adgangskodeadministrator** (eller adgangsnøgler) til mail og sociale medier — din mail kan nulstille alle dine andre konti.
- **Gavekort, krypto og overførsler til fremmede er svindlerbetaling.** Ingen rigtig virksomhed, myndighed eller arbejdsgiver kræver dem.

Opdater nu — hackere udnytter disse fejl denne måned

Sårbarheder i almindelige forbrugerprodukter, som hackere aktivt udnytter, tilføjet inden for de sidste 30 dage til den amerikanske myndighed CISA's liste over kendte udnyttede sårbarheder (cisa.gov/kev). Data pr. 24. november 2026.

Hvis du bruger	Sådan opdaterer du	Markeret
Microsoft Office CVE-2026-124194	Åbn et Office-program → Filer → Konto → Opdateringsindstillinger → Opdater nu.	2026-11-10
Google Chrome CVE-2026-125350	Menu (⋮) → Hjælp → Om Google Chrome, og klik derefter på Genstart.	2026-11-10
iPhone, iPad og Mac CVE-2024-27834	Indstillinger → Generelt → Softwareopdatering (Mac: Systemindstillinger → Generelt → Softwareopdatering).	2026-11-04

Den svindel, danskere mister penge til

Falsk pakke-SMS

En SMS siger, at en pakke fra PostNord, GLS eller DAO venter, men at der mangler porto eller told. Linket fører til en perfekt kopi af den rigtige side, der beder om dine kortoplysninger.

> **Afsløringen:** Et lille beløb, en kort frist og et link. Tjek selv i fragtfirmaets app med dit pakkenummer.

Investerings- og kryptosvindel

En reklame viser en kendt dansker — ofte en deepfake-video — der roser en platform. En venlig »rådgiver« viser dig stigende gevinster på en skærm og beder dig sætte flere penge ind.

> **Afsløringen:** Du kan ikke hæve pengene uden først at betale »gebyr« eller »skat«. Tjek altid firmaet på finanstilsynet.dk.

Online »opgave-job«

En rekrutterer skriver på WhatsApp eller Telegram: tjen penge på at bedømme produkter eller like videoer. Små udbetalinger kommer først — så skal du indbetale for at låse større opgaver op.

> **Afsløringen:** Et job, hvor du skal betale, typisk i krypto. Et rigtigt job betaler dig.

DBA- og Marketplace-svindel

Som sælger får du et link til at »modtage betalingen« eller »bestille fragt«. Som køber finder du et godt tilbud, men sælgeren er »bortrejst« og vil have penge på forhånd.

> **Afsløringen:** Et link, hvor du skal indtaste kortoplysninger for at modtage penge. Man skal aldrig give kortdata for at få penge.

Kontoovertagelse og falsk support

En SMS eller et opkald fra »banken«, »MitID« eller dit teleselskab siger, at din konto er kompromitteret, og beder dig godkende, oplyse en kode eller flytte penge.

> **Afsløringen:** De beder om en kode eller en MitID-godkendelse, du lige har fået. Det er dem, der logger ind som dig.

Sextortion og afpresning

En, du har mødt online — eller en fremmed, der påstår at have hacket dit kamera — truer med at dele intime billeder, hvis du ikke betaler. Unge drenge er særligt udsatte.

> **Afsløringen:** Pres for at betale med det samme. Betal ikke, stop med at svare, gem beskederne og anmeld til politiet — unge kan også få hjælp hos Red Barnets SletDet-rådgivning.

Nummeret på din skærm kan være falsk

Svindlere kan vise et hvilket som helst nummer — selv det rigtige nummer til din bank, politiet eller Skattestyrelsen. Det kaldes **spoofing**. Beder et opkald om penge, koder, MitID-godkendelse eller personlige oplysninger, så **læg på og ring selv op** på nummeret bag på dit kort eller fra den officielle hjemmeside.

Bloker svindelopkald på din egen telefon

- **Android:** Telefon-appen → Indstillinger → *Opkalds-id og spam* → slå spamfiltrering til (Samsung: *Opkalds-id og spambeskyttelse*). Pixel har også *Opkaldsscreening*.
- **iPhone:** Indstillinger → Telefon (eller Apps → Telefon) → *Gør ukendte opkald lydløse*: numre uden for dine kontakter går til telefonsvareren.
- **Enkelte numre:** bloker dem fra seneste opkald — det hjælper lidt, men svindlerne skifter nummer hele tiden.
- **Dit teleselskab:** mange tilbyder gratis filtrering af spamopkald — spørg dem.

Dette er generel information og ikke juridisk, økonomisk eller politimæssig rådgivning. Telefonnumrene er tjekket på organisationernes egne hjemmesider (senest tjekket november 2026), men numre og procedurer ændrer sig — bekræft altid et nummer på den officielle

hjemmeside, før du stoler på det. Ring altid 112 i en nødsituation. Live-afsnittet er dannet automatisk den 24. november 2026 ud fra offentlige kilder; det viser kun fejl i almindelige forbrugerprodukter.