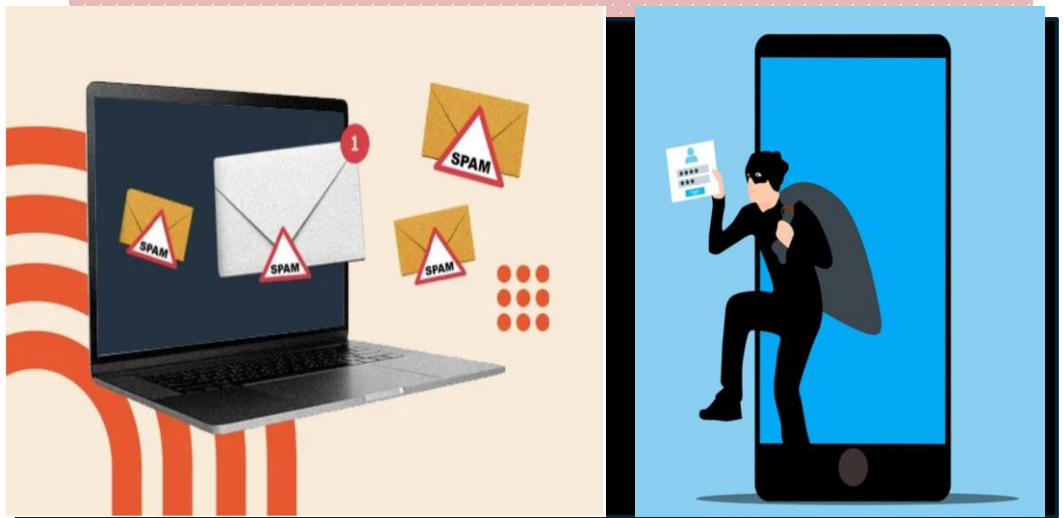
Seniornett ULLENSAKER

Informasjonssikkerhet for seniorer

Dagens mest utbredte nett-bedragerier

Svein R. Aarvik



De kriminelle spiller på følelser og er ikke ute etter deg som person dvs.

Sosial manipulasjon

- **Frykt**
- **Fristelser (penger / kjærlighet)**
- **Tillit**
- **Tidspress**
- **Hva andre gjør**
- **Autoriteter**
- **Teknisk informasjon**

Seniornett ULLENSAKER

Sosial manipulasjon

Epost
«trond.mo@gmail.com»

Mobilnummer
«900 56 046»

Personnummer
29.06.55 40634

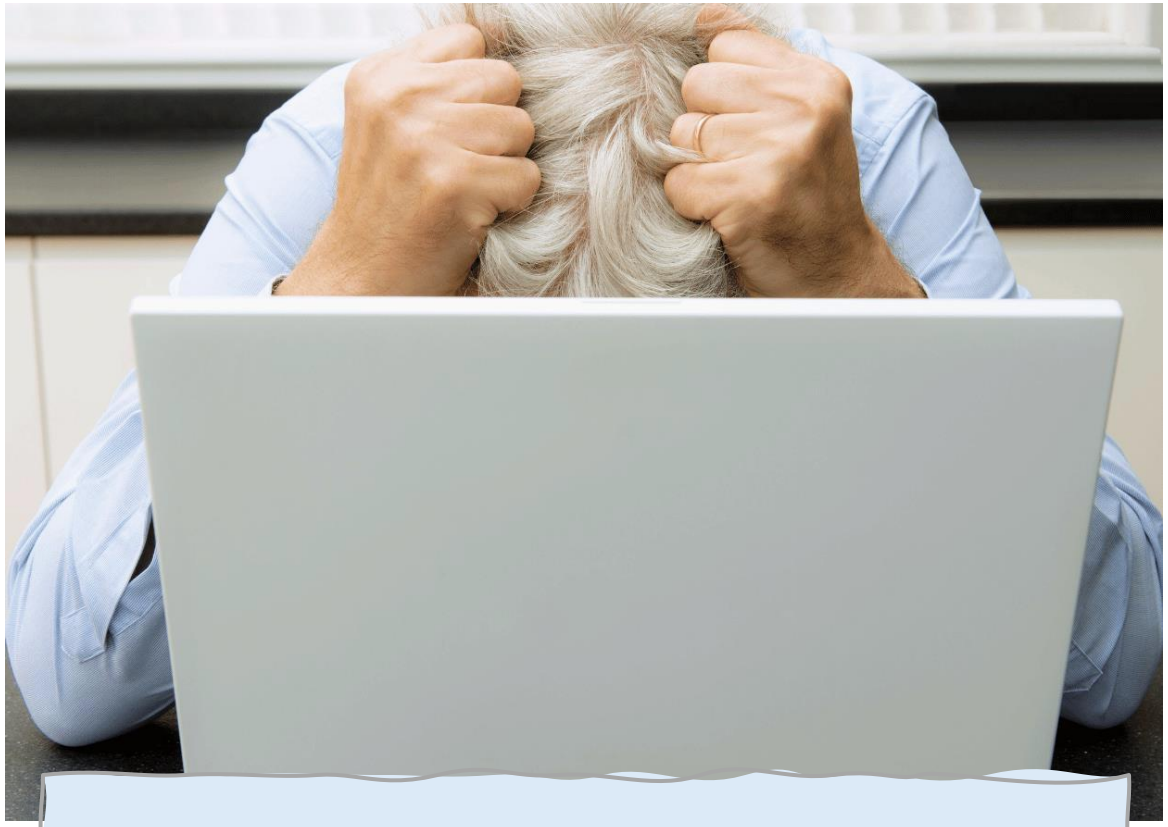
Mobiltelefon (sikkerhetskode)
«2345»

BankID
«Hurra002»

Passord på nettside
«Kjellemann55»

Passord på facebook
«Facebook55»

Sikkerhetskode fra mobil
«3003»



Seniornett ULLENSAKER

Slik lurer de deg med falske Google-meldinger

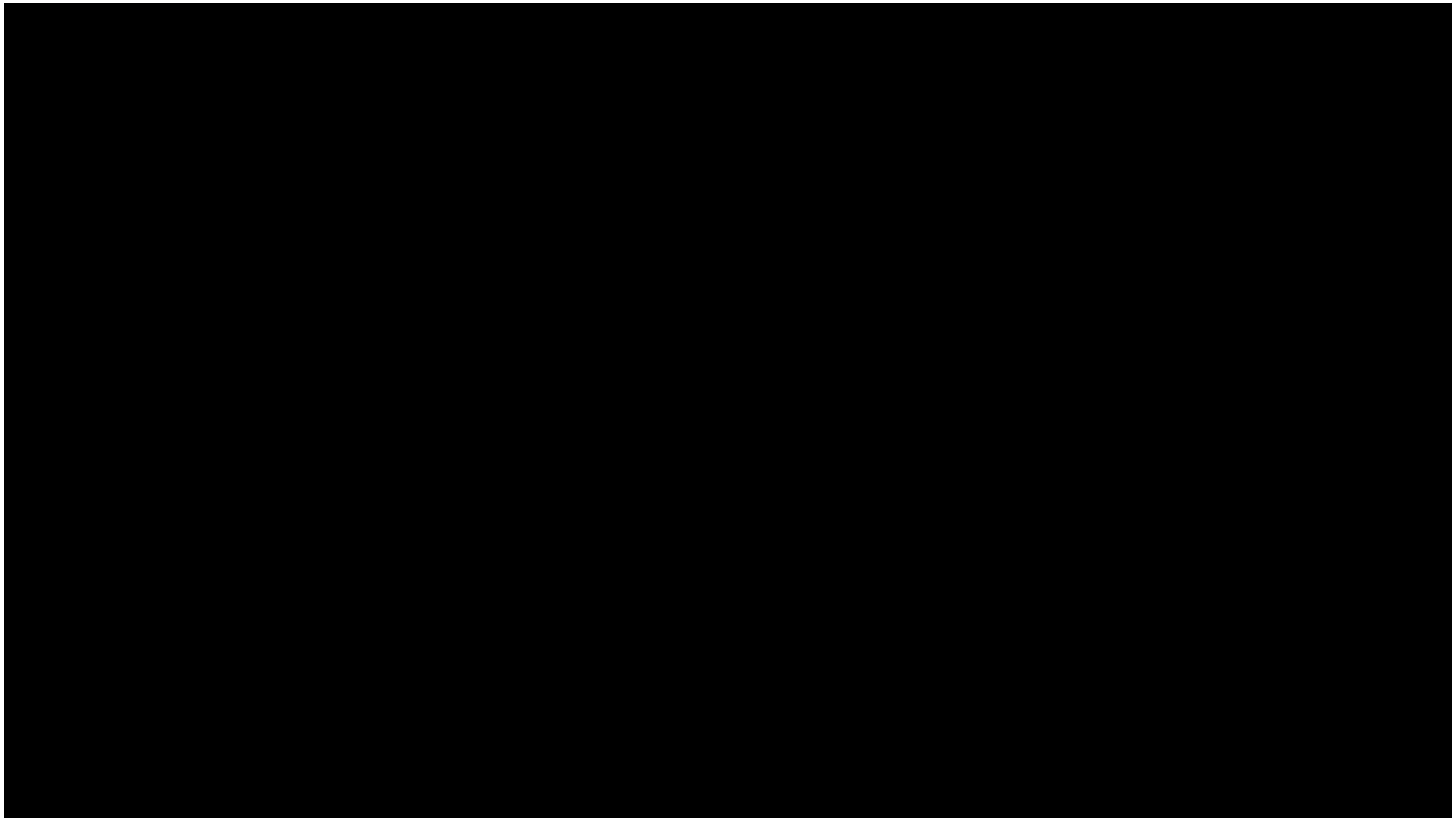
– Telenor ringte opp svindlerne

SVINDELMELDING: Bildet viser en reell svindelmelding, som har lagt seg sammen med andre ekte meldinger i en meldingstråd fra Google.

Ringer du opp til dette nummeret, kommer du til det som tilsynelatende er Googles supporttjeneste – men som altså i virkeligheten er svindlere.

Seniornett ULLENSAKER

Svindelsamtale

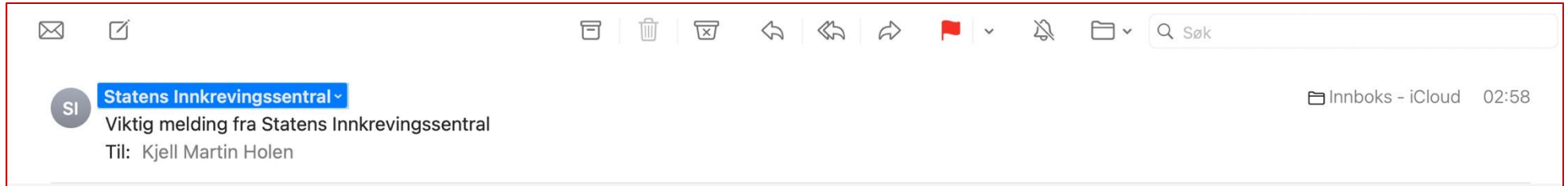


Seniornett ULLENSAKER

Hensikten med samtalen er å holde deg på tråden mens de tømmer kontoene din.
De som står bak er utrolig dyktige på å manipulere ofrene sine.
I løpet av samtalen får de tilgang på alt de trenger av informasjon, og kan også lure ofrene til å godkjenne transaksjoner med BankID.

Hva skal du gjøre om du får en slik SMS?

- Det ingen grunn til uro om du får en slik SMS, ettersom de mest sannsynlig går ut til tusenvis av tilfeldige numre.
- Bare ignorer meldingen, eller rapporter den som uønsket – da får også Telenor beskjed, og kan følge opp på sin kant med å sperre nummeret og blokkere SMS-ene.
- Og for all del, ikke ring opp til numre oppgitt i SMS-er som dette – selv om nummeret er norsk og det står at det haster. Bruk alltid offisielle nettsider eller apper for å kontakte bedrifter, eller søk opp riktig kontaktinformasjon selv.
- Og aldri oppgi betalingsinformasjon eller BankID!

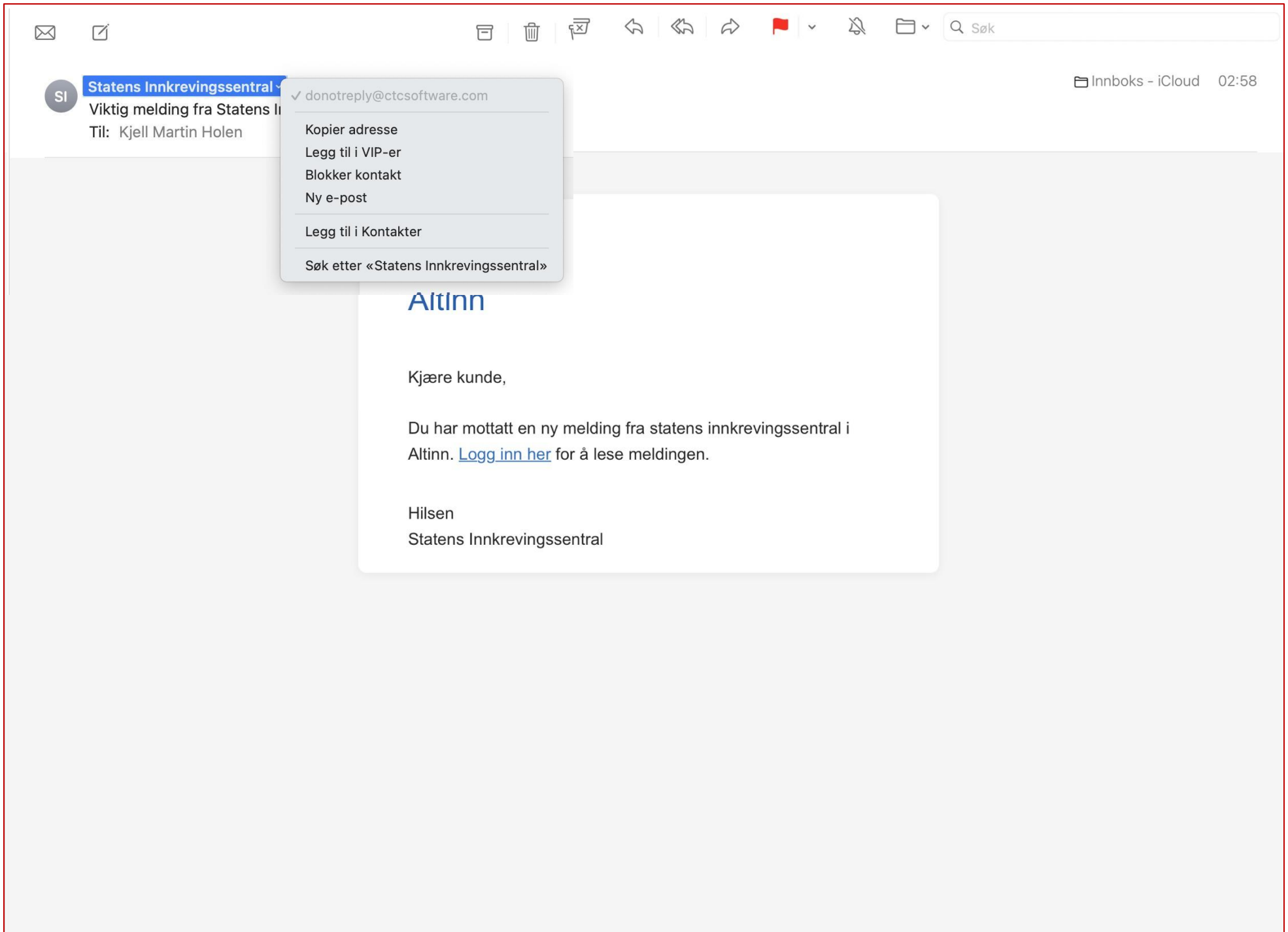


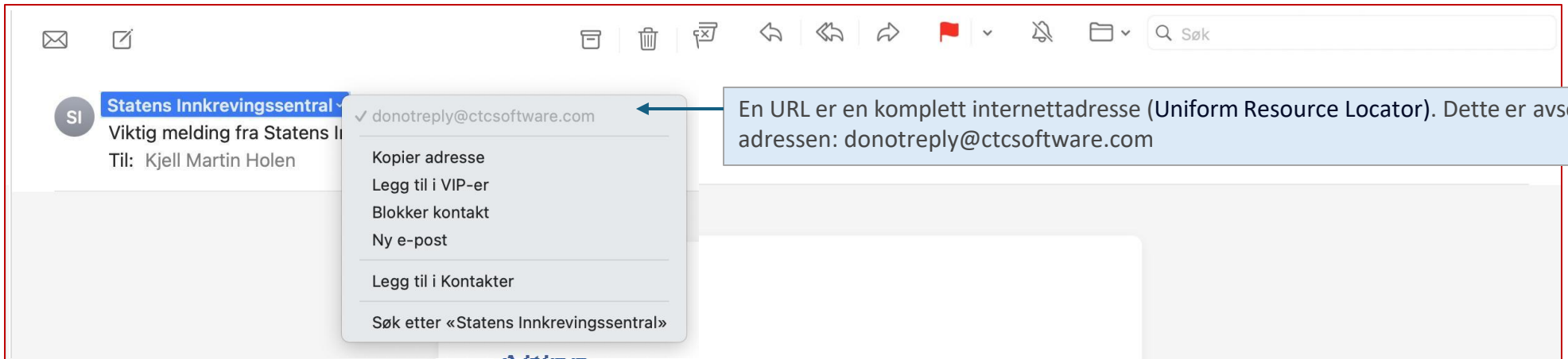
Altinn

Kjære kunde,

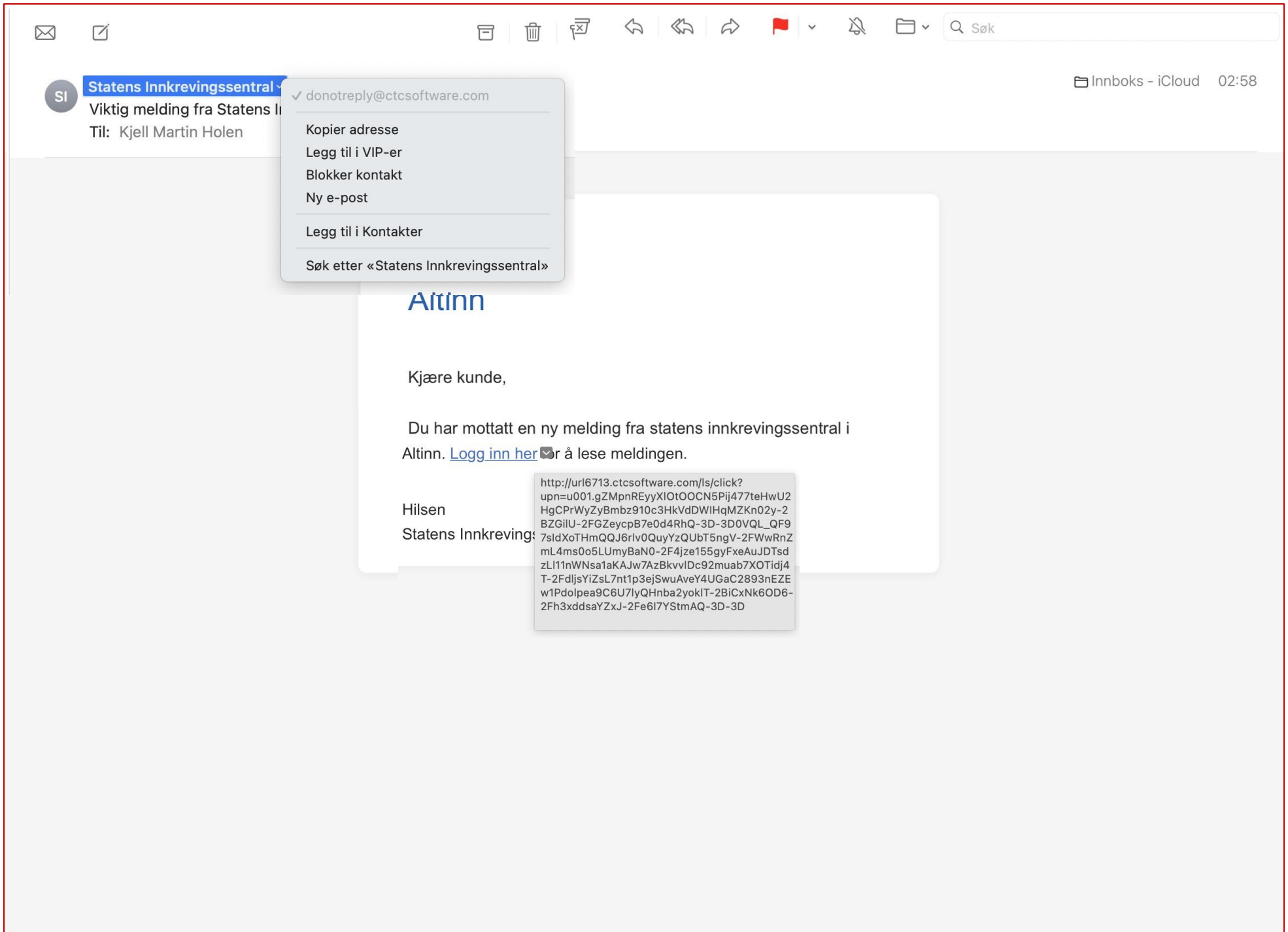
Du har mottatt en ny melding fra statens innkrevingssentral i Altinn. Logg inn her for å lese meldingen.

Hilsen
Statens Innkrevingssentral

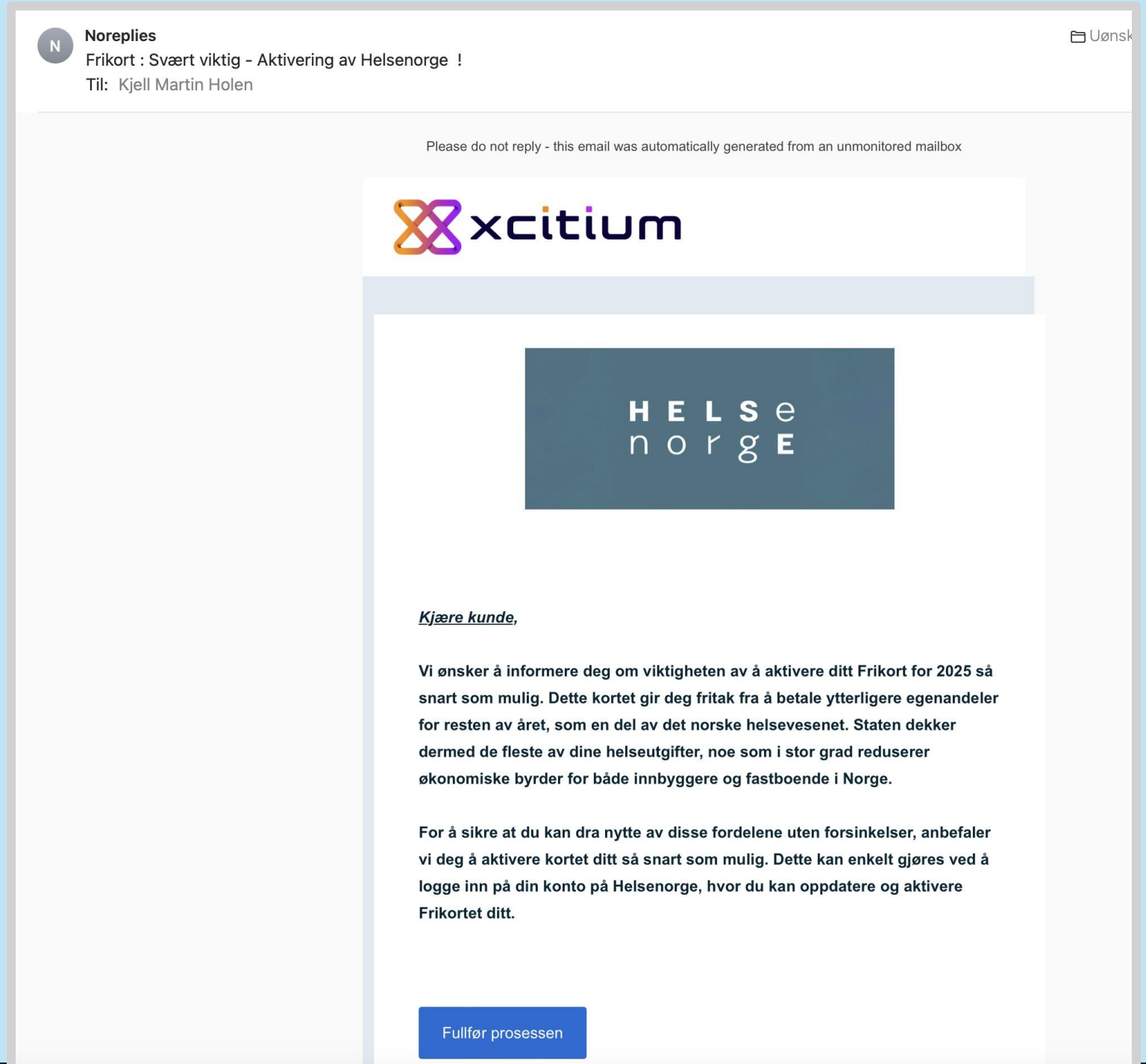

Søk
SI
Statens Innkrevingssentral
donotreply@ctcsoftware.com
Kopier adresse
Legg til i VIP-er
Blokker kontakt
Ny e-post
Legg til i Kontakter
Søk etter «Statens Innkrevingssentral»
Viktig melding fra Statens I
Til: Kjell Martin Holen
Innboks - iCloud 02:58
Altinn
Kjære kunde,
Du har mottatt en ny melding fra statens innkrevingssentral i Altinn. Logg inn her for å lese meldingen.
Hilsen
Statens Innkrevingssentral



En URL er en komplett internettadresse (Uniform Resource Locator). Dette er avsender-adressen: donotreply@ctcsoftware.com


Søk
SI
Statens Innkrevingssentral
donotreply@ctcsoftware.com
Viktig melding fra Statens I
Til: Kjell Martin Holen
Innboks - iCloud 02:58
Kopier adresse
Legg til i VIP-er
Blokker kontakt
Ny e-post
Legg til i Kontakter
Søk etter «Statens Innkrevingssentral»
Altinn
Kjære kunde,
Du har mottatt en ny melding fra statens innkrevingssentral i Altinn. Logg inn her for å lese meldingen.
http://url6713.ctcsoftware.com/ls/click?upn=u001.gZMpnREyyXlOtOOCN5Pij477teHwU2HgCPrWyZyBmbz910c3HkVdDWIHqMZKn02y-2BZGilU-2FGZeycpB7e0d4RhQ-3D-3D0VQL_QF97sIdXoTHmQQJ6rlv0QuyYzQUbT5ngV-2FWwRnZmL4ms0o5LUmyBaN0-2F4jze155gyFxeAuJDTsdzLl11nWNsa1aKAJw7AzBkvvIDc92muab7XOTidj4T-2FdljsYiZsL7nt1p3ejSwuAveY4UGaC2893nEZEw1Pdolpea9C6U7lyQHnba2yokIT-2BiCxNk6OD6-2Fh3xddsaYZxJ-2Fe6l7YStmAQ-3D-3D
Hilsen
Statens Innkrevings

Ekte eller falsk?



N

Noreplies

Frikort : Svært viktig - Aktivering av Helsenorge !

Til: Kjell Martin Holen

Uønsk

Please do not reply - this email was automatically generated from an unmonitored mailbox

xcitium

HELSE norge

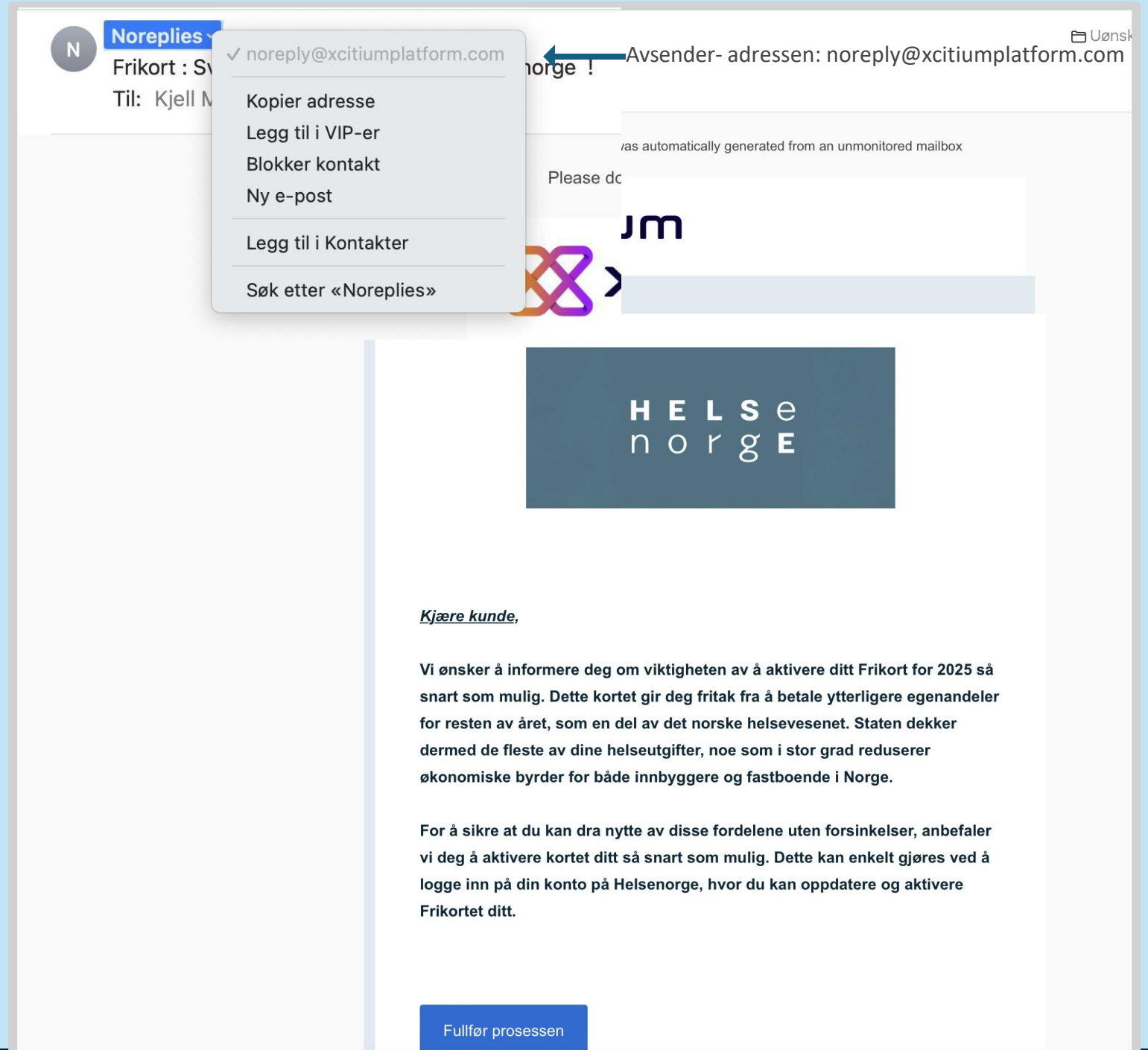
Kjære kunde,

Vi ønsker å informere deg om viktigheten av å aktivere ditt Frikort for 2025 så snart som mulig. Dette kortet gir deg fritak fra å betale ytterligere egenandeler for resten av året, som en del av det norske helsevesenet. Staten dekker dermed de fleste av dine helseutgifter, noe som i stor grad reduserer økonomiske byrder for både innbyggere og fastboende i Norge.

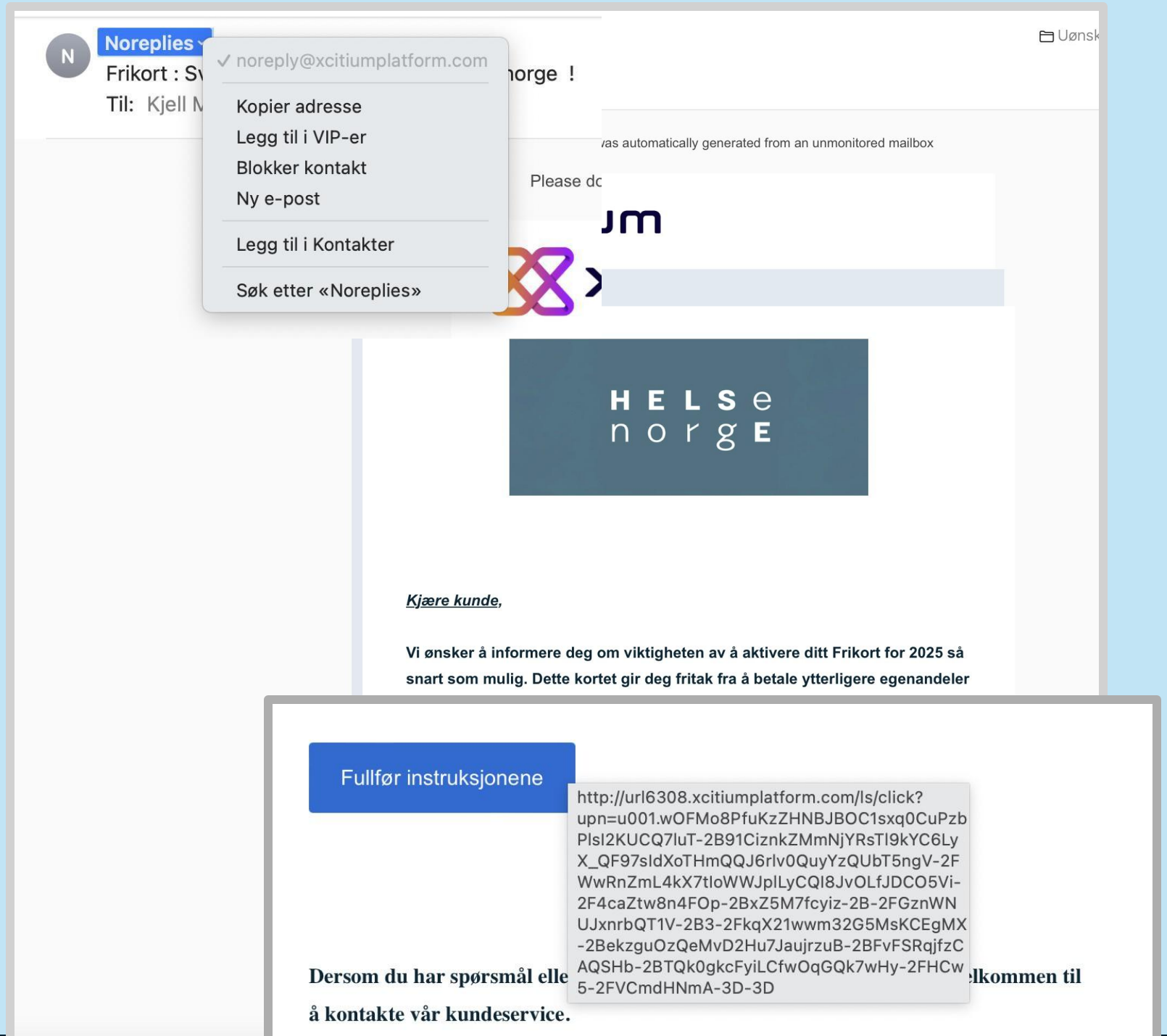
For å sikre at du kan dra nytte av disse fordelene uten forsinkelser, anbefaler vi deg å aktivere kortet ditt så snart som mulig. Dette kan enkelt gjøres ved å logge inn på din konto på Helsenorge, hvor du kan oppdatere og aktivere Frikortet ditt.

Fullfør prosessen

Ekte eller falsk?



Ekte eller falsk?



helsenorge.no

Helsenorge – din helse på nett - Helsenorge

HELSE norge

Meny

Søk

Logg inn

Ikke klikk på lenker i e-post som utgir seg for å være fra Helsenorge

Hei,
hva vil du gjøre?

- Lese melding eller brev
- Bestille time
- Se og fornye resept

Innboks

Meldinger og brev fra

Timeavtaler

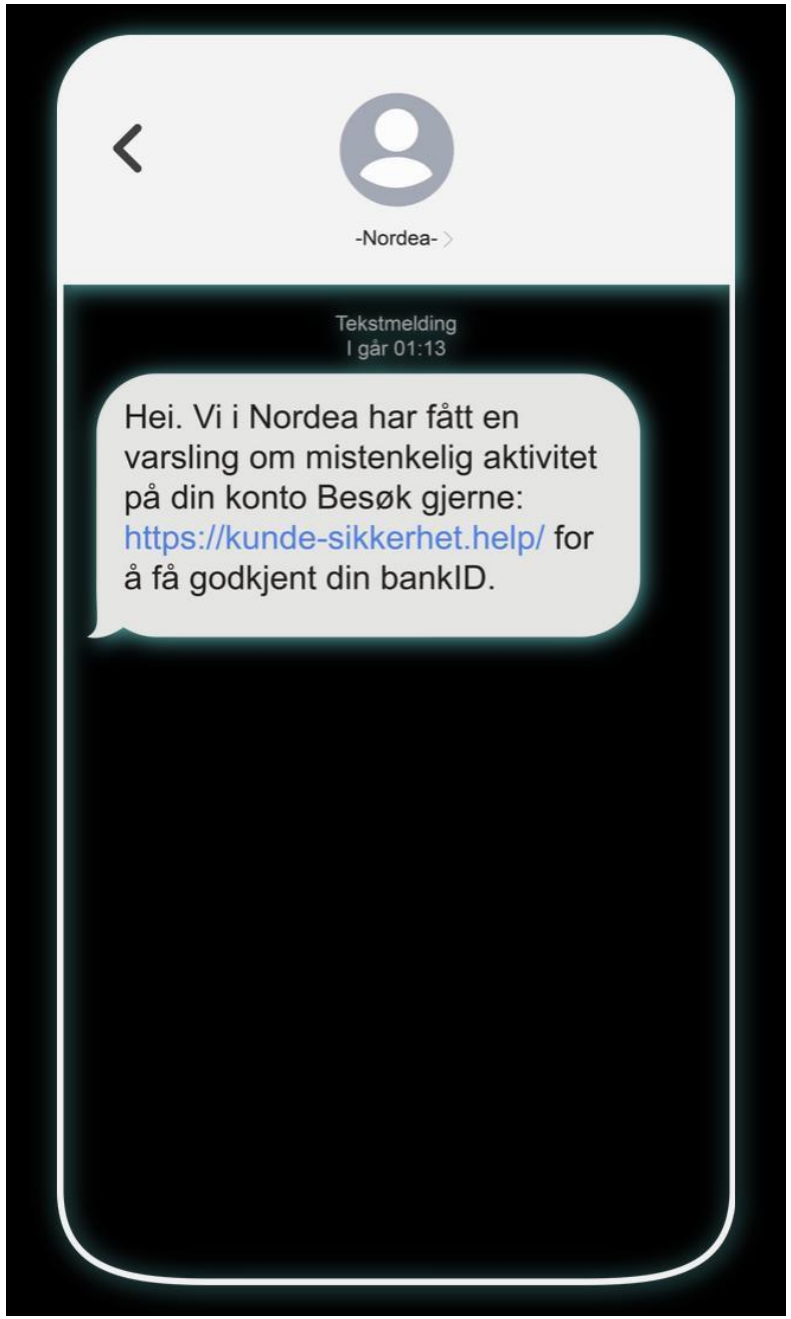
Timer og avtaler med

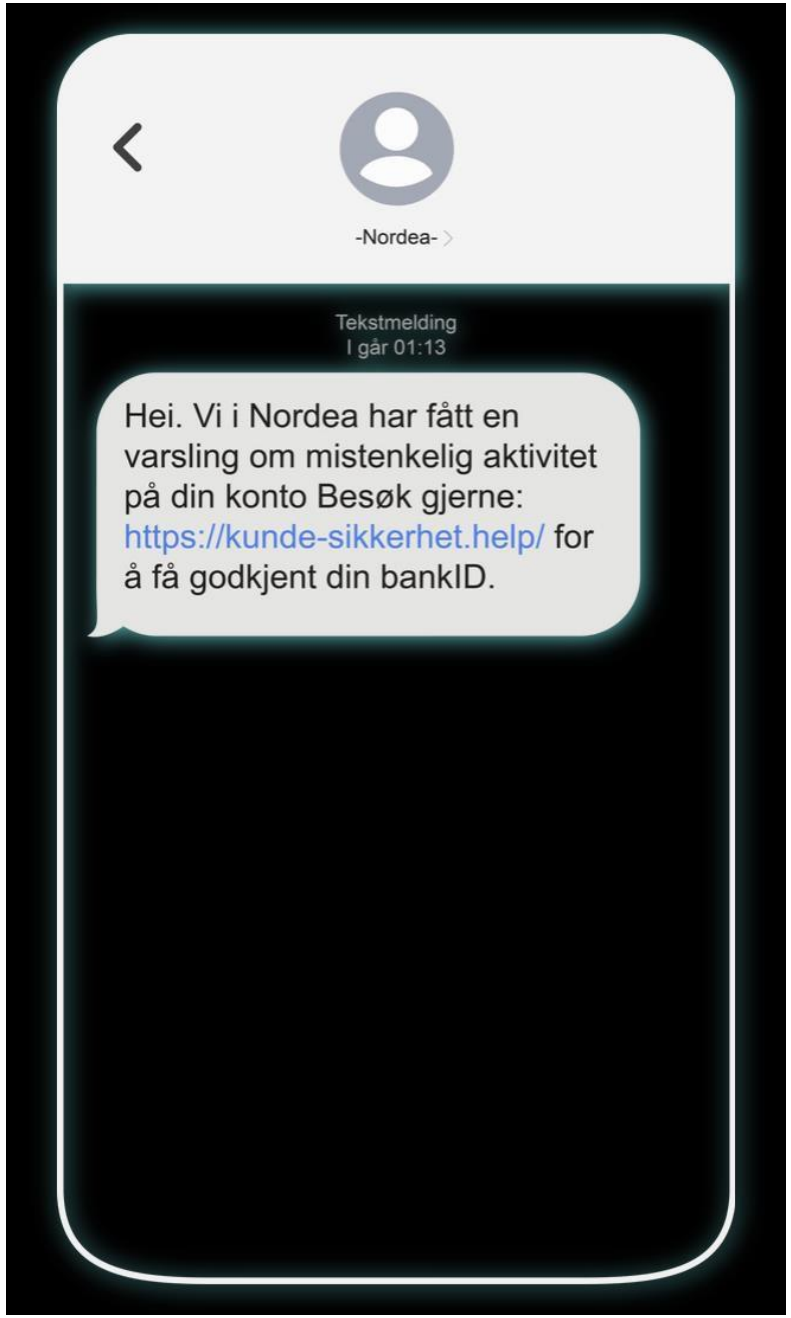
Henvisninger

Henvisninger til sykehus

Resepter

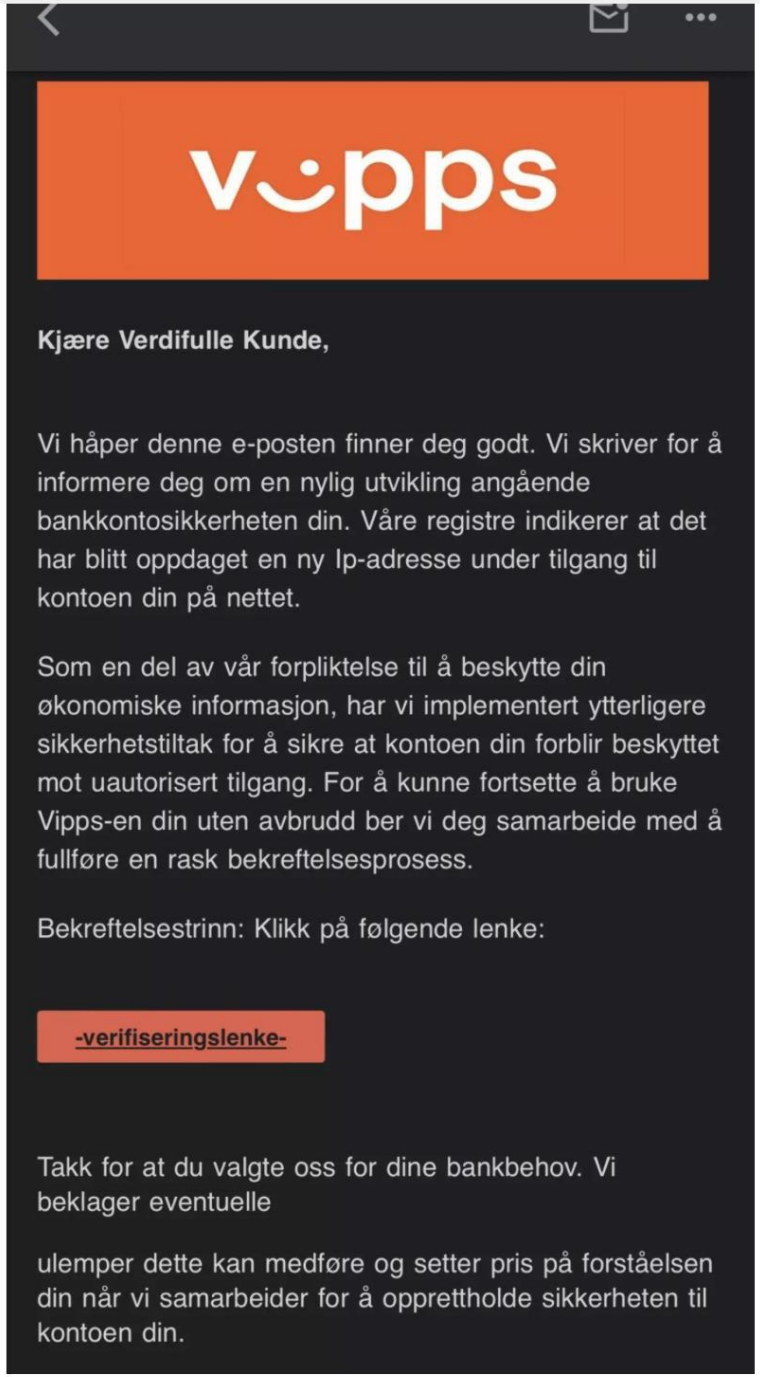
Resepter på medisiner og


-Nordea-
Tekstmelding
I går 01:13
Hei. Vi i Nordea har fått en varsling om mistenkelig aktivitet på din konto Besøk gjerne: https://kunde-sikkerhet.help/ for å få godkjent din bankID.

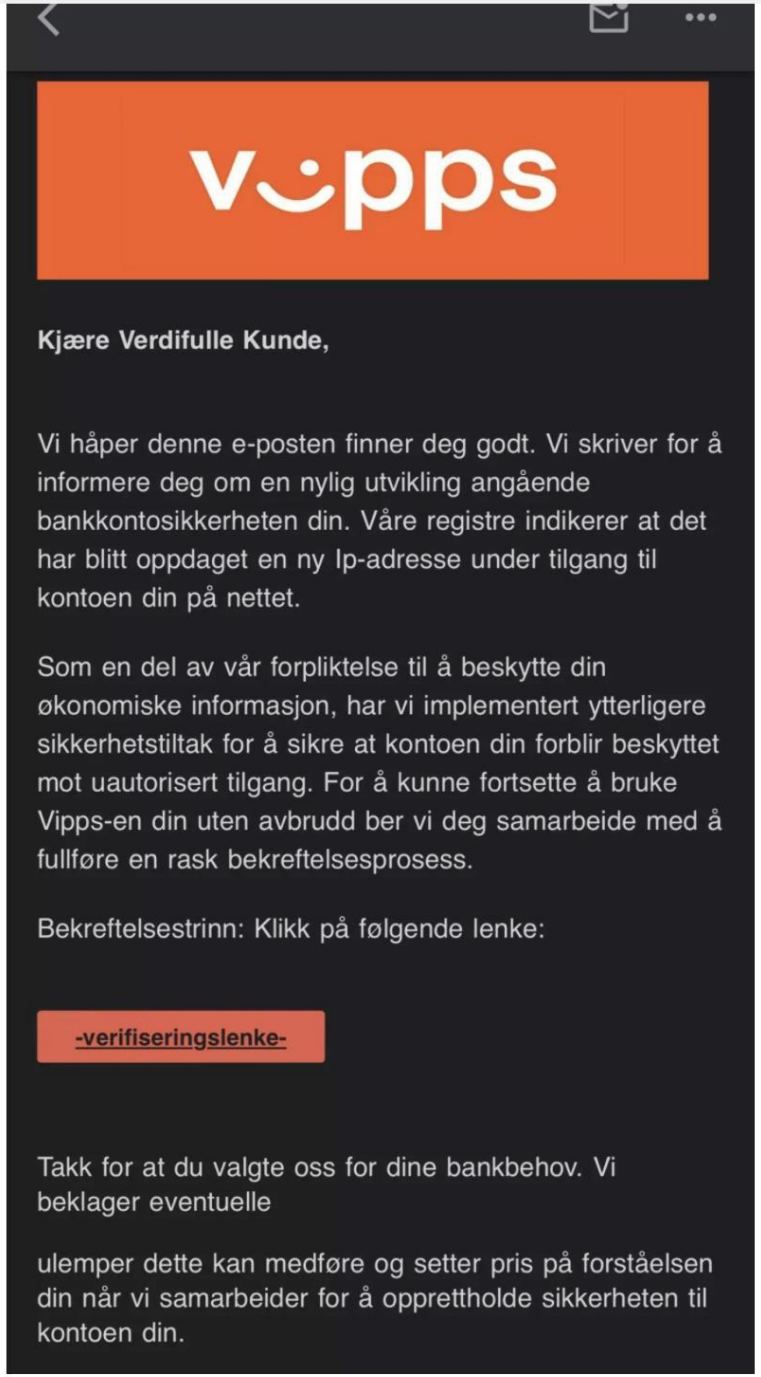


Slik avslører du phishing:

- Dobbelsjekk avsendernavn og nummer. Husk at svindlerne kan endre nummer eller navn slik at avsender har et norsk nummer.
- Hvilket tidspunkt mottok du SMSen på? De færreste seriøse henvendelser blir sendt midt på natten.
- Se etter språklige feil. Selv om mange svindlere har blitt bedre på rettskriving, er dette ofte et tegn på svindel.
- Er det en lenke i meldingen? En seriøs aktør vil aldri lenke direkte til en innloggingsside i SMS eller e-post. Søk i stedet selv opp hjemmesiden og logg inn derfra, i stedet for å gå via lenken.



Skjermbilde av en svindel-epost som bruker Vipps sitt navn og logo



Skjermbilde av en svindel-epost som bruker Vipps sitt navn og logo

Ikke trykk på lenker i meldinger !

Bruk heller den originale appen

– Vi vil aldri spørre kunder om å trykke på en lenke gjennom e-post eller sms. Er man usikker, gå til Vipps-appen. Der kommuniserer vi trygt, sier Lunde.

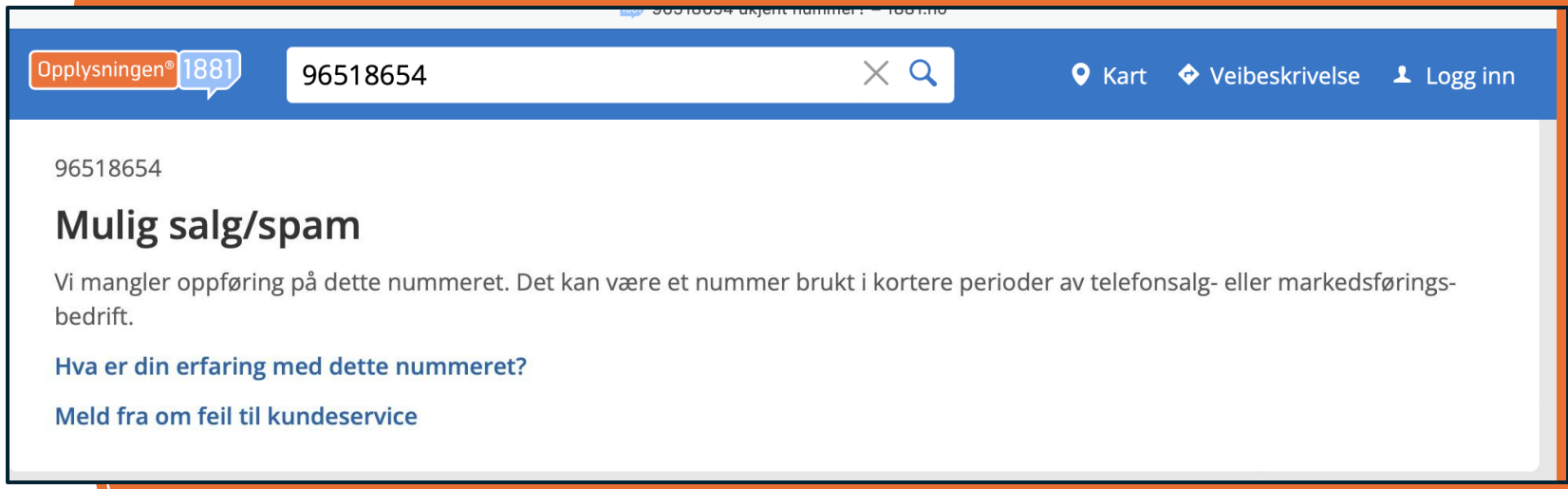
Og om noen velger å trykke på disse lenkene som kommer fra svindlerne, er det fint lite Vipps kan gjøre.

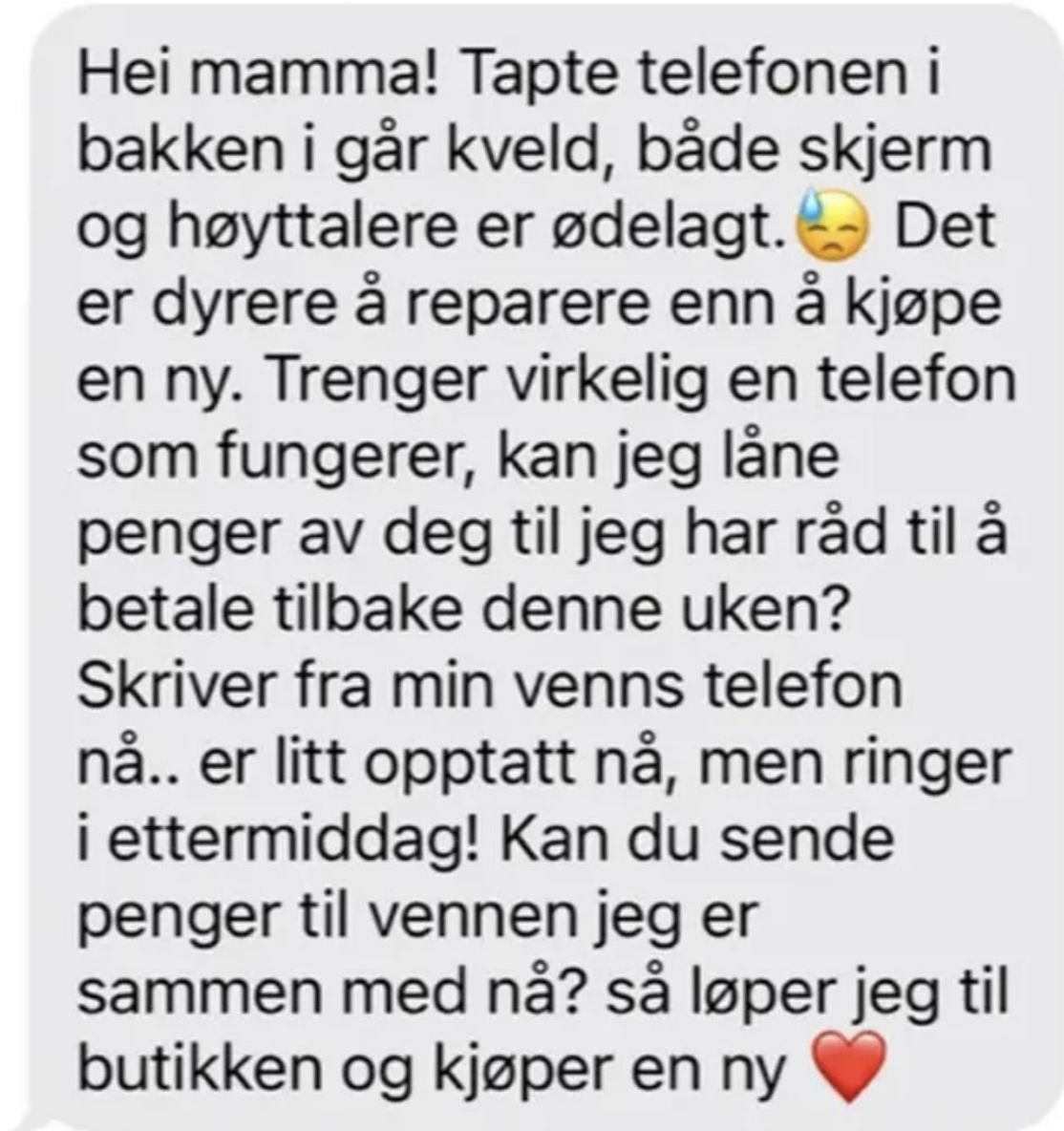
– Vi får dessverre ikke gjort så mye. Vi får ikke stoppet det. Derfor er det viktig at man går inn i appen. Det er viktig om folk blir mer skeptiske også, sier Lunde.

Vær obs på at en QR-kode er en lenke!

Falsk eller ekte?

Falsk eller ekte?

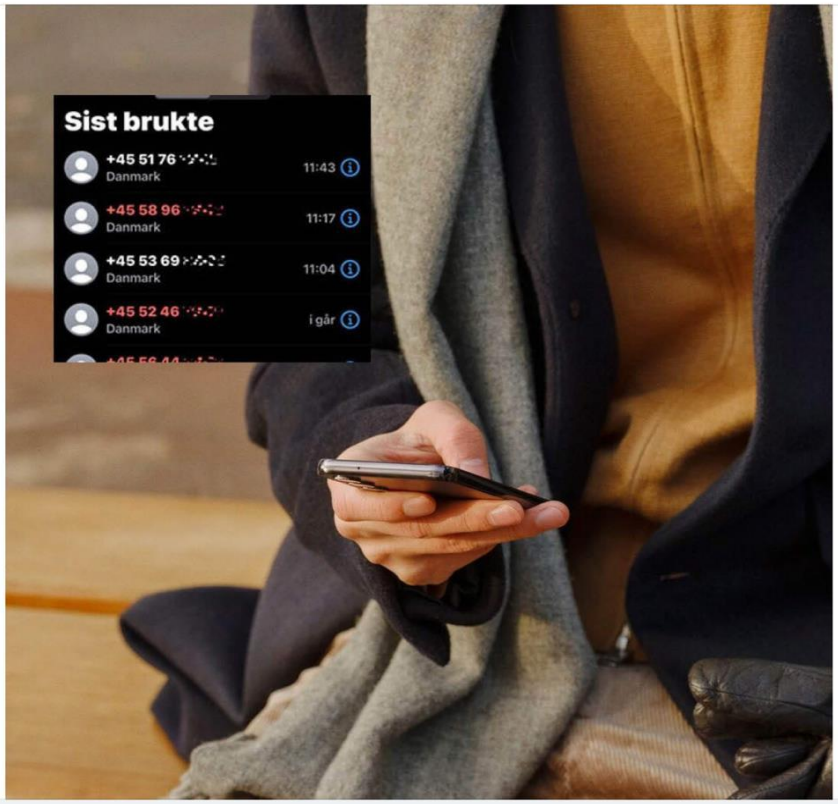




UTBREDT SVINDEL: Eksempel på en «Hei mamma!»-melding Telenor har blokkert.

Telenor: «Se opp for Paypal-svindel»

Vær ekstra forsiktig med danske og svenske numre, advarer sikkerhetsekspert.



TELENOR.NO
Advarer om stor svindelbølge
Finn ut mer

Arvid Martin Holen og 836 andre 330 kommentarer 136 delinger

Hva er Paypal-svindel?

- Paypal-svindel er anrop hvor du blir ringt opp av en automatisk melding som forklarer at en bestilling er feilregistrert på deg og at du må trykke «1» for at de skal hjelpe deg.
- Hvis du trykker «1» blir du satt over til en «saksbehandler» som vil prøve å få tilgang til betalingskortene dine for senere å misbruke eller stjele Bank-IDen din.
- Får du en slik telefonsamtale, bør du legge på. Husk at du aldri må oppgi sensitiv informasjon på telefon.
- Telenor ser nå en stor svindelbølge fra svenske og danske numre.

Seniornett ULLENSAKER

Vanlige typer AI-svindel

🎭 **1. Deepfake-videoer og -bilder**

Manipulerte videoer eller bilder av kjente personer eller venner/familie.
Brukes ofte til å få deg til å tro at noen ber om penger eller promoterer investeringer.

🎤 **2. AI-genererte stemmer (voice cloning)**

Svindlere kan kopiere stemmen til en du kjenner ved hjelp av korte lydklipp.
Typisk scenario: En «slektning» ringer og sier de trenger penger umiddelbart.

💬 3. **AI-skrevne meldinger og e-poster**

Svært overbevisende e-poster som etterligner banker, offentlige etater eller arbeidsgivere.
AI gjør språket mer naturlig og feilfritt, noe som gjør dem vanskeligere å avsløre.

Seniornett ULLENSAKER

📞 4. AI-styrte telefonsamtaler

Roboter som svarer intelligent og tilpasser seg samtalen.
Brukes i falske kundeservice-henvendelser eller «teknisk support».

💸 5. Falske investeringsmuligheter

Deepfake-videoer av kjendiser som «anbefaler» kryptoinvesteringer eller raske penger.
AI-genererte nettsider som ser profesjonelle ut.

🛍️ 6. Falske nettbutikker laget med AI

AI brukes til å lage troverdige produktbilder, anmeldelser og tekster.
Butikken forsvinner etter at du har betalt.

Seniornett ULLENSAKER

👩‍💻 7. AI-genererte kundeservice-chatter

Svindlere bruker AI-chatbots som utgir seg for å være legitime selskaper.
De kan be om personopplysninger eller betaling.

📄 8. AI-forfalskede dokumenter

Lønnsslipper, ID-kort, kontrakter eller fakturaer laget med AI.
Brukes i alt fra boligsvindel til bedrageri mot bedrifter.

Seniornett ULLENSAKER

Hvordan beskytte seg

Vær skeptisk til uventede henvendelser, selv om de virker ekte.

Bekreft alltid via en annen kanal (ring tilbake på et kjent nummer).

Ikke del personopplysninger eller koder.

Sjekk avsenderadresser og URL-er nøye.

Stol på magefølelsen – hvis noe virker «litt rart», er det ofte det.

Konklusjon: Vær skeptisk

- Sjekk språket, formelt vs uformelt, skrivefeil
- Hastverk og stress — Må du ordne det fort?
- Er avsender riktig?
- Er klokkeslettet mistenkelig?
- Er det lenke i meldingen?