

Hvordan unngå å bli svindlet?

Black Week flommer over av mange gode tilbud
– hvordan unngå svindelforsøk mot deg?

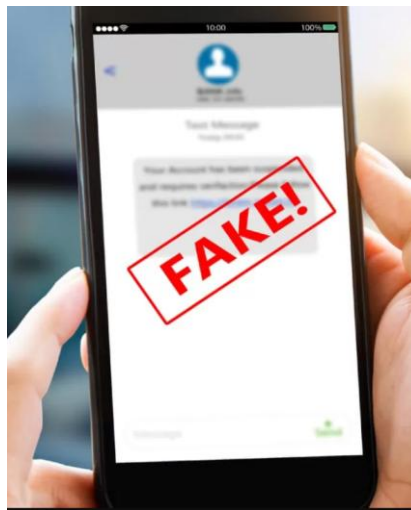


Vi skal se på ulike metoder for svindel



Telenor, ICE og TV2

- Spoofing
- Smishing
- Vishing
- Prompt injection
- ID-tyveri



Telenor

- Gode tilbud?!
- Falske nettbutikker
- Sikker betalingsmåte
- Pakke er på vei – falsk melding
- Opptre sikkert!

Spoofing

- Svindlere ringer **deg** og utgir seg for å være fra PayPal eller andre kjente selskaper
- Spoofet nummer = et telefonnummer som er blitt **forfalsket** slik at samtalen ser ut til å komme fra en pålitelig kilde
- Millioner av anrop daglig fra svindlere som brukte spoofede nummer fra Nederland, Irland og Romania



Smishing

- Svindleren ber deg ringe til et mobilnummer
- Du blir møtt av en svært overbevisende «kundebehandler» som forsøker å lure til seg informasjon
- Du gjerne melding fra bank eller en offentlig instans
- Stadig opp nye svindelmetoder vi må være bevisste på
- *HUSK! Offentlige instanser eller banker ber deg **aldri** ringe til et mobilnummer*



Vishing

Vishing (voice phishing) er svindel via telefonsamtaler. Ofte starter det med en SMS (smishing), før du blir bedt om å ringe tilbake.

Slik beskytter du deg:

- Legg på dersom du blir usikker
- Aldri oppgi sensitiv informasjon på telefon
- Ring alltid opp via offisielt nummer



Prompt injection

Prompt injection handler om å manipulere KI-systemer til å dele informasjon eller utføre uønskede handlinger. Dette rammer særlig bedrifter som tar i bruk kunstig intelligens.

Slik beskytter du deg:

- Bruk sikre og oppdaterte KI-løsninger
- Ha rutiner for testing og overvåkning
- Ikke stol blindt på svar fra KI – verifiser kritisk informasjon



ID-tyveri

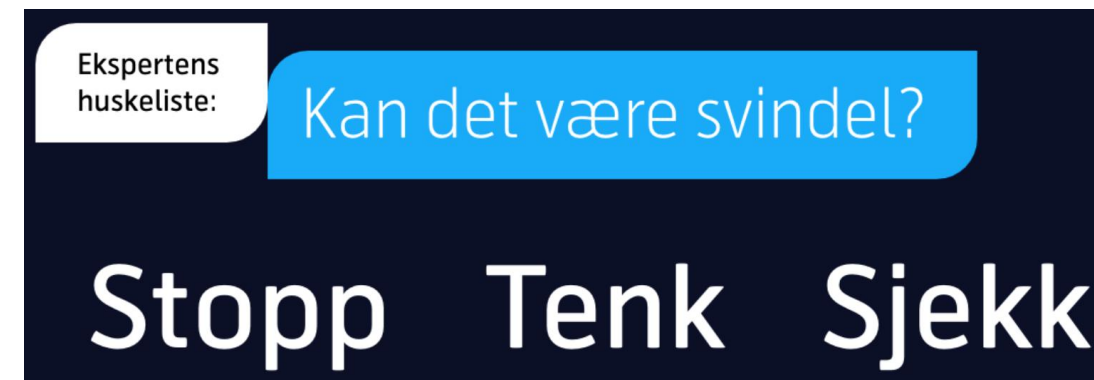


Boardingkort kan brukes til hacking og ID-tyveri

- Svindlere oppretter mobilabonnement i navnene til personer som allerede er utsatt for ID-tyveri
- Abonnementene brukes til å sende ut SMS-er med falske beskjeder, for eksempel at et kredittkort er sperret
- Mottakeren blir bedt om å ringe et oppgitt nummer for å ordne opp
- Nummeret går til et annet falskt abonnement opprettet med stjålet ID
- Når offeret selv ringer inn, får svindlerne et psykologisk overtak
- Samtalene kan vare i over en time. På den andre enden sitter profesjonelle svindlere som utgir seg for å være fra banken eller et kundesenter. Målet er å få tak i sensitiv informasjon som kontonummer, kortnummer eller BankID

Hvordan sikre deg?

- Oppgi aldri sensitive opplysninger på SMS, telefon eller e-post
- Stol aldri på meldinger fra banken, NAV, politiet eller Posten som ber om kort- eller BankID-informasjon
- Sett opp flerfaktorautorisering
- Bruk mobilnett framfor åpne WiFi-nettverk
- Klikk ikke på lenker fra ukjente avsendere
- Dersom du har delt informasjon:
Kontakt banken din umiddelbart!
- Gjennomgå sikkerheten jevnlig



For godt til å være sant



- La deg ikke lure i hektisk førjulstid
- Gode priser kan være svindel
- Bruk alltid trygge nettbutikker med .no bakerst i nettadressen
- Kjenner du ikke til nettbutikken fra før og ikke er helt sikkert på at den er seriøs, bør du alltid være kritisk til butikken før du handler
- Lukk heller siden, og søk opp butikken på Google

Gode betalingsvaner



- Vær trygg på at du samhandler med noen du stoler på
- Velg trygge betalingsmåter som Vipps, Apple Pay, Google Pay eller Klarna
- Bruk helst **kredittkort** eller kort der du må identifisere deg med BankID
- Du har utvidede rettigheter og garantier i «kortet»



Trygge rutiner

Trygge nettbutikker
- unngå å bli svindlet!

- Ukjent mobilnummer? Bruk nummeropplysningstjenestene for å **Se hvem** som eier nummeret
 - Sjekk ut avsender via andre kanaler – Googlesøk, Facebook og andre sosiale medier
- HVIS!**
- Sperr kort- eller kontoopplysninger umiddelbart
 - Skift passord umiddelbart da konto er oppe igjen



Lykke til med alle dine innkjøp til jul