

DIGITAL SVINDELORDLISTE

1.Spoofing:

Kan komme fra norske numre, hyppig brukt svindelform, der svindlerne later som de er noen du stoler på- bank, teknisk support etc.,for å vinne tilliten din og lure deg.

Mål: få deg til å røpe informasjon eller sende deg en lenke som de vil du skal trykke på

Trykker du på lenken, kan svindlerne få kontroll over din PC og i verste fall presse deg for penger



DIGITAL SVINDELORDLISTE forts.

2. Phishing/smishing:

å fiske etter sensitiv informasjon.

Tilsendt e-post eller SMS fra svindlere der de utgir seg for å være Posten eller DNB el.l

Her prøver svindlerne å lure deg til å oppgi dine personopplysninger/BankID -til økonomisk vinning.



DIGITAL SVINDELORDLISTE forts.

3.«Wangiri»

Tapt anrop eller korte anrop, ofte bare et ring, fra et **utenlandsk** nummer, hvor svindlere vil lure deg til å ringe tilbake til dyre numre.

Det koster ingenting å ta telefonen, det er kun hvis du ringer tilbake

4.«Robocalls»

Automatisert telefonsamtale som leverer en forhåndsinnspilt melding. Robocalls brukes ofte til å utgi seg for å være fra pålitelige aktører og lure mottakeren til å dele sensitiv informasjon eller foreta betalinger.



DIGITAL SVINDELORDLISTE forts.

5. Kjærlighetssvindel eller noen som er i nød

Kynisk bedrageri

Eldre og sosiale datingsider

Bygge tillit/ vanskelig å gjennomskue kan bruke lang tid

I tvil? Ikke send penger. Snakk med noen du stoler på og sjekk med dem om du er i ferd med å bli svindlet





Politiets sterke oppfordring

- **TENK DEG OM**
- Ville du gitt husnøklene til noen du ikke kjenner?
- BankID = di personlige nøkkel til dine penger
- Kode og kodebrikke
- Forespørsler om engangskode og passord over telefon = svindler
- Bank eller politi ber deg **ALDRI** om bankID, kode eller passord



«Digital svindel i Norge. En umulig kamp?»



Telia m.fl. på Arendalsuka

- Svindlere basert i De forente arabiske emirater har denne våren sendt over 30 000 phishing -sms til nordmenn via norske telefonnumre.
- SMS-ene er « snudd på hodet» slik at mottaker må ringe svindlerne istedenfor å trykke på en lenke. Ringer du tilbake har du allerede « bitt på» og er lettere å påvirke med manipulasjon.
- Telias analyser viser at over 50 kunder har ringt tilbake og snakket mer enn 10 minutter med svindlerne. Lengre samtaletid fører til høyere sannsynlighet for å ha blitt lurt.

- Telia, norske banker, kunder og mottakere av SMS er berørt
-
- Svindlere har bestilt over 30 abonnement hos Telia ved å bruke BankID-en til ulike nordmenn, De fleste er født før 1950. Svindlerne har fått fatt i deres BankID.
- SMS svindelen oppdaget gjennom Telias løpende svindelmonitorering og saken er nå anmeldt til politiet.
-
-

Hva gjør Telenor med svindelforsøk?



I 2. kvartal i år foretok Telenors sikkerhetsfiltre 459 millioner blokkeringer på nett.

I tillegg blokkerte de 9 millioner forsøk på svindel via anrop og 10,9 millioner via SMS. Jevn nedgang. Mindre wangiri anrop – funnet måter å oppdage og stoppe disse.

Kjente svindelsider, forsøk på spredning av skadevare samt Phishing utgjør de største kategoriene av blokkeringer på nett.

Det er fortsatt høy svindelaktivitet rettet mot nordmenn. Metodene som benyttes har endret seg fra forrige kvartal.



Holdninger til digital sikkerhet

Telenors spørreundersøkelse i juni 2025:

- Nær halvparten av de spurte har endret sin digitale atferd det siste året som følge av frykt for svindel eller datainnbrudd.
- Godt over halvparten av de spurte er flinke til å bruke tofaktorautentisering eller passnøkler,
- Mer enn halvparten svarer de er flinke til å oppdatere apper og programvare. De eldste er vesentlig bedre enn de yngre her





**Telefon og nettsvindel er mest
brukt**

STOPP TENK SJEKK

Ring gjerne politiet 02800 for hjelp eller
Nettpatruljen på FB/Instagram

 **Seniornett**