# RørosBanken advarer mot svindelaktivitet:

# Dette må du passe deg for

— De fleste svindelforsøk kan stoppes ved å bruke sunn fornuft. Kontakt oss hvis du er usikker.

**Siw Brean, kunderådgiver i RørosBanken**


**Tlf 72 40 90 00**

*man - fre 07 - 21*

*lør - søn 09 - 21*

**firmapost@rorosbanken.no**


RørosBanken

## Oversikt over noen svindel-metoder

Spoofing: Telefon- og SMS-fisking

Svindleren ringer deg (eller sender melding) og utgir seg for å være fra banken, og ber deg om å oppgi BankID-informasjon. En bank vil aldri be deg om slik sensitiv informasjon.

Falske lenker

Noen gang trykket på en lenke som ledet deg til en suspekt nettside? Er du usikker på om du skal trykke på lenken så kan du holde musepekeren over lenka. Da skal adressen til nettsiden komme opp. Vær skeptisk til rare, lange og sammensatte navn.

Utgir seg for å være datahjelp

Blitt oppringt av noen som mener du har pc-problemer? Større problemer venter deg hvis du svarer ja. Svindlerne forsøker å få tilgang til dataen din, via fjernstyring.

Falske investeringer

Fått tilbud om å investere med skyhøy avkastning, sammen med noen du aldri har hørt om? Slike tilbud er ofte for gode til å være sanne, og du risikerer å plassere pengene dine hos noen du kanskje ikke hører fra igjen.

Falske nettbanker

Mottatt en e-post eller melding med lenke til nettbanken? Ikke trykk. Vi vil aldri sende deg en lenke hvor vi ber deg logge inn, med mindre du har avtale med oss om signering av dokumenter og lignende. Er du usikker så sjekk det med oss først.

Kjærlighetssvindel (Olgasvindel)

Møtt den store kjærligheten på nettet? Svindleren kan bruke flere måneder på å sjarmere deg før svindelen starter, og kan være veldig overbevisende. Det kan være vanskelig å godta at personen kun er ute etter penger.

Mistenksomme SMS-er fra Posten

Vær spesielt oppmerksom på SMS og e-poster fra Posten, og andre som leverer dine varer. Denne typen svindel dreier seg ofte om SMS-er hvor det står at mottaker har en pakke på vei, men må betale en lav avgift for å få denne utlevert. I realiteten gir man fra seg kortopplysninger og blir svindlet for potensielt flere tusen kroner. Et godt tips er å unngå å ha mye penger stående på brukskontoen, i tilfelle noen forsøker å trekke penger fra denne uten tillatelse.

Identitetstyveri på sosiale medier

Politiet mottar flere henvendelser fra folk som har blitt utsatt for svindel på Facebook, Instagram og Whatsapp. De hacker din Facebook- eller Instagram- konto, for å få tilgang til kontaktene dine. Videre tar de kontakt med dine kontakter, og utgir seg for å være deg. Dette gjør de for å svindle personer for penger.

Falske konkurranser

Svindlerne frister med flotte premier eller gaver for å få deg til å delta i en falsk spørreundersøkelse eller konkurranse. Som oftest imiterer svindlerne store og kjente merkevarer, slik at du får tillit og er villig til å gi fra deg personlige og økonomiske opplysninger.

Falske nettbutikker og kortsvindel

Hvis du vurderer å handle på en nettside som du ikke har handlet på før, bør du sjekke om den er trygg. Dårlig språk på nettsiden er et faresignal. Husk at seriøse nettbutikker alltid har lovpålagt informasjon lett tilgjengelig, som for eksempel at de opplyser om adresse, e-post og organisasjonsnummer. Ikke glem at tilbud som åpenbart er altfor gode - ofte er for gode til å være sanne.

# Rådene som beskytter deg mot BankID-svindel

- Aldri oppgi BankID-informasjon til andre, hverken venner, familie eller banken.
- Alternativt kan du be en av dine nærmeste veilede deg. Da bør du selv logge inn og taste inn passordet ditt, uten at noen ser det.
- BankID eller banken ber deg aldri om å oppgi koder og passord via e-post eller telefon.
- BankID vil aldri sende ut SMS-er som inneholder lenker. Får du en SMS med en lenke fra noen som utgir seg for å være BankID, så er dette svindel.
- Bruk et unikt passord for BankID. Bruk gjerne en enkel og positiv setning som er lett å huske. Og du, husk at du kan bruke mellomrom i BankID-passord! Dette vil fungere som et spesialtegn.
- Ta heller kontakt med banken din en gang for mye enn en gang for lite om du mistenker svindel.

## Bruk kredittkort til netthandel

Handler du på nett, er det viktig å bruke kredittkortet ditt når du betaler, enten du velger å bruke Vipps eller kortbetaling.

Grunnen er at kredittkortet er tryggere enn ditt vanlige bankkort. I det du bruker kortet, er det nemlig bankens penger du handler med, og ikke dine egne. Skulle du derfor være uheldig og bli svindlet, er det ikke lønnskontoen din som blir tappet.


Kredittkortet fra oss gir deg mange fordeler, enten du er på reise, handler på nett, eller når noe uforutsett skjer. Det er rett og slett gull å ha i lommeboka eller reiseveska. Effektiv rente 25,11 %, v/15.000,- o/12 mnd. Kostnad 1.563,68 kr. Totalt 16.563,68 kr.

## Har du blitt svindlet?

Om uhellet skulle være ute, er det én ting som betyr noe: Gi beskjed til banken så fort som mulig for å få sperret kort og konto som kan være utsatt for svindel. Jo raskere vi får vite om svindelen, jo større sjanse er det for å få stanset det og få pengene dine tilbake.

**Mette Nesvold, seniorrådgiver i RørosBanken**

**Skann QR-kode for å se hjelpsomme videoer som kan hjelpe deg med å identifisere svindel:**

https://www.rorosbanken.no/Sikkerhet/Svindel