POLITIET telenor DNB

BEDRAGERI MOT ELDRE

Bedrageri og svindel blir stadig mer utspekulert. Eldre er en målgruppe som svindlerne retter seg spesielt mot.

Svindelmetodene som oftest brukes mot eldre er telefon - og nettsvindel. Svindlernes mål er å få tak i pengene dine.

Næringslivskontakt i Oslo politidistrikt, Christina Rooth

Sikkerhetsekspert i Telenor Norge, Thorbjørn Busch

Leder for bedrageribekjempelse i DNB, Terje Fjeldvær

Her er enkle råd du kan følge for å unngå å bli lurt, utformet av politiets næringslivskontakter i samarbeid med Telenor og DNB.

Tenk deg om

Du ville ikke gitt bort husnøkkelen til noen som spør!

På samme måte må du aldri gi fra deg informasjon fra din BankID, kodebrikke eller personlige passord. Å gi fra seg dette kan sammenliknes med å signere på et blankt ark, og gi dem fullmakt til å skrive hva de vil.

BankID er din personlige nøkkel til dine penger. Koden fra kodebrikken og passordet må du ikke gi til andre. Hvis noen ringer og spør om engangskoden og passord er dette en svindler. Banken eller politiet vil aldri be deg om BankID, koder eller passord.

Slik kan svindlerne lure deg

Såkalt "Olga-svindel" er en svindelmetode som foregår via telefon der svindleren har utpekt seg ofre med "gamle" navn som var vanlige å gi barna sine for 70-80 år siden.

Svindlerne utgir seg for å være fra norske banker, og ringer for å fortelle at lånet ditt er klart for utbetaling. Når du svarer at du ikke har søkt om lån, tilbyr svindleren å sette deg over til banken så de kan stoppe utbetalingen.

I realiteten blir du satt over til en annen svindler, som skal få deg til å oppgi BankID og annen innloggingsinformasjon.

Vær oppmerksom på at sosial manipulasjon er verktøy som brukes i nesten all mobil- og nettkriminalitet. Er du bevisst på dette, har du allerede gjort veldig mye for å sikre deg. Den generelle regelen er:

STOPP – TENK - SJEKK

Husk også på at svindlerne hele tiden fornyer seg og benytter argumenter som passer til situasjonen vi befinner oss i. I det siste har det vært mange ulike typer svindel som har relatert seg til Covid-19.

Sosial manipulasjon

Ofte spiller svindlerne på følelsesregisteret vårt. Svindlerne prøver å få deg til å føle frykt, stress og usikkerhet, eller de gir uttrykk for at de liker deg. Andre ganger spiller de på nysgjerrighet og frister med økonomisk gevinst. Svindlerne gir uttrykk for at du må gjøre som de sier med en gang, ellers forsvinner muligheten.

Mistet sparepengene

En kvinne i 80-årene mottok en telefon fra en som sa han var fra banken. Han fortalte at lånet var klart til utbetaling. Kvinnen hadde ikke tatt opp noe lån og ble nervøs. Hun sa at dette var en feil. Den som ringte sa han ville sette samtalen over til en annen kollega i banken. Pausemusikken ble slått på, og hun fikk snakke med en ny, hyggelig mann. Han ville hjelpe til med å stanse lånet, og sa han trengte hennes BankID-passord og kode fra brikken. Problemet var at mannen ikke var fra banken, han var en svindler og stjal alle sparepengene hennes.

Svindlet for flere hundre tusen kroner

En eldre mann ble oppringt av en hyggelig dame som utga seg å være fra banken han benytter. Damen lurte på om han hadde kjøpt mobiltelefoner for 300 000 kroner samme dag. Han ble forskrekket og benektet at han hadde gjort dette. Damen sa at han da var i ferd med å bli lurt. For å få stoppet svindelen sa hun at han raskt måtte logge seg inn med BankID på den lenken hun skulle sende han. Mannen ble stresset og gjorde derfor som damen sa. Han trykket på lenken han fikk tilsendt på SMS og brukte sin BankID. Damen var ikke fra banken, og mannen endte opp med å bli svindlet.

Dersom du mottar en uventet henvendelse via SMS, e-post eller telefon, er det viktig å spørre seg:

- Prøver de å skape hastverk? Lokkes eller trues det? Etterspørres personlig informasjon? **STOPP**
- Forventer jeg å få denne henvendelsen? Hva er det avsenderen egentlig vil meg? **TENK**
- Er det lenker til ukjente nettsteder? Ring banken eller finansinsitusjonen på offisielt nummer for å verifisere innholdet. **SJEKK**

Gode råd mot bedrageri og svindel

Ikke gi koden og passordet til din BankID til noen som ber om dette, uansett hvem som spør. Hvis noen spør om dette, er det en svindler. Det samme gjelder hvis du bruker BankID på mobil. NB! Ingen kjenner kodeordene som kommer fram på din telefon - ikke banken, BankID eller andre.

Digital informasjon kan lett forfalskes – vurder alltid informasjonen nøye.

Du trenger ikke sitte alene med disse vurderingene. Ring en god venn, noen i familien eller banken for å rådføre deg hvis du er i tvil.

Oppgi aldri sensitiv informasjon til noen som kontakter deg. Seriøse aktører ber deg aldri oppgi slik informasjon på telefon eller gjennom en lenke de sender deg på SMS eller på e-post. Er du i tvil om det er banken som ringer deg, bør du selv kontakte banken på kjent nummer.

Ikke stol på de som ringer, sender e-post eller SMS og som sier at de skal hjelpe deg med din PC. Dette er alltid svindel.

Husk å etablere en totrinnsbekreftelse på alle nettsider som tilbyr dette. Totrinnsbekreftelse (autentisering) er et ekstra sikkerhetsnivå for innlogging.

Informasjon om vanlige svindelmetoder

Phishing (fiske etter informasjon)

Svindlerne sender deg en e-post eller SMS, gjerne fra et kjent merkevarenavn for å skape troverdighet. Meldingsinnholdet er forlokkende og svindlerne spiller ofte på fristelser, nysgjerrighet eller frykt. Typisk innhold kan være at du har ubetalt porto, eller at du må oppdatere betalingsopplysningene dine for å hindre avslutning av et abonnement eller en konto.

Formålet til svindlerener er å få deg til å trykke på en lenke. Trykker du på lenken ledes du til en nettside som svindlerne har kontroll på. Dette kan være en kopi av en velkjent nettside hvor du blir bedt om å skrive inn brukernavn, passord og kortinformasjon.

Gjør du det, får svindlerne kontroll på opplysningene dine, og kan misbruke disse. Svindlere kan også utgi seg for å være fra banken for å få deg til å gi fra deg BankID på en falsk nettside som ligner bankens.

Misbruk av norske numre

Svindlerne kan enkelt utgi seg for å ringe fra et hvilket som helst telefonnummer. Ofte benytter de norske mobilnumre og fastnettnumre for å skape troverdighet, og få oss til å besvare.

Svindlerne vil typisk presentere seg som medarbeidere i Microsoft eller en annen teknisk support. Deretter vil de si du har et alvorlig problem med PC-en din, og at de kan fikse det. Målet er å få deg til å røpe informasjon de kan misbruke, eller de vil sende deg en lenke som de vil du skal trykke på. Trykker du på lenken får svindlerne kontroll over PC-en din, og vil stenge deg ute. De presser deg deretter for penger mot at de skal gjenåpne.

Investeringsbedrageri

Det finnes mange falske annonser som misbruker navn og bilde til kjente personer som deler et investeringstips, etterfulgt av en påstand om at banken din ikke vil at du skal kjenne til denne smarte måten å investere på.

Det er enkelt å sette inn beløp, og om du ikke klarer det selv, blir du kontaktet av hyggelige personer som hjelper deg. Disse later som de bryr seg om deg og innbyr til tillit. Det de egentlig gjør, er å få deg til å overføre pengene dine til falske investeringer - slik at du aldri får dem igjen. De kan også spørre om passordene dine, eller få deg til å laste ned et program som gjør at de får kontroll over PC-en din. Selv om de fremstår som høflige, har svindlerne ondsinnede motiver. Her er det er bare å legge på røret.

Ikke invester penger før du er 100 prosent sikker på at det ikke er svindel.

Kjærlighetssvindel eller noen som er i nød

Dette er en kynisk form for bedrageri som spiller på menneskers ønske om å bli likt eller elsket. De spiller også på folks ønske om å hjelpe andre. Svindleren påstår for eksempel at han er NATO soldat som trenger penger for å komme hjem.

Her bruker svindlerne tid på å bygge opp tillitt og det kan være vanskelig å avsløre hensikten bak. Til slutt vil de be om penger. Hvis du er i tvil, rådfør deg med noen du stoler på. Har du blitt avstandsforelsket og avtalt å treffes? Skjer det noe rett i forkant av dette? Gjentar historien seg? Hvis svaret er "ja" på noen av disse spørsmålene, er du trolig i ferd med å bli svindlet.

Tapte anrop fra utenlandske nummer

Du får et tapt anrop fra et utenlandsk nummer. Svindlerne vil du skal ringe tilbake til dyre utenlandske numre. Hvis du ikke forventer en samtale fra utlandet, trenger du ikke ringe tilbake.

Kontakt:

DNB: DNB Kundeservice 915 04800

Telenor: Kundeservice 915 09000
Les mer om digital sikkerhet på:
https://www.telenor.no/sikkerhet/

Politiet: Ring 02800
Ved behov for øyeblikkelig hjelp ring 112
www.politiet.no