Hvordan unngå å bli lurt i hverdagen?

Litt om vanlige svindelmetoder vi kan møte i hverdagen, og noen enkle metoder for å avdekke og håndtere svindel.

Stein Stegen

Svindel er ikke noe nytt

- Svindel har eksistert siden «tidenes morgen»
- Noen forskjeller fra tidligere tider
  - Trenger ikke å møte offerer «face to face».
  - Alle som bruker Internett er potensielle offer.
    - PC, nettbrett, mobil
  - Mye lettere å skjule sine spor, lav risiko for å bli avslørt.
  - Med potensielt veldig mange offer kan selv små beløp lønne seg.
  - Kan «automatiseres»

Ulike kanaler

- Svindler har mulige mange kanaler
  - E-post, SMS, Messanger, Facebook, Telefon, sholdersurfing (skulder sørfing)
- Kan sendes meldinger til ett stort antall mottakere samtidig,
  - i håp om at noen går på.
    - (Samme prinsipp som uadressert reklame.)
- Phishing, «automatisk» mot mange brukere samtidig
- Spear Phishing, mer målretter mot spesielle grupper
  - «Olga» svindel (personer med «gamledagse» navn)

Svindlere spiller på

- Frykt, trusler.
- Fristelser (typisk penger eller kjærlighet).
  - Grådighet.
- Tillit, utnytter noe eller noen vi stoler på.
  - Autoriteter
- Nysgjerrighet
- Manglende beredskap hos offeret

Vanlige misforståelser

- Det vanlig å tenke:
  "hvorfor skulle noen være interessert i meg?"
- Vi har jo virusprogram og brannmur
  - Maskinen eller program kan ikke stoppe oss når vi selv velger å gjøre «dumt».
  - Går etter det svakeste ledd, personen bak «tastaturet»

Hva er de ute etter

- Ikke ute etter deg som person.
  - Men dine penger, eventuelt identitet.
  - Kan bruke dine kontaktlister for videre angrep.
- Hvordan
  - Sosial manipulering og kontroll.
  - Programvare for overvåking og manipulering av aktivitet på PC og mobil.
- Hvorfor
  - Kontroll over din aktivitet for å berike seg selv

Ville du gått på?

- Det er lett å tenke «dette hadde ikke jeg gått på!».
- Det benyttes psykologi for å manipulere og stresse deg.
- Det kan være vanskelig å oppfatte at det er svindelforsøk.
  - Svindlere er veldig flink med sosial manipulering.
  - Prøver å stresse deg. «Superselger»
  - Gir deg liten mulighet for å tenke selv. Prater hele tiden, «tekno babbel»

Eksempel på fristelser

- Vunnet stort i konkurranse du ikke har deltatt i.
  - kan lure fra deg både personlig og betalingskortinformasjon.
  - Hvor skal premien sendes, bankkonto
- «UNIKT TILBUD», «BARE FOR DEG»
  - for å få deg på «kroken».
  - du blir beæret av å få «eksklusive» tilbud.
- Veldig god avkastning på investeringer.
  - Kryptovalutta

Teknisk informasjon som påskudd

- Selv det spilles på psykologi, brukes ofte tekniske elementer for å forsterker psykologien.
  - Telefon fra «Microsoft», eller andre som påstår at det er funnet virus eller feil på utstyret ditt.
- Systemene sårbare for
  - Brukerfeil.
  - Feil «Bugs» i programvare.

Nettbutikker

Nettbutikker

- De fleste nettbutikker er seriøse.
- Der en normalt ikke farlig å handle på nett.
- Her kommer noen punkter for å «flagge» mistenkelige butikker.

Nettbutikker

- Er et tilbud for godt til å være sant, er som oftest usant.
  - Er priser omtrent som i andre butikker?
  - Veldig stort, generelt og mangfoldig utvalg
- Store mengder positive omtaler
- Sjekk opplysninger om nettbutikk før du kjøper noe
  - Feks https://www.trustpilot.com
  - Har nettstedet/butikken vært i drift lenge?
    - Søk på butikknavn og omtaler.
  - Kontaktinformasjon, oversiktlige returregler.

Nettbutikker

- Noen «Røde» flagg
  - Annonser via Facebook
  - Bare positive omtaler
  - «Utrolig» lave priser
- På Norsk,
  - Mangler norsk kontakt info
  - Ikke informasjon om eiere
    - momsregister
    - Ikke besøkadresse
- Bare betaling med kort
- Betalingmuligheter
  - Debetkort
  - Kredittkort
  - Vipps
  - Klarna
  - Pay-Pal

Ikke svindel, men…

- Tjenester vi ikke trenger
  - Forsikring ved kjøp. Hva dekker vanlig innboforsikring?
  - Avbestilling forsikring. Dekkes normalt av vanlig reiseforsikring.
- Kjøp av strøm, telefon eller andre abonnement på gata.
  - Forsikring mot bortfall av arbeidsinntekt. (Pensjonist)
  - Får du telefon om kjøp av strøm, forsikring eller andre abonnent
    - Si tydelig «NEI», og «Ikke interessert» så legger du på.
    - Skulle du likevel få tilsendt kontrakt, få hjelp stoppe den snarest.
      - 10 dagers angrefrist

Sider for bestilling av reiser

- Det er mange sider som samler informasjon om og tilbyr.
  - Flyreiser, Hotell, Leiebil osv.
  - Sidene er seriøse, men
    - Ofte blir du videresendt til andre nettsider
    - Hvem har juridisk ansvar bestillingen?
- Spørsmål
  - Hvem dekker utgifter ved kansellering?
  - Hvem skal du klage til dersom noe går «galt»?
  - Det er viktig å sette seg inn i alt med «liten skrift»

Noen generelle råd for å sikre seg mot svindel.

Pass godt på deg selv på nettet

- Stopp opp, tenk deg om før du klikker på noe, eller oppgir informasjon til andre.
- Ikke opplys personnummer selv om du blir bedt det via e-post, SMS eller telefon.
  - Ikke oppgi betalingskortinformasjon ukritisk på nett.
    - Har du oppsøkt stedet som ber om slik informasjon?
  - Banker, forsikringsselskaper osv sender ikke ut forespørsler om viktig informasjon gjennom e-post eller tekstmeldinger.

Pass godt på deg selv på nettet

- Får du e-post eller SMS fra bekjente eller firma med krav om å gjøre noe, ring for å bekreftet at dette er reelt.
  - Spesielt dersom du ikke har kontaktet vedkommende først.
- Det er lett å bli usikker, og er du i tvil så spør noen.
  - Snakk med en venn, noen i familien eller nabo.
  - Her gjelder prinsippet: «Ikke la tvilen komme tiltalte til gode»
- Vær minst like forsiktig og tilbakeholden med å gi opplysninger om andre som om deg selv.

Noen tegn på at noe er galt!

- Du blir kredittvurdert uten å forstå hvorfor.
  - Ta straks kontakt med den som vurdere deg, meld fra at du ikke har gjort noe som krever kredittvurdering.
- Feil tid siden innlogging i banken.
- BankID ber om bekreftelse «ut av det blå»
  - Ta kontakt med banken for å avklare hva som skjer
  - Uforståelige kontobevegelser.
  - Hold oversikt over saldo

Vanskelig å avsløre

- Ikke tro at svindler er lette å avsløre på dårlig design, dårlig norsk eller usannsynlig innhold.
  - Dagens svindler er svært proft utformet.
- Ikke vær for snar på nett, tenk deg om når du opplever uventet eller merkelige ting.

- Lev etter prinsippet: "**Stopp - Tenk – Klikk**"

Førstelinje «forsvar» 1, Betaling

- Stopp, tenk. Still spørsmål!
- Er dette noe jeg forventer skal komme?
  - Har jeg gjort noe som kan forklare dette?
  - Er dette normalt oppførsel fra avsender?
- Har jeg, eller har hatt, kundeforhold, medlemskap?
  - Blir jeg normalt fakturert herfra?
  - Har jeg betalt to ganger? Sjekk i banken!
  - Dobbel betaling blir ikke «inndratt»,

Førstelinje «forsvar» 2, Epost, SMS

- Stopp, tenk. Still spørsmål!
- Stemmer retur epost adressen eller linken med påstått avsenders?
- Spiller dette på følelser og tidspress.
  - Stresser dette meg. (Ta en kopp kaffe/ Trekk puste, tell til 10)
- Hvorfor
  - vinner jeg i ett lotteri jeg aldri har hørt om?
  - skal noen jeg aldri har hørt om gi meg penger?

Førstelinje «forsvar» 3, Epost, SMS

- Stopp, tenk. Still spørsmål!
- Ikke trykk på lenker i epost eller SMS.
  - Dersom det ser ut som om meldingen er fra noen du har kundeforhold til:
    - Bruk bokmerke du har lagret.
    - eller skriv adressen direkte i nettleseren.
  - Ikke åpne vedlegg fra tilfeldige avsendere.
  - Ikke bruk «unsubscribe/avmeld», da viser du at eposten din er aktiv.
  - Send useriøse epost til SPAM mappen, slett SMS umiddelbart.

Førstelinje «forsvar» 4, Telefon

- Stopp, tenk. Still spørsmål!
- Telefon fra Politi, bank eller andre.
  - Be om navn og tlfnr til vedkommende for å ringe tilbake.
    - Dersom vedkommende advarer deg om å ringe tilbake, eller nekter å oppgi kontakt info, avslutt samtalen med en gang.
    - Dersom vedkommende oppgir tlfnr, ikke ring dette. Bruk «Gule sider» eller institusjonens hjemmeside.
    - Det er ingenting som haster så mye at du ikke har tid til å ringe tilbake.
- Sjekk nr på «Gule sider» ellet telefonterror.co.no
- Seriøse aktører vil aldri ringe deg for å be om BankID, brukernavn, passord osv.

Førstelinje «forsvar» 5, skulder sørfing

- Stopp, tenk. Still spørsmål!
- Personer står sitter rett bak deg når du bruker pinkode i butikk, minibank osv.
  - Ofte er det nok å snu seg å se litt «hardt» på vedkommende.
- Hjelpsomme personer når du skal bruke minibank.
  - Avslå slik hjelp, hev stemmen om de ikke flytter seg, skap oppmerksomhet.
  - Ikke kast minibank utskrifter i offentlige søppelbokser
- Ikke legg ut bilder av billetter på sosiale medier.

Hvis du tror du er svindlet

- Ikke vent og se om det går bra.
- Ikke gå i dialog med svindleren.
- Kontakt banken, kortselskap øyeblikkelig
  - Sperr alle kort.
- Endre passord på viktige nettsted.

Hvis du tror du er svindlet

- Uansett type svindel, på nett eller andre steder, anmeld til politiet.
  - En anmeldelse er nødvendig for å kunne rydde opp i konsekvensene av svindelen.
- Fortell familie/venner at du er svindlet.
  - Du kan bli misbrukt av svindlere for å angripe andre.
- Kontakt hjelpetjenester som slettmeg.no