
Sikkerhet
på nett
Digihjelpen kurs

# Nettfiske (phishing)

**Nettfiske** (phishing) er en teknikk for å fralure deg passordet ditt, ellerannen opplysning om deg. Med andre ord "fisker" svindlerne etter ditt passord/opplysning.

Dette skjer ved at du blir satt i en situasjon der du føler, eller tror, at du må oppgi denne informasjonen.

Svindleren utgi seg for å representere en tjeneste, og prøver å lure fra deg ved at de:

- **Ringer** deg opp
- Sende deg en **e-post** eller **tekstmeldinger** som direkte eller indirekte ber om disse opplysningene
- Lage **falske nettsider** med innlogging som er kopier av de ekte nettsidenes design og innhold, da kan de lese passordet ditt

Får du slike henvendelser så ikke svar direkte, snakk gjerne med noen eller kontakt/ring den tjenesten det tilsynelatende skal være.

# NETTFISKE (PHISHING)

I alle tilfellene nevnt på forrige side skal du **ikke oppgi passord.**

Blir du ringt opp så avslutt samtalen.
Får du e-post eller tekstmeldinger der du blir bedt om å oppgi passord skal du ikke svare.
E-post systeme har som regel en folder for søppelpost, legg den der.

**Det er med andre ord ingen som med ærlige hensikter noen gang spør om passord** gjennom telefon, e-post eller tekstmeldinger.

# Hva er gode passord?

**Hvilke passord er det lurt å unngå?**

Passord kan også bli «hacket» av svindlere. Svindlere bruker egne «passordprogrammer» slik at de vha. teknikk får tak i passord. «Passordprogrammene» tar ofte utgangspunkt i ord/bokstaver fra ordlister, derfor skal du **ikke bruke et enkelt ord som passord** som du vet en kan finne der.

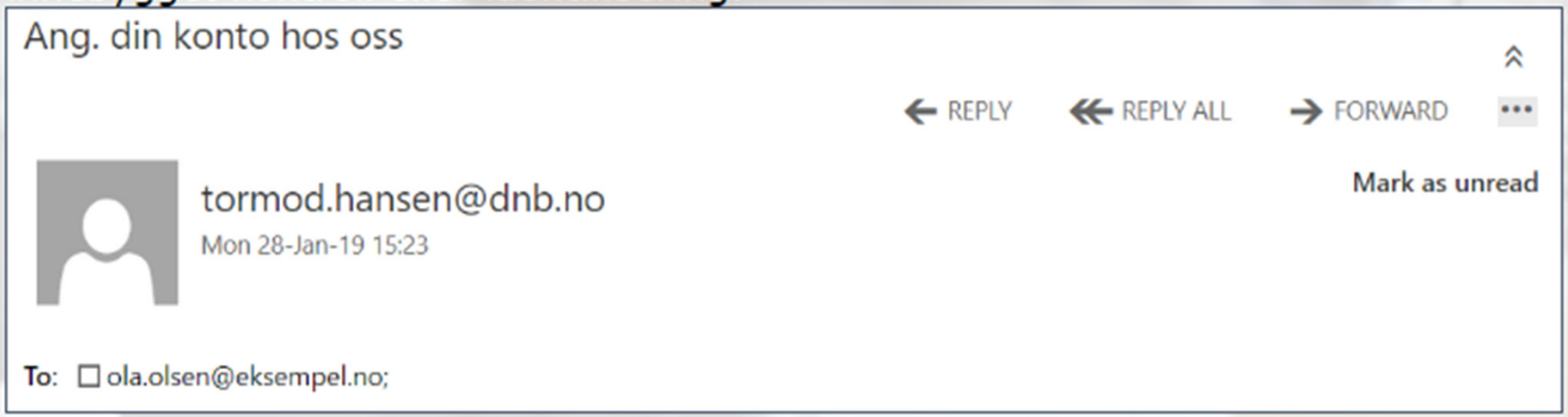
Ved valg av passord:

- I stedet for ord velg en setning, eks. fra en sang eller regle du lett husker, slik at antall bokstaver og tegn tilsammen er mer enn 16
- Bruk både små og store bokstaver i tillegg til spesialtegn og tall
- For å huske passord skriv de ned på et ark som du lagrer på et sikkert sted

I slutten av denne kursmodulen viser vi til linker på nettvett.no med råd om passordhåndtering.

# FORFALSKNING AV AVSENDER

I introduksjonsmodulen omtalte vi forfalskning av avsender. Dette er et så viktig budskap at det gjentas.
**Avsender på en e-post er svært lett å forfalske**, og det finnes ingen innebygget kontroll eller identifisering.




Du kan altså **aldri stole på at avsender av en e-post er den en gir seg ut for.** Stemmer ikke innholdet med hvordan avsender vanligvis formulerer seg, så gjør en ekstra **kontroll eks. via telefon**. Mao. tenk deg om hvis innholdet i e-posten "skurrer"

# HVORFOR FÅR JEG E-POSTSVINDEL?

Svindlere samler e-postadresser slik som **selgere samler telefonnummer**.

Jo flere steder du oppgir e-postadressen, jo større sjanse er det for at e-postadressen kommer i svindlernes besittelse. Typisk ved at tjenester **selger adresser**, at de blir hacket eller at de er satt opp for å samle adresser.

Du kan redusere sannsynligheten for å få e-postsvindel ved å være litt skeptisk til hvor **du oppgir e-postadressen din**. Spesielt **konkurranser og undersøkelser** er noe som lett bør unngås.

# SVINDELINNHOLD

E-post benyttes ofte til tradisjonelle svindler der det ønskes å komme i kontakt med deg som mulig offer.
Følgende innhold er svært vanlig i svindler:

- **Lånetilbud**
- **Forretningsmuligheter og investeringsmuligheter**
- **Utdeling av gaver og fristene konkurranser**
- **Arv og kontakt fra påståtte advokater**
- **Jobbtilbud**
- **Kjæresteforhold og pornografisk innhold**
- **Salg av tabubelagte varer** (potensmiddel, helsekost osv.)
- **Gode tilbud på luksusvarer** (Rolex, mobiltelefoner osv.)

E-post med slikt innhold bør medføre grunnholdningen din om at det kan være en svindel. **Tenk deg om for hva du gjør videre.**

# SIKKERHETSVERKTØY

Som nevnt i introduksjonen til dette kurset er de fleste farer i dag basert på **sosial manipulasjon**.

Vi nevnte også at din **egen vurdering** ofte er viktigere og mer effektiv enn tekniske verktøy.

Vi skal likevel ta for oss noen **sikkerhetsverktøy**, for det er jo ikke slik at disse er uten effekt. Vi bør som minimum ha:

- rutiner for **oppdatering** av utstyr og systemer
- gode rutiner for **sikkerhetskopiering (backup)**
- **søppelpostfilter** for din e-post
- **antivirusprogram for din PC**

Installsjon og oppsett av det som er nevnt over kan være for teknisk for mange, i så fall få hjelp av de du vet kan dette, der er viktig at dette er i orden.

- Hold programmer og apper på datamaskin og mobil **oppdaterte** til nyeste versjoner, **si ja til automatisk oppdateringer**
- Sørg for å ha et **nyere antivirusprogram med en aktiv oppdatering på din PC** (kan kreve et aktivt abonnement)
- Meldinger og nettsider som slipper gjennom. antivirus og filtre er **ikke nødvendigvis trygge**
- Det er fort gjort å glemme å ta sikkerhetskopier. Sørg for å ha **gode rutine eller automatikk, lurt å ta sikkerhetskopi av utstyr du skal ha med på reise**
- Sørg for å ha en **sikkerhetskopi av all informasjon og bilder** du ikke vil miste
- **Oppbevar sikkerhetskopier adskilt fra maskinen** der originalen ligger.


Terminal i bibliotek


På hjemmesidene

Her finner du hele sikkerhetskurset eller  skriv inn:

https://nettvett.no/kurs/sikkerhet-for-seniorer/

i din nettleser og legg den som favoritt.