«Banken ringer»

«Dere har blitt svindlet,
hjelp er på vei ….»

En aktuell sak fra VG 16.10.24

VG onsdag 16. oktober 24

Proffe, fryktboble og glade for hjelp

- Oppringt fra «egen» bank → dere ha blitt svindlet
- To unge menn kom for «å hjelpe» dem
- Hun: Melding fra Statens Vegvesen, den hadde en lenke til Altinn som hun trykket på. Falsk nettside, ingen personer var registrert
- Hun ringte OBOS-banken og sperret kortene sine
- Hun blir oppringt fra «sikkerhetsavdelingen etter en time. «Sikkerhetsmannen» han sier at de har virus på nettverket. Mannen får telefonen, de er «sikre» på at de snakker med banken
- Han burde overføre egne penger til «sikker konto», han blir bedt om å logge på nettbanken på PC-en. Mennene fortalte ham hva han skulle gjøre og de styrte musa ….
- Hun blir bedt om å vippse penge til mannen sin
- De får besøk av to «teknikker» for å sjekke ruter og kredittkort, paret har lagt fram kredittkortene sine med post it lapp med saldo og pinkode

NettVett.no

- Han fatter mistanker, de var for unge til å jobbe i bank
- Han ringer banken og de bekrefter at en svindel har funnet sted
- Svindlerne klarte tappe kortene for over en million kroner, men sikkerhetssystemene i bankene gjør at de til slutt får igjen alt som tatt ut

Hva gjør du – telefonsvindel

- ***Legg på*** hvis du får en «rar» samtale
- ***Ring banken*** på deres offisielle nummer med en gang og fortell
- ***Ring politiet på 112*** og fortell hvis fremmede forsøker å komme inn gjennom døra di
- ***Pass godt på BankID og passordet ditt***, INGEN skal se disse

Hva gjør du – SMS- eller e-postsvindel

- Oppgi aldri BankID eller passord til andre
- Sjekk avsenders telefonnr eller e-postadresse skikkelig
- Unngå å klikke på lenker direkte i SMS eller e-post, sjekk avsender ved å benytte nettsiden

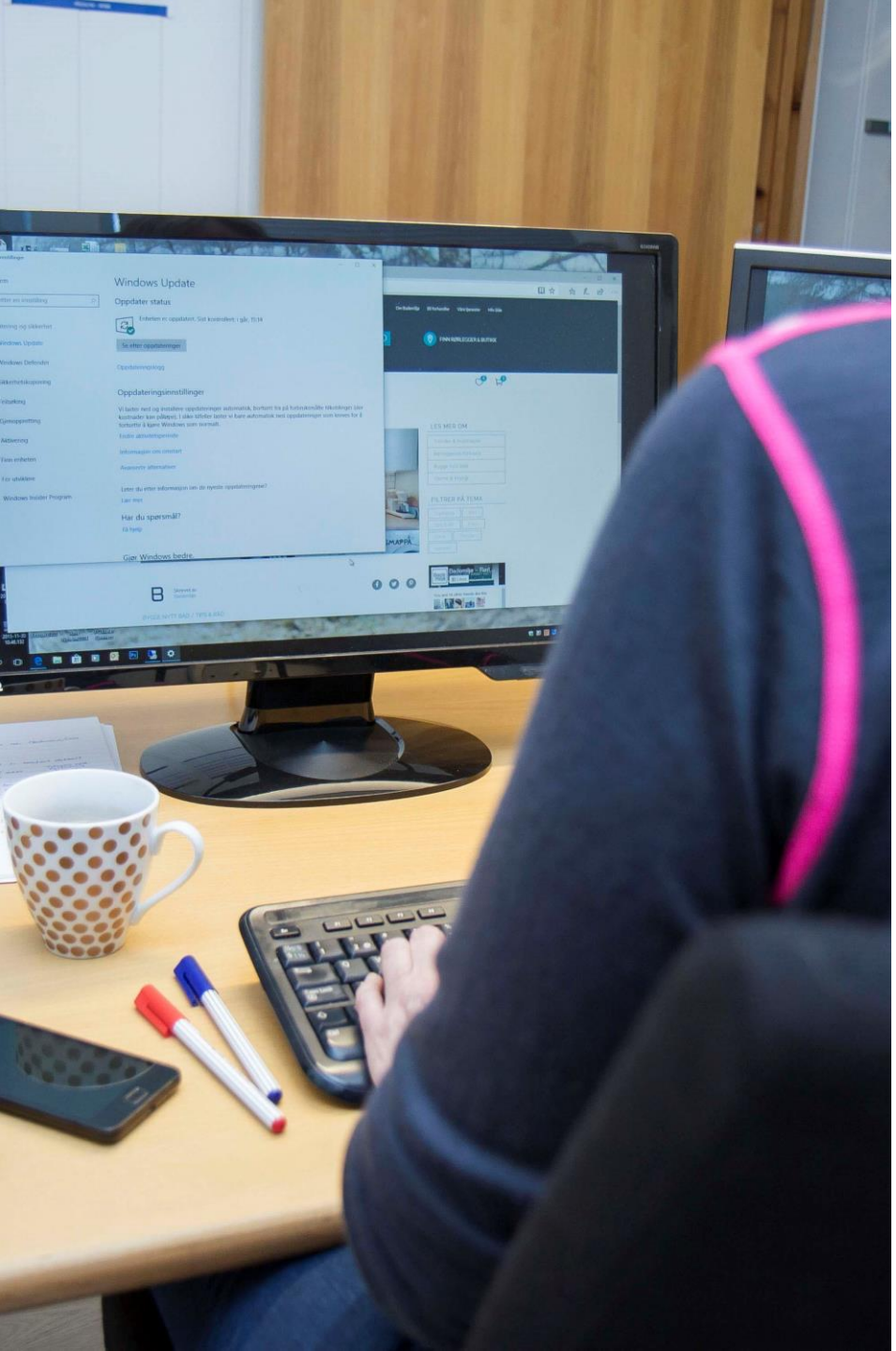
NettVett.no

Informasjonssikkerhet for seniorer

«Brukerkontoer»

Kilde: Norsk Senter for Informasjonssikring

NettVett.no



Sikre din brukerkonto på internett

Ved hjelp av internett kan du trekke tjenester inn på ditt eget kjøkkenbord.

I tillegg til å skaffe deg all verdens informasjon kan du benytte deg av offentlige tjenester, handle på nett, bruke tjenester fra banker og forsikringsselskaper eller tjenester fra andre service institusjoner.

Når du bruker disse tjenestene må du først opprette en brukerkonto så du tilkjennegir at du er deg, med riktig navn, adresse, og andre opplysninger om deg.

Denne kursmodulen gir deg råd hvordan du kan sikre dine opplysninger som er knyttet til dine brukerkontoer, slik at dine rettigheter og opplysninger ikke blir misbrukt.

NettVett.no

Passord og pinkode på PC/nettbrett/mobil

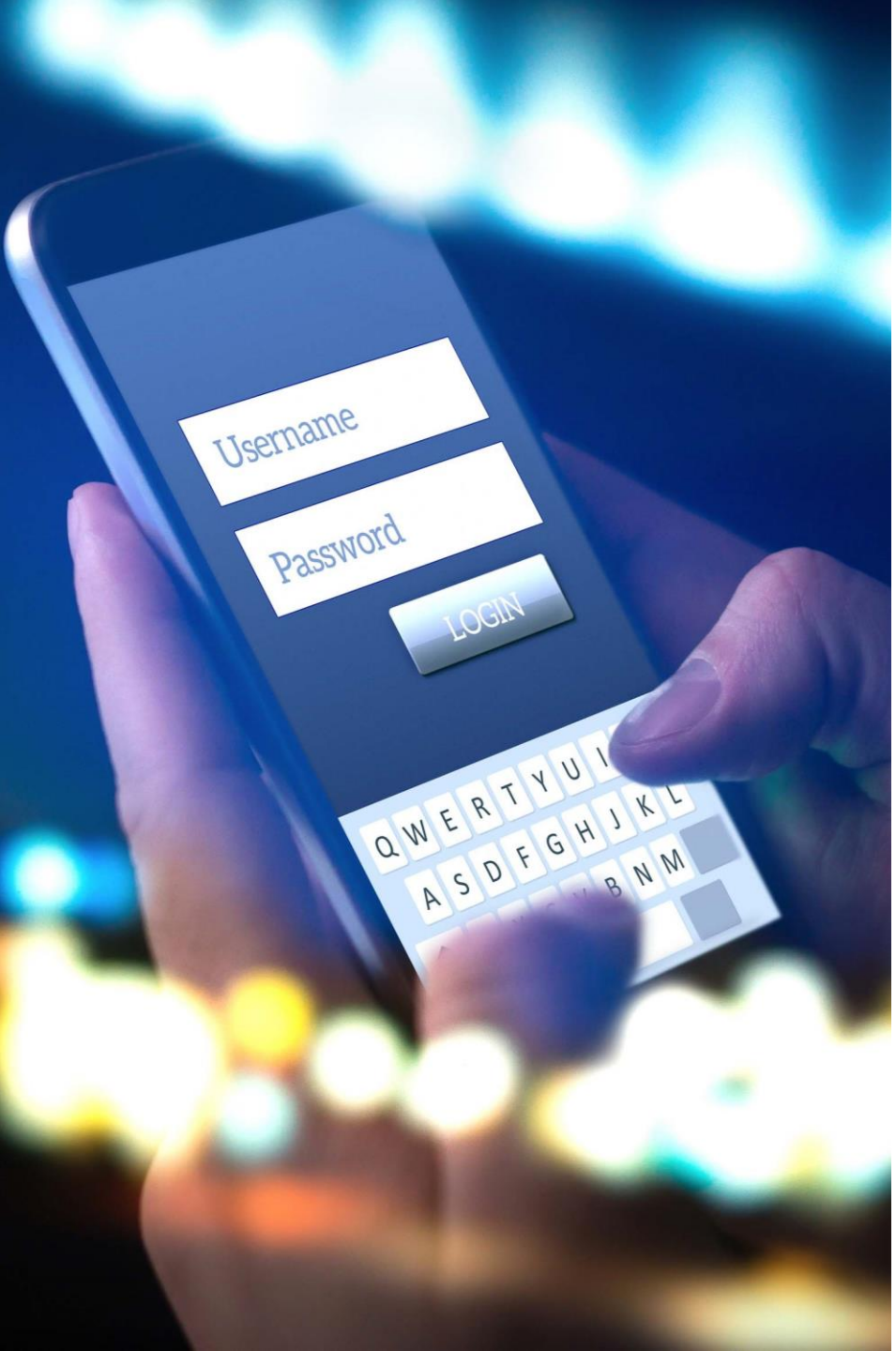
Kommer din mobilen, nettbrettet eller PC'en over på uvedkommendes hender, kan utstyret brukes til å svindle deg.

Det er derfor viktig når du setter opp dette utstyret at ***du legger inn passord for å starte opp PC'en***, eller pinkode for å starte nettbrett og mobil.

Skulle du miste eller forlegge utstyret, vil det da ikke kunne bli misbrukt om det kommer over på uvedkommendes hender.

Legger du fra deg PC, nettbrett eller mobil, der andre kan få tilgang til dette utstyret, så husk på å ***låse utstyret slik at en kun kan åpne det med passordet eller pinkoden.***

NettVett.no



Passord på programmer og tjenester

Alle brukerkontoer er beskyttet av passord som **bare du skal vite hva er.**

Hemmelighold av passordet er det som sikrer at bare du skal kunne bruke tjenester i ditt navn og med dine rettigheter.

Passord knyttet til en tjeneste du bruker lagres normalt sikkert hos tjenesteleverandøren, for å unngå at andre kan bruke din brukerkonto med ditt passord.

Passord kan likevel komme på avveier. Videre i denne kursmodulen viser vi hvordan det kan skje, og hvordan du skal beskytte deg.

Nettfiske (phishing)

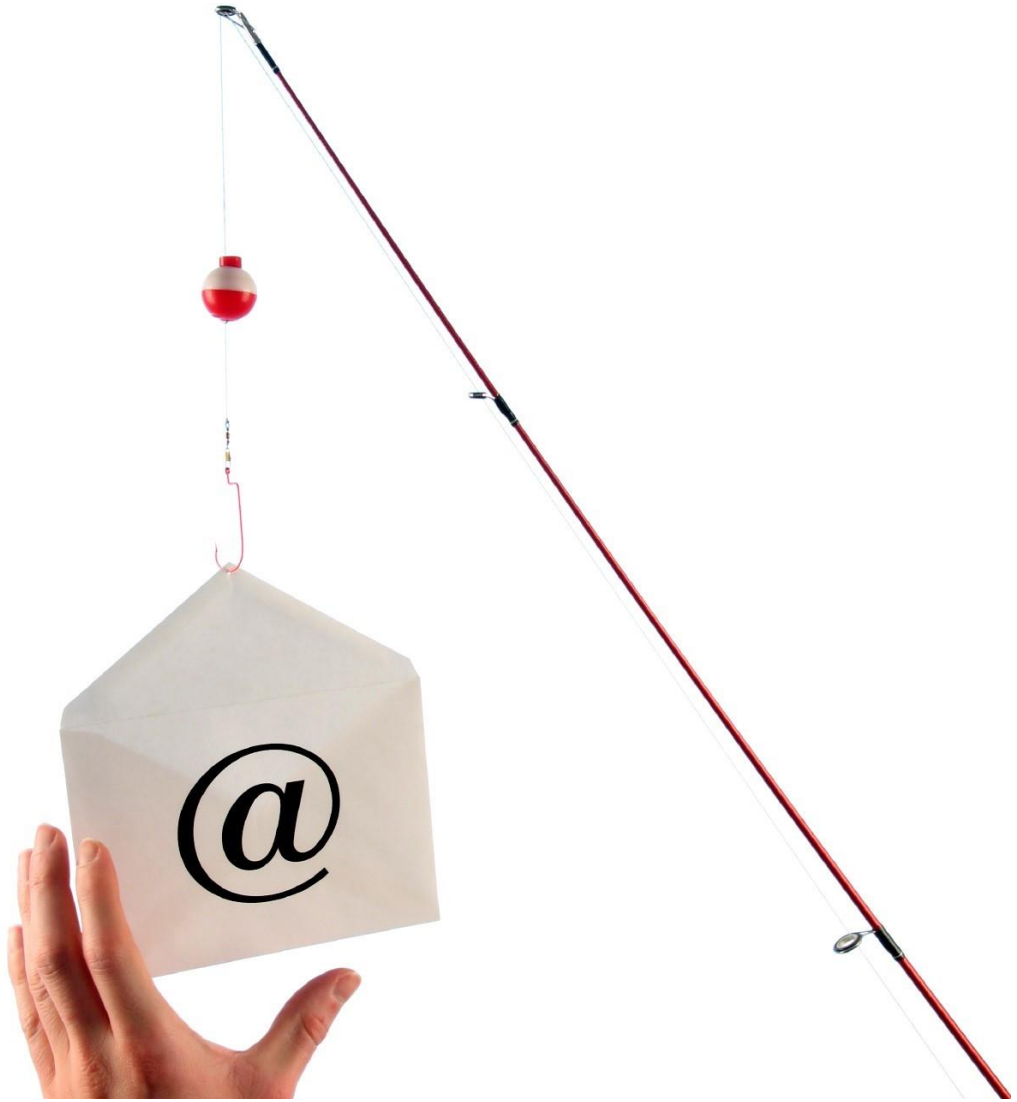
Nettfiske *(phishing) er en teknikk for å fralure deg passordet ditt, eller annen opplysning om deg.* Med andre ord "fisker" svindlerne etter ditt passord/opplysning.

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

Svindleren utgir 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.

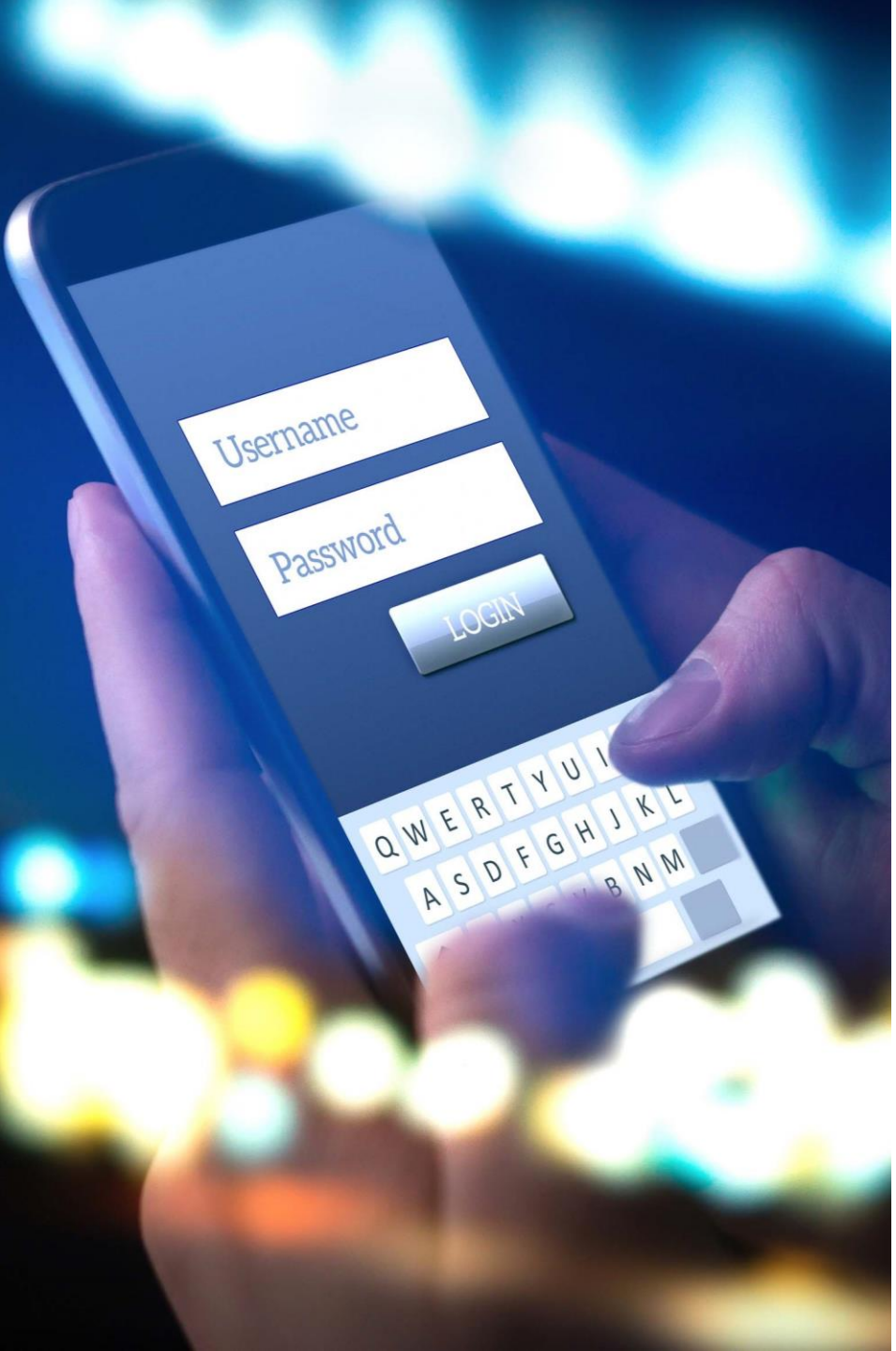


Nettfiske (phishing)

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

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

NB! **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.

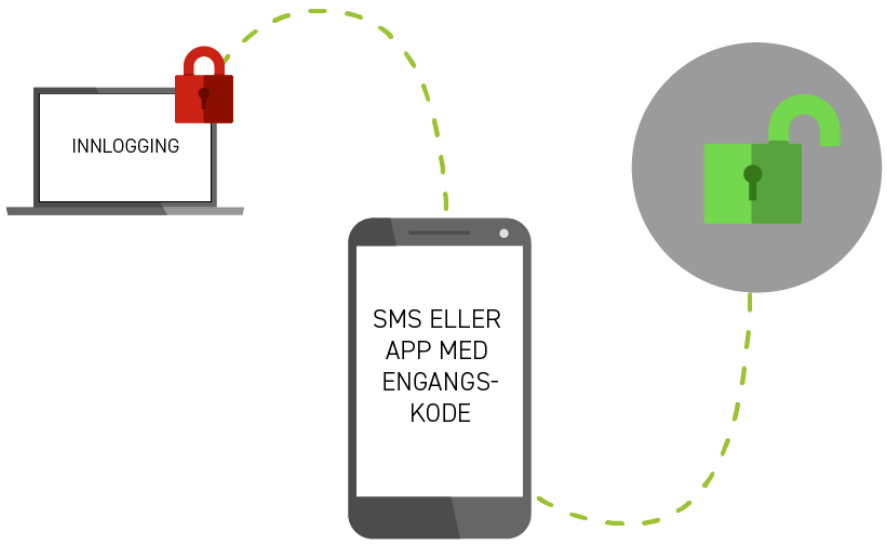
Ved valg av passord:

- *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.

NettVett.no

Sikre din brukerkonto med totrinnsbekreftelse



Fordi passord både kan lures fra deg, og at det finnes passordprogram som teknisk sett avslører ditt passord, har leverandører **innført totrinnsbekreftelse for å være sikrere på at det er du som logger deg inn på din tjeneste. BankId er en slik metode.**

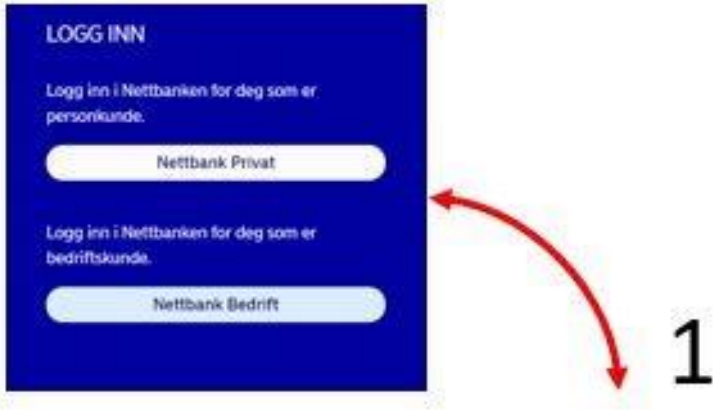
1. Når du logger deg inn, taster du inn ditt brukernavn og passord, da er du ferdig med det første innloggingstrinnet.

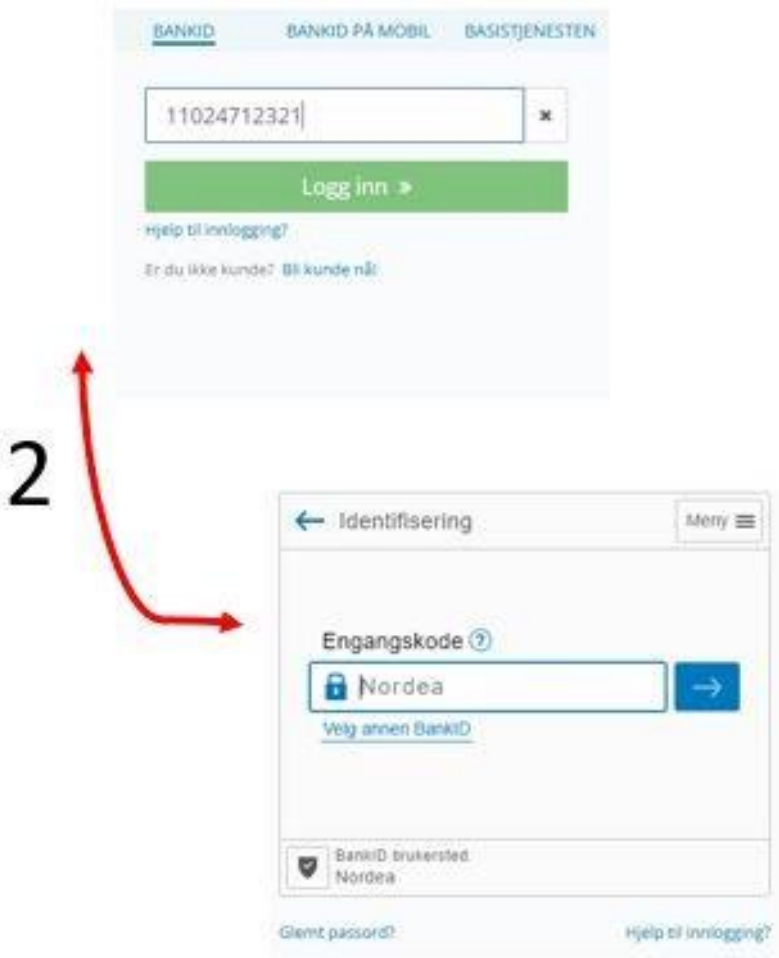
2. Det andre trinnet er at det sendes en kode til din mobil eller kodebrikke som du taster inn i et anvist felt i innloggingen.

3. Når du har tastet inne denne koden, blir du logget inn.

Mange leverandører tilbyr totrinnsbekreftelse som du kan sette opp selv.

NettVett.no





Bank ID er et eksempel på totrinnsbekreftelse

Når du logger deg inn mot din bank, brukes BankID for å være helt sikker på at ***ingen andre enn deg kan logge seg inn i dine bankkontoer.***

Dette gjøres ved at du på forhånd hos banken *har registrert din mobil eller kodebrikke*, slik at banken kan sende koden for pålogging til din kodebrikke eller mobilen, som du deretter taster inn i innloggingsbildet.

Banktjenester med BankID er en sikker måte å logge seg inn på.

NettVett.no

Sikre din brukerkonto med totrinnsbekreftelse

Hvorfor er totrinnsbekreftelse sikrere?

- Hvis en svindler har fått tak i ditt brukernavn og passord, har han det første trinnet i påloggingen.
- Når du deretter, som andre trinn, får tilsendt koden du skal taste inn på din kodebrikke eller mobil er det **du som har kodebrikken eller mobilen i hånda og ikke svindleren**

NettVett.no

Sjekk korrekt nettadresse (URL) for tjeneren

En kjent måte å svindle på er å *opprette nettsider som ser identisk ut som den tjenesten du skal inn på, såkalte* ***falske nettsider*****.**
Disse ser ut som siden du vil inn på, men er i realiteten opprettet for å svindle brukere.

Måten å lure deg på er at du får beskjed om å klikke på en link i en mail eller SMS, og så fører denne linken deg til den falske siden.

På denne siden kan du bli fralurt brukernavn og passord.

Da kan svindleren opptre som deg i ettertid, svindle deg eller misbruke dine rettigheter som hører til tjenesten som du tror du har logget deg på.

NettVett.no

Sjekk korrekt adresse for tjeneren

Når en svindler setter opp en falsk side brukes ofte ***adresser som ser korrekte ut***.
Poenget med å sette opp falske sider er å lure fra deg brukernavn og passord.
Du tror du logger deg inn på den riktig siden, men svindleren har satt opp sida du egentlig kommer inn på slik at han kan lese av ditt brukernavn og passord når du taster det inn.

I dette eksempelet er bokstaven o byttet ut med tallet 0.

Gjør det til en vane å sjekk om adressen til nettsiden du skal inn på er korrekt *med å se på nettadressen oppe i adressefeltet.*

NettVett.no

Sikre din brukerkonto

Finn utfyllende tips på nettvett.no ved å se på veiledningene under:

Sikker pålogging.
Slik lager du sterke passord
Oppskrift for å sette opp totrinnsbekreftelse for noen tjenester
Hvordan oppdage phishing, nettfiske
Eksempel på SMiShing, nettfiske vha. SMS

Microsoft Office/Office365 er mye brukt.

Microsoft ber oss bruke appen **Microsoft Authenticator** for sikker innlogging**,** du kan lese mer på

https://support.microsoft.com

NettVett.no