Digital sikkerhet for seniorer

Seniornett
Sammen for digital mestring

Innholdsfortegnelse

Innledning

Digital sikkerhet er et vidt begrep og kan omfatte mye. Det viktigste er å unngå å bli svindlet og unngå at noen stjeler personlig informasjon.

Dette heftet beskriver hvordan du kan beskytte deg digitalt. Det viser eksempler på noen av metodene svindlerne bruker og gir noen tips til hvordan du kan unngå å bli svindlet. Heftet inneholder også enkle råd til deg som vil sikre dine data (for eksempel dine bilder) slik at du ikke mister dem ved et uhell.

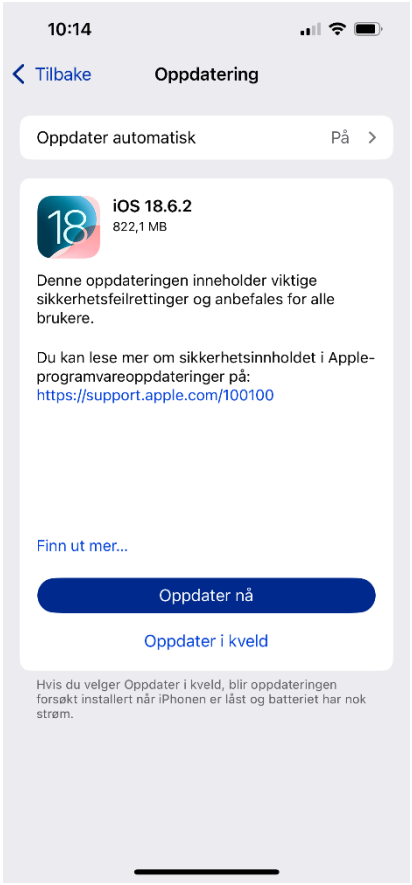
Enkle regler for å beskytte seg digitalt

1. **Sjekk om din enhet er oppdatert**

Med «enhet» menes her PC, nettbrett eller mobiltelefon. Eller i prinsippet hvilken som helst annen digital «dings» (for eksempel smartklokke, smart-tv).

Alle enheter har en programvare som må oppdateres med jevne mellomrom. Oppdateringer er viktig fordi de retter opp feil i programvaren og kan sikre enheten mot digitale angrep. Grunnen til at det stadig kommer nye oppdateringer er kappløpet mellom nye svindelmetoder og sikrere programvarer.

Hvordan sjekker jeg om enheten er oppdatert?
På «innstillinger» i din enhet kan du se om det er en oppdatering tilgjengelig.



De fleste enheter gir et varsel når det er oppdatering tilgjengelig, men det er lurt å lære seg hvordan du sjekker om det er ventende oppdateringer på egenhånd.

Mange enheter er satt opp med «installer oppdateringer automatisk». Installer oppdateringer så snart de er tilgjengelige.

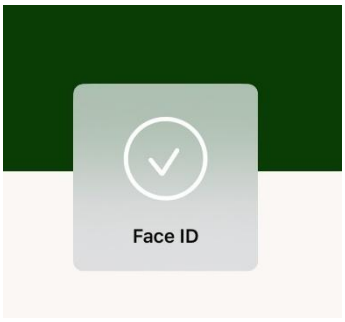
Er du usikker på hvordan du holder din enhet oppdatert? Ring datahjelpen i Seniornett.

Ha lås på mobilen

Det finnes ulike typer låser:

- Ansiktsgjenkjenning
- Fingeravtrykk
- PIN-kode.
- Mønster

Det enkleste å bruke er **ansiktsgjenkjenning**. Da behøver du bare å se på mobilen, så låser den seg opp. Dette må i tilfelle installeres på enheten din.



1: Face ID er det engelske uttrykket for ansiktsgjenkjenning.

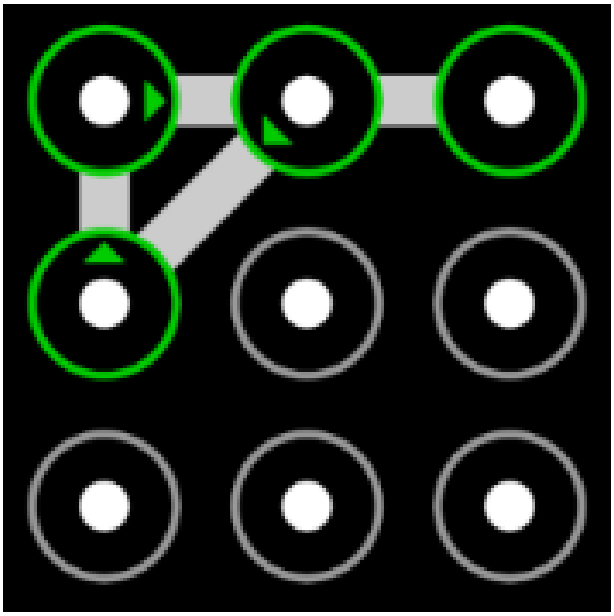
For lås med **fingeravtrykk** kan du registrere flere fingre, slik at den kan brukes også hvis du har fått et sår på fingeren.

Bruk av ansiktsgjenkjenning eller fingeravtrykk kalles biometri.

Det er ikke alle mobiler som tilbyr ansiktsgjenkjenning eller fingeravtrykk.

PIN-kode er en (vanligvis) 4 eller 6-sifret kode du velger, som skal tastes inn for å låse opp telefonen. Den må du også bruke dersom gjenkjenning via biometri ikke skulle fungere. PIN-koden må du altså ikke glemme!

Mønster betyr at du i en ramme med 9 prikker skal tegne et mønster. For eksempel slik:



(Her er mønsteret fra prikk2 til 4 til 1 til 2 til 3)

Du holder en finger nede på skjermen mens du tegner mønsteret.

Du velger altså et mønster som du klarer å huske.

Tid før mobilen låses

Det finnes innstillinger på din enhet hvor du kan legge inn hvor lang tid mobilen skal være ubrukt før den låses. Her snakker vi om antall sekunder eller (noen få) minutter.

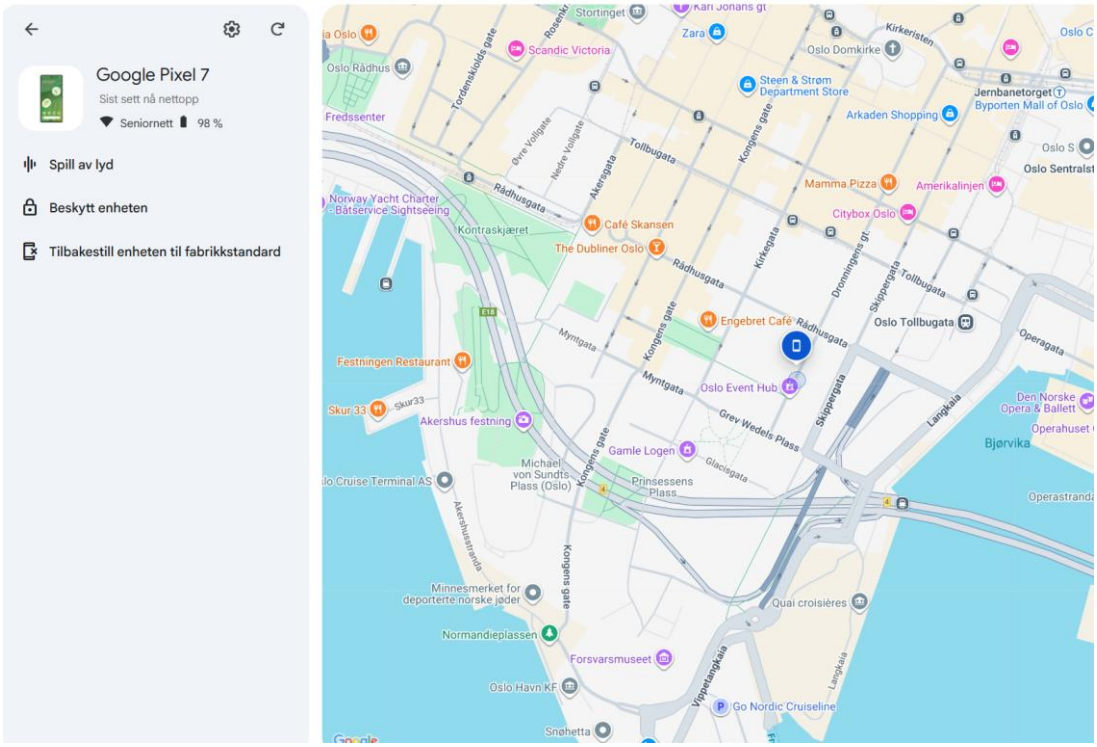
2. Ha en plan for hva du gjør dersom du mister telefonen din eller den blir stjålet

Undersøk på forhånd hvordan du sporer din mobil. Dersom den er på og er koblet til internett, kan du fra en PC eller nettbrett se hvor mobilen din er.

For iPhone går du inn på https://www.icloud.com/find. Du må logge deg inn med din apple-id.
På telefonen må du på forhånd ha slått på «Hvor er»:

For android-telefon gjør du dette ved å gå inn på https://www.google.com/android/find
Har du ikke logget deg inn med din google-konto vil du bli bedt om å gjøre det.

Et eksempel på hvordan det kan se ut for Android:



Du ser hvor telefonen er (det blå symbolet i kartet) og du ser at det er 3 ulike operasjoner du kan utføre:

- **Spill av lyd**
  Da vil telefonen «ule» i 5 minutter. Kjekt å gjøre når du eller din hjelper er i nærheten og skal finne den. Den vil «ule» selv om den er på lydløs.
- **Beskytt enheten**
  Da blir den låst og avlogget slik at andre ikke kan bruke den.
- **Tøm enheten**
  Da fjernes alt på telefonen og den tilbakestilles til fabrikkinnstillinger.

Dersom du har slått av mobildata på mobilen din, vil ingen av disse funksjonene virke. Derfor er det lurt å alltid ha mobildata slått på.

3. Vær bevisst hvordan du bruker passord

Passord kan være noe herk. De må huskes og brukes og de må være sikre. Men de er nødvendige i svært mange tilfeller for å beskytte dine digitale data.

Noen tips når det gjelder passord og pålogging:

- Bruk to-trinns pålogging der det er mulig.
  To-trinns pålogging betyr at du må ha 2 «nøkler» for å logge inn på et nettsted.
  Se eksempel og detaljer på neste side.
  Les mer om totrinns pålogging her: https://nettvett.no/2-trinns-bekreftelse/

- Ikke lag passord som er lette å gjette seg fram til for andre som for eksempel navnet + fødselsår til ditt barn.

- Lag gjerne et system som gjør at passordene til ulike påloggінger ser helt «tilfeldig» ut.
  Bruk en setning som passord. Så bytter du ut noen ord utfra hvilken nettside du er på.

- Vurder hvilke passord du bruker hvor
  - Ikke bruk samme passord overalt
  - Men ikke alle passordene behøver å være unike
  - Bruk unike passord der du har lagret sensitive data

- Husk de viktigste passordene, skriv ned resten.
  Det er smart å notere passordene i en bok eller på et ark.
  Legg arket på et sted hjemme som er trygt og som du husker.
  Oppdater arket når du bytter passord. Noen nettsteder krever at du bytter passord med jevne mellomrom.

To-trinns pålogging

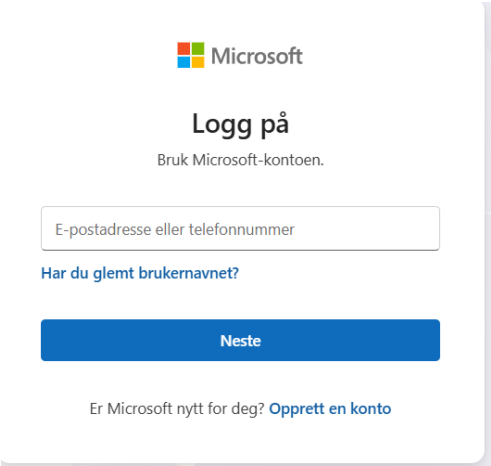
Ditt passord er nøkkel nr. 1.

Nøkkel nr. 2 er gjerne mobilen eller andre enheter som du må identifisere deg på.
På mobilen kan det være at du må inn i en app som viser en tallkode eller du må bekrefte med ditt fingeravtrykk eller sende svar på en SMS.

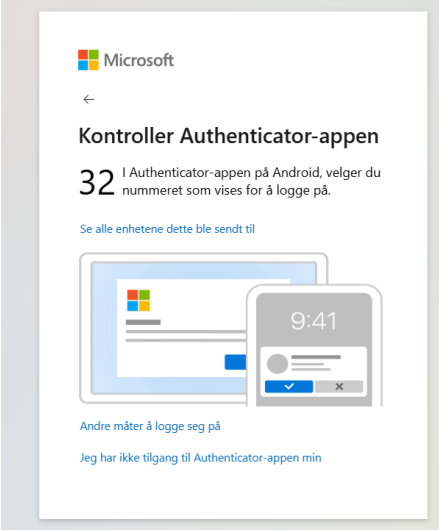
Bank-id med kodebrikke er et eksempel på to-trinns pålogging.

Eksempel på to-trinns pålogging når jeg prøver å logge deg inn på min side på Microsoft.com på en PC:

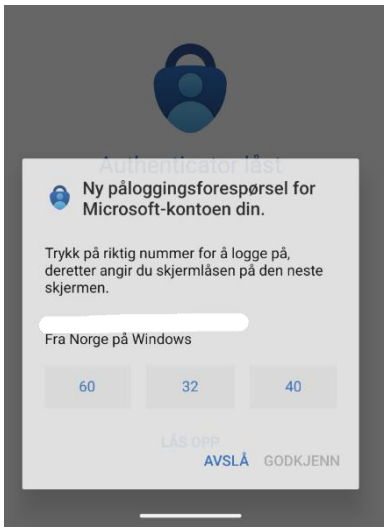
Først gir jeg inn mitt brukernavn (min e-postadresse):



Deretter kommer denne meldingen på PC-en:



På app-en på telefonen kommer denne meldingen:



Svindelprinsipper

Svindel er et forsøk på å lure noen til å gi bort informasjon eller gjøre en handling som fører til tap av penger eller anseelse.

Svindel eller bedrageri har eksistert i alle år. Men i den digitale tid har svindelmetodene blitt mer og mer avanserte.

Ved å klare å gjenkjenne de forskjellige metodene, ved å bruke sunn fornuft og ved å «holde hodet kaldt», kan du være bedre rustet for å unngå svindel.

Prinsippene som brukes for å forsøke å svindle deg på handler alle om manipulering og de fleste spiller på:

- Fristelse
- Frykt
- Tillit

Fristelse

Eksempel «Du er den heldig vinner av …….» -
Her får du melding om at du har vunnet eller er berettiget penger eller en annen gevinst. Typisk et lotteri som du ikke har deltatt i.

Hva bør du tenke og gjøre?

- Du kan ikke vinne i et lotteri hvor du ikke har deltatt.
- Ingen gir bare bort penger.
- Ikke la deg friste til å trykke på lenken som typisk følger med meldingen.
  Det er her svindelen begynner.
- Er du usikker på om det kanskje kan være reelt likevel, ta kontakt med avsender via en annen kanal (ring, men ikke bruk kontaktinfo som følger med meldingen. Ring via det offisielle telefonnummer).
- Ignorer meldingen og slett den!

Frykt

Du får melding om at noe fryktelig vil skje. Meldingen sier at du må utføre en handling veldig kjapt for å forhindre dette.

Det meldingen sier er at du må gå inn på et nettsted der du må oppgi personlige og/eller sensitive opplysninger. Eller betale et beløp.

Typisk:

- Oppringing om at noe er galt.
- Melding om at din enhet er infisert.
- Beskjed om at noen har filmet deg mens du ser på porno.
- Beskjed om at noen har tatt et kompromitterende bilde av deg.

Hva bør du tenke og gjøre?

- Ta det med ro. Det haster ikke.
- Gjør en vurdering hvor sannsynlig det kan være at dette er sant.
- Ikke svar på meldingen.
- Snakk med noen andre, ring gjerne Seniornett.
- Hvis meldingen gjentas og truslene virker reelle, kontakt politiet.

Årsaken til at svindleren sier at det haster er at du skal agere uten å tenke deg om.

Tillit

Du får melding fra en du kjenner eller stoler på, som ber deg om å utføre en handling. Eller du blir ringt opp av en du stoler på. Dette kan være noe som ser ut som:

- en melding fra Posten eller PostNord om at du må betale for å få en pakke levert.
- en melding fra banken om at noen prøver å stjele dine penger.
- en melding fra Politiet om at noen prøver å svindle deg.
- en oppringing fra Microsoft som sier at du har fått virus på din PC.

Det svindleren ber deg om å gjøre er gjerne noe som involverer penger. For eksempel at du må betale eller oppgi passord.

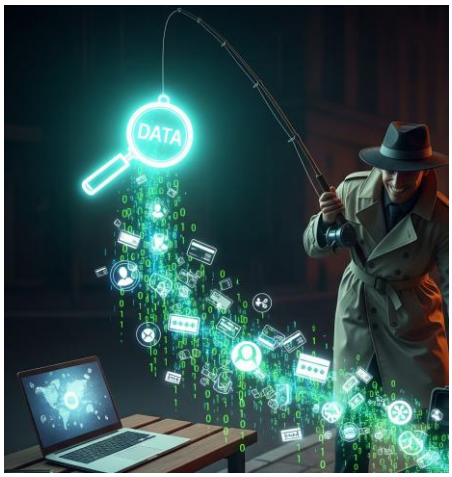
Svindleren vil spille på din følelse av at du stoler på vedkommende. Noen kan også bruke lang tid på å overbevise deg om at du kan stole på dem.

Hva bør du tenke og gjøre?

- Tenk deg om. Kan dette virkelig være sant?.
- Er det en lenke i meldingen som den ber deg om å trykke her, ikke trykk!
- Kontakt vedkommende gjennom en annen kanal (ring) for å sjekke hvor reelt dette er.
- Ring via offisielle telefonnummer, ikke det som eventuelt står i meldingen.
- Er du i tvil, ring Seniornett.

Svindelmetoder

Phishing



Dette er den mest brukte formen for svindel. Phishing er det engelsk ord for «fiske». Det innebærer at de prøver å «fiske ut» personlig informasjon fra den som skal svindles.
Det kommer som regel i form av en e-post eller en SMS.
Disse e-postene eller SMS-ene inneholder gjerne en lenke som fører til en falsk nettside. Nettsiden ser ut som nettsiden til en tilsynelatende pålitelig bank eller nettbutikk. Det handler for eksempel om at du har vunnet noe eller at du skal betale fra din bankkonto. Målet er å få tak i (fiske ut) personlige opplysninger som da kan misbrukes for å svindle deg.

Vennebedrageri

En såkalt bekjent kontakter deg i form av en e-post, en SMS eller en melding på Messenger, gjerne med begrunnelsen at han eller hun er i nød og ikke lenger har tilgang til pengene sine. Typisk er den såkalt bekjente på ferie i utlandet og har blitt frastjålet både bankkort og pass. Han/hun trenger penger for å komme seg tilbake til Norge og ber deg om hjelp.

Kjærlighetssvindel

Svindlere er veldig gode til å finne sårbarheter hos ofrene sine. For eksempel kan de spille på at du er ensom og singel. De vet at de oppleves godt og smigrende med pene ord og bekreftelser og vet akkurat hvilke knapper de skal trykke på. De holder kontakten med deg i lang tid, både via telefon eller meldinger.

Svindlerne utgir seg gjerne for å være utenlandske forretningsmenn, diplomater, misjonærer, hjelpearbeidere eller krigsveteraner. Fellesnevneren er ofte at de har en viktig jobb eller et oppdrag i utlandet som de skal gjennomføre. Dette sier de for å få din sympati.

Men det oppstår komplikasjoner, og snart kommer spørsmålene om penger. Det kan være en ødelagt mobil, eller at en slektning er blitt syk og trenger hjelp til å betale sykehusregningen.

Historiene kommer i mange varianter. Formålene fremstår som gode, noe du mer enn gjerne vil bidra til.

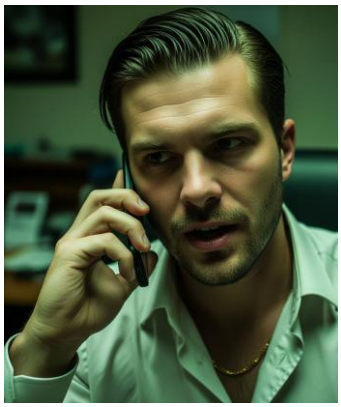
Svært mange av dem som blir svindlet på denne måten er kvinner. Ofrene er gjerne i starten av 60-årene, men svindelen kan ramme alle aldersgrupper og kjønn. Ved å dikte opp historier og interessante bakgrunner, fanger svindlerne oppmerksomheten din og prøver å smigre deg. De finner svakheter og utnytter følelser som ensomhet og sorg, eller et behov for bekreftelse. Over tid klarer svindlerne å overbevise deg om at dere har en genuin relasjon over nett, chat eller telefon. I virkeligheten er det bare kynisk og manipulerende svindel bak tastaturet, med mål om å få fatt i pengene dine.

Som offer opplever du svindleren som snill og hjelpsom, og det føles godt å hjelpe til. Mange har opplevd å til slutt overføre store beløp til «sin kjære».

Wangiri

Ordet Wangiri kommer fra japansk og betyr «ett ring og kutt».
Det innebærer (som definisjonen av ordet) at det kommer et anrop fra et utenlandsk nummer som ringer kun én gang. Målet er at du skal ringe tilbake. Du ringer nemlig tilbake til et telefonnummer med veldig høy takst. Ofte er det en telefonsvarer eller lydfil i enden av det utenlandske høytakst-nummeret som skal holde samtalen i gang lengst mulig. Jo lenger du lytter desto større blir telefonregningen din og desto mere tjener svindlerne.

Spoofing



Dette er en teknikk som gjør at svindlere utgir seg for å kontakte deg fra et troverdig norsk nummer. Spoofing betyr at de forfalsker eller kamuflerer seg bak en avsender et eksisterende nummer.

For å utføre spoofing på telefon bruker svindlerne en programvare som viser et annet nummer enn det faktiske nummeret de ringer fra. Dermed kan samtalen se ut som at den kommer fra et norsk nummer, noe som ofte vekker mer tillit enn et utenlandsk.

Det er gjerne slik at nummeret som vises på din telefon ser ut til å komme fra en instans som du normalt har stor tillit til, som for eksempel Politi, NAV, Skatteetaten eller lignende. Men det kan også vises som et (tilfeldig) norsk mobilnummer.

Dersom mobilnummeret ditt skulle bli spoofet, betyr det bare at svindlerne bruker ditt telefonnummer. Sannsynligvis er det tilfeldig at ditt nummer brukes, og det betyr ikke at din mobil er blitt hacket.

Spoofing brukes både på telefon, e-post og sms. Målet er som regel å fiske ut informasjon fra deg, som kan misbrukes til å svindle deg.

Investeringssvindel

Du har kanskje sett tilbud om investeringer som lover eventyrlig profitt og lav risiko? Annonser med norske kjendiser som sier de har tjent store penger og som anbefaler deg å slå til med det samme. Det er lett å la seg friste, men stort sett er det for godt til å være sant.

«Skyhøy avkastning til lav risiko». «En dobling av inntekten på bare to måneder».

I dag er investeringssvindel blant de vanligste måtene folk lures på. Her får svindlerne deg til å overføre pengene selv – gjennom å investere i alt fra krypto til aksjer og eiendom. Og mens du føler deg smart og unik som har kommet over en ny forretningsidé – med et stort potensial som garantert vil gi avkastning – sitter det drevne og utspekulerte svindlere bak tastaturet og gjør alt de kan for å manipulere deg om igjen og om igjen.

Gratislotteri

«Du kan vinne en gratis iPhone, om du bare svarer på noen spørsmål». Eller så får du en melding eller e-post at du allerede er trukket ut som vinner av en premie. Dette virker kanskje kjent for mange. Da blir mange fristet til å gi fra seg personlig informasjon, og til og med betalingskortinformasjon for å dekke frakten av premien de har vunnet.
Ja, det er veldig fristende med konkurranse der man med minimal innsats har en mulighet til å vinne en flott premie. Dessverre er det ingen som vinner noen ting. Den eneste som vinner er den som er svindler.

Hva må du se etter for å oppdage svindel

- Phishing gjøres vanligvis på vegne av banker, myndigheter, selskaper og abonnementstjenester, dvs. instanser og avsendere du stoler på.
  Sjekk avsender nøye!
- Du vil bli ofte bedt om å klikke på en lenke eller betalingsforespørsel. Vurder om dette er trygt å gjøre.
- De sier at det haster. Gjør alltid en vurdering av om det virkelig kan haste så mye.
- Se nøye etter språk- og stilfeil i meldingen.
  Se spesielt etter nesten-korrekte ord (for eksempel: Telenord istedenfor Telenor).
  Språket kan virke underlig og gammeldags og ikke helt sånn som denne avsenderen normalt vil kommunisere med.
- E-postadressen vil gjerne ligne det det falske selskapet utgir seg for å være, men er alltid litt annerledes likevel.
  For eksempel skattteetaten.no (med en ekstra ‘t') eller ‘DNB-payment.no'.
- Meldingen har merkelige vedlegg.
  Vær skeptisk til vedlegg. Som hovedregel, ikke klikk på disse.
  Vedlegg kan inneholde virus.

Råd for å unngå svindel

- Bruk sunn fornuft.
  Ikke foreta deg noe før du har tenkt deg godt om.
  Ikke la deg lure til å handle for raskt!
- Ikke ring tilbake hvis du ser at et ukjent nummer fra utlandet har ringt deg.
- Ikke klikk på lenker du har mottatt fra ukjente nummer eller ukjent avsender.
  Hvis du har klikket på lenken, sjekk hvilken nettadresse du er på.
- Slett/ignorer e-poster og SMS-er som kommer fra totalt ukjente eller som ikke virker legitime eller ekte.
- Ikke last ned apper fra ukjente nettbutikker.
- Fremstår et tilbud for godt til å være sant, er det som hovedregel svindel.
  Ikke slå til!
- Aldri invester penger via lenker på e-post, Facebook eller andre sosiale medier.
- Oppgi aldri BankID-koden din til noen andre, selv ikke til politiet.
  Det er ingen andre enn du selv som skal bruke din BankID eller kjenne til koden(e).
- Banken vil aldri be deg overføre penger til en såkalt «sikker» konto.
- Vær generelt kritisk til henvendelser.
  Husk at ingen profesjonelle/offisielle aktører spør etter personlige opplysninger over telefon eller e-post.
  Banker, Posten eller andre myndigheter vil aldri be deg om å trykke på en lenke.
  De vil be deg om å logge inn på nettstedet på vanlig måte.

- Kontakt banken din eller andre offentlige instanser via deres offisielle numre hvis du får en henvendelse du mistenker ikke er legitim.
  Husk at nummeret kan være såkalt spoofet. Bruk derfor ikke «ring tilbake»-funksjon, men slå inn nummeret selv.
- Ikke tillat fjernstyring av din PC med mindre du er helt sikker på at dette er noen du stoler på.
  Seniornett bruker fjernstyring, og når du har ringt oss på vårt offisielle telefonnummer, kan du være sikker på at det er trygt.
- Ring datahjelpen hos Seniornett dersom du er i tvil.

Sikre dine bilder og dokumenter

Har du dine digitale bilder og dokumenter lagret kun på én enhet? Da risikerer du miste dem ved et uhell, om enheten blir stjålet eller går i stykker.

Når du kjøper ny PC, nettbrett eller telefon bør bildene og dokumentene dine være med på flyttelasset automatisk. Løsningen heter Skylagring.

Hva er skylagring

Skylagring betyr at kopier av filene dine ligger i et datasenter, kalt «skyen», og er tilgjengelig via internett.

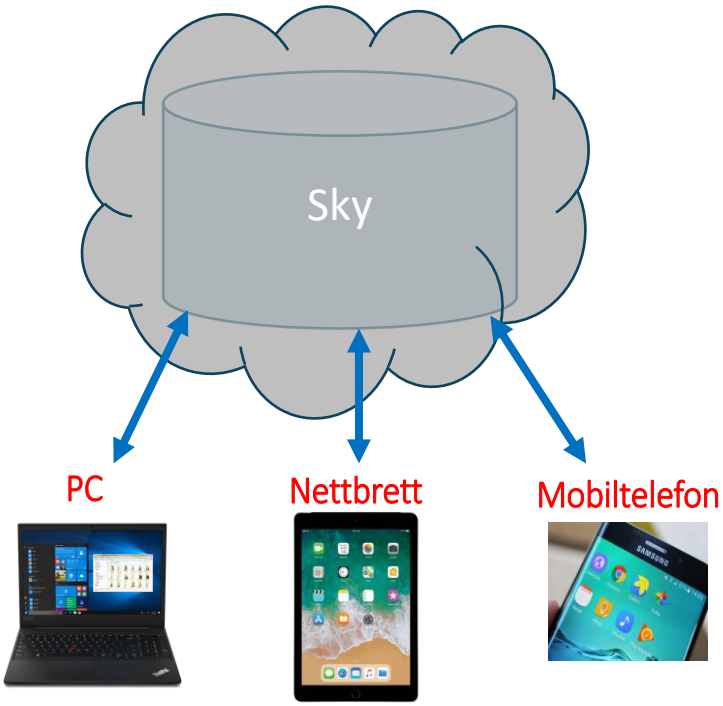
- *Skyen* er et datasenter som ligger ett eller annet sted i verden. Den er tilgjengelig når som helst og hvor som helst.

- Inneholder kopi av dine bilder og dokumenter.

- Du får tilgang via pålogging med brukernavn og passord.

- Hvis du tar bilder ute uten å være koblet til internett så vil bildene bli sendt til «skyen» straks du er tilkoblet internett igjen.

- Skylagringen sørger for at dine data sendes til alle dine enheter. Dette er praktisk slik at når du har tatt bilder med din telefon kan du etterpå vise bildene (og redigere dem) på en PC eller nettbrett.



Fordeler med skylagring

- Du mister ikke filene dine selv om du mister eller bytter enhet.

- Du får automatisk sikkerhetskopi som beskytter deg mot eventuelle uhell.

- Det er enklere å redigere og organisere bilder på PC enn på telefon.

- Du kan lage «album» via sky-apper (f.eks. Google foto, iCloud). Sky-appene lager også automatiske album for deg.

- Du kan søke opp bilder på dato, person, objekt mm.

- Du kan dele dokumenter eller bilder med Flere personer.
  Dette betyr for eksempel at når du legger et dokument i en mappe, så kan andre som du har gitt tilgang, se det samme dokumentet umiddelbart. Veldig kjekt hvis det er en vennegruppe eller forening som skal se felles dokumenter og bilder.

Ulemper med skylagring

- Du vet ikke hvor bildene eller dokumentene dine faktisk lagres. EU krever at dataene skal lagres i Europa, men det er ikke alltid garantert.
- Hva skjer om leverandøren går konkurs?
- Det kan koste, spesielt om du buker mye lagringsplass, utover det som er gratis.

Hva må du passe på

- Hver skytjeneste har sin grense for hvor mye data du kan lagre gratis.
  Grensen for hva som er gratis varierer og prisen på ekstra lagringsplass varierer også.

- Noen skytjenester inkluderer dine eposter i den totale lagringsplassen.
  Det er derfor lurt å følge litt med på hvor mye av lagringsplassen du har brukt.

- Rydd jevnlig!
  Det er gjerne mange dokumenter og bilder du ikke lenger har bruk for. Logg deg da på skytjenesten (eller gå inn på det området der filene ligger) og fjern det du ikke trenger. Da holder du forbrukt lagringsplass nede.

Aktuelle leverandører av skytjenester

- **One Drive**

Denne er drevet av Microsoft. Har du en Microsoft-konto har du også OneDrive tilgjengelig.
Har du Windows-PC har du normalt en microsoft-konto installert.
Den gir 5 GB gratis lagringsplass.

- **Google**

Har du en gmail-epost så har du google skytjenste (Foto, Drive, Mail). Har du en Android-telefon så har du også en google-konto og har normalt Google Foto installert på din telefon.
Den gir 15 GB gratis lagringsplass, men dette inkluderer også e-post (inkludert alle e-postene du ikke har slettet).

- **iCloud**

Dette er skytjenesten til Apple. Har du en iPad eller iPhone har du også en iCloud-tjeneste (som du logger på via din apple-id).
Du har 5GB gratis.

- **Dropbox**

  Er spesielt enkelt å dele dokumenter med andre.
  Kun 2 GB er gratis, men det hender de har kampanjer med mer lagringsplass.

- **Telenor Min sky**

  Denne har ubegrenset med lagringsplass, men gjelder kun hvis du har telenor-abonnement.
  Den binder deg til Telenor. Kanskje ikke så smart hvis du en gang ønsker å bytte telefon-abonnement.

- **Telia sky**

  Tilsvarende som Telenor. Ubegrenset lagringsplass så lenge du har Telia-abonnement.

Hvordan installerer du en skytjeneste

Søk opp ulike skytjenester via en nettleser. Når du har bestemt deg, gå inn på tjenestens nettside og opprett en konto (eller logg deg inn med din bruker id).

Gjelder det mobiltelefon eller nettbrett, last ned app-en fra Google Play butikk eller Apple app-store.

Gjelder det Windows-PC eller Mac, last ned programmet fra skytjenestens nettside.

Når du starter opp programmet eller app-en, må du logge deg på. Det gjøres normalt kun én gang. Da er du i gang og kan lene deg tilbake og vite at dine data er trygge.

Var det vanskelig? Kontakt datahjelpen på Seniornett. Vi hjelper deg!

Oppsummering

1. Bruk sunn fornuft og ta deg litt ekstra tid til å sjekke

Dersom det dukker opp noe du er i det minste tvil om er svindel eller ikke gjør noen undersøkelser.
Bruk altså litt ekstra tid for å sikre deg.

2. Er det for godt til å være sant, så er det nok det

Vær ekstra skeptisk til tilbud som avviker fra det andre kan tilby. En svært stor andel av disse tilbudene er nemlig for gode til å være sanne, altså svindel.

3. Du vinner ikke noe

Selv om vi ikke kan si at alle konkurranser er svindel, bør man unngå konkurranser fordi det er ekstremt vanskelig å skille ekte fra falske konkurranser.

4. Hold alle enheter du har oppdatert

Oppdatering av alle enheter du bruker er en av de beste sikkerhetstiltak du kan gjøre selv. Oppdateringer tetter hullene i sikkerhetsnettet, som gjør at det er mer sikkert å bruke enheten, spesielt når du går på nettet.
Regelmessige oppdateringer er viktig.

5. Ingen skam å bli svindlet

Det å bli offer for svindel kan være litt skambelagt. Det er likevel viktig å melde fra om datakriminalitet, og å dele erfaringen med andre. Det vil gi myndighetene og andre en bedre innsikt i hvor stort problemet er. De kan sette det enda mer på dagsorden og forhindre at det skjer igjen og med andre.
Ikke skam deg, du er helt bestemt ikke alene. Dette skjer med flere tusen mennesker hvert år i Norge.

6. Vær skeptisk, men ikke engstelig

Selv om det er en del søkelys på alt det «skumle» som kan skje i den digitale verden, og det faktisk også er en realitet at det skjer, er det viktig å ikke la frykten ta overhånd. Vær skeptisk, men ikke engstelig. Digitaliseringen gir oss mange muligheter som vi skal være glade for. Sunn skepsis og et kritisk blikk på alle henvendelsene du mottar er nyttig og nødvendig.

7. Kommer dette fra den jeg tror det kommer fra?

En kjent framgangsmåte for svindlere er at de utgir seg for å være en person du kjenner.
Dobbeltsjekk direkte med den kjente, dersom du kjenner på at det er noe som virker rart eller unormalt.

8. Ikke si: «Det vil aldri skje meg»

Det heter at «alle som har en e-postadresse, et mobilnummer eller en konto på sosiale medier, er mulige ofre».
Viktig er å nevne at dette med svindel sjelden handler om deg personlig. Det er som regel tilfeldig at du blir utsatt for svindel. I noen tilfeller er det en bestemt liste de går etter, men som regel er alt fullt automatisert og tilfeldig.
Om du er bevisst på at du er like utsatt for svindelforsøk som alle andre vil det gjør det lettere å avsløre svindelforsøk.

9. Passord er personlig

Passord er for mange en utfordring.
Det å lage gode og mange forskjellige passord har vist seg å være vanskelig for mange. Sørg likevel for å ha gode passord og å ha orden på dem. De er en del av din sikkerhet.
Husk også at 2-trinns pålogging er en «ekstra lås på døren» ved innlogging til forskjellige kontoer.

10. Generelle råd for å unngå svindel

Ikke ring tilbake hvis du ser at et ukjent nummer fra utlandet har ringt deg, og klikk aldri på lenker du har mottatt fra et ukjent nummer.
Vær kritisk når en såkalt profesjonell aktør spør etter personlige opplysninger.
Kontakt banken din via offisielle numre hvis du får en henvendelse du mistenker ikke er legitime. Og aldri oppgi BankID-koden din til noen, selv ikke til politiet.