

Sikkerhet

Digital trygghet for seniorer
Av Morten Bolstad



Seniornett

- Jobber for at seniorer skal bli bedre på å beherske digitale verktøy
- Stiftet i 1997
- Ca. 9 000 medlemmer
- Ca. 230 lokalforeninger
- Samarbeid og dialog med kommuner, eldreråd, bibliotek, servicetorg og andre organisasjoner og lag
- Driver med påvirkningsarbeid
- Organiserer opplæring, kurs og konferanser



Hva Seniornett tilbyr for medlemmer

- Kurs og veiledning i bruk av digitale verktøy og tjenester
 - Både lokalt og sentralt
- Datahjelp på telefon
 - Ubegrenset på alle hverdager
- Tilgang til alle artikler på seniornett.no
- Nyhetsbrev elektronisk en gang i uken
 - Aktuelle saker, tips og «bruksanvisninger»
- Seniornettmagasinet i posten
 - 2 ganger i året
 - Redaksjon er frivillige seniorer
- Laste ned eller kjøpe spesialmateriale
 - Digital arv
 - Kursmanualer
- Koster kr 400 pr år

Meld deg inn nå!

Fyll ut baksiden av magasinet

Kom til meg etter møtet

Gå til nettstedet seniornett.no

Digital trygghet

- Hvordan opererer svindlere
- Hva kan du gjøre for å unngå å bli svindlet

Husk at du er et mål for hackere
Ikke si at «det vil aldri ramme meg»

- Hvordan kan du sikre dine bilder og dokumenter



Digital trygghet: tips

- Hold din enhet oppdatert
- Unngå å bli «fisket»
Pass på merkelige SMS-er, e-poster og oppringinger
- Ha en bevisst passordstrategi
- Bruk to-trinns pålogging
- Vær bevisst på hva du klikker på
 - Hvem er avsender
 - Hva er adressen til der du klikker
- Ikke legg fra deg utstyr uten «vakt»
- Lås mobilen (pin, ansikt mm)
- Bruk skytjenester for bilder og dokumenter på telefon/brett



Unngå å bli «fisket»

Phishing er digital snoking eller fising etter sensitiv informasjon, som passord eller kredittkortnummer.

- Ikke følg lenker, tast heller inn nettadresse
Eks: du får en melding som ser ut som om den er fra banken din. Der står det at du skal «trykke her» for å fikse.
- Sjekk hvem som faktisk er avsender av melding med lenke
- Sjekk nettadressen ved lenker



Unngå å
bli
«fisket»

Fra Netflix <test@jsinvestment.pl> ⓘ

Til Meg <morbol.oslo@gmail.com> ⓘ

mne **Account Update Required**

Svar

Videresend

Arkiver

Ua

N

Your payment method needs to be updated.

Your account needs to be updated.

Your membership will automatically continue as long as you choose to remain a member.



**** * **** *

[Update Information](#)

NETFLIX

Questions? Call 0800-681-122

[Communication Settings](#)

Copyright 2022 NetflixInternational B.V

» <http://hovermop.com/00443812933560508156369976859280653569813&4776015296737257180124007432942193301858&morbol.oslo@gmail.co...>

Ulest: 57 To

Wangiri – Tapte anrop fra utlandet

- Du kan bli oppringt fra et ukjent telefonnummer, ofte fra utlandet, som bare lar det ringe én eller et par ganger før det blir stille.

Når du ringer opp igjen, belaster de deg for dyre summer.

- Vær bevisst hvilke numre du ringer tilbake til.

Kjenner du ikke igjen nummeret, eller ikke venter å få en samtale fra det aktuelle landet, bør du ikke ringe tilbake – uansett hvor nysgjerrig du er.

Passordstrategi

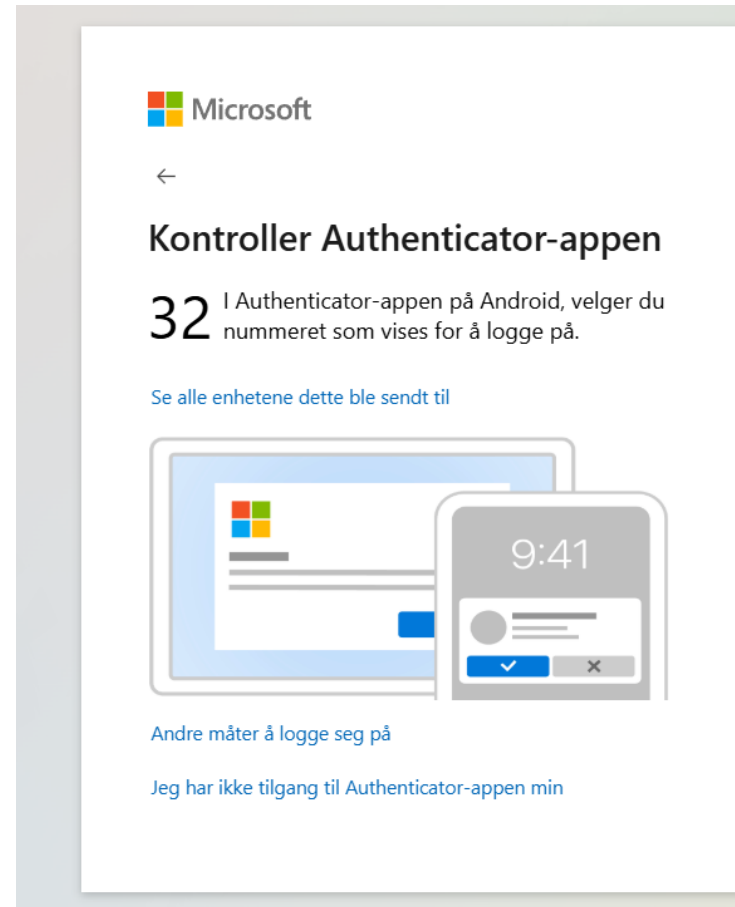
- Det vanligste passordet i verden er 123456
Ikke bruk dette!
- Lag et system som gjør at passordene til ulike pålogginger ser helt «tilfeldig» ut
- Ikke bruk samme passord overalt
 - Men ikke alle passordene behøver å være unike
 - Tenk litt på hvor sensitive data de ulike nettstedene lagrer
- Passordapp
Husker passordene dine. Men du må huske passordet til App-en
- Husk det viktigste passordet, skriv ned resten
Legg arket på et sted hjemme du husker



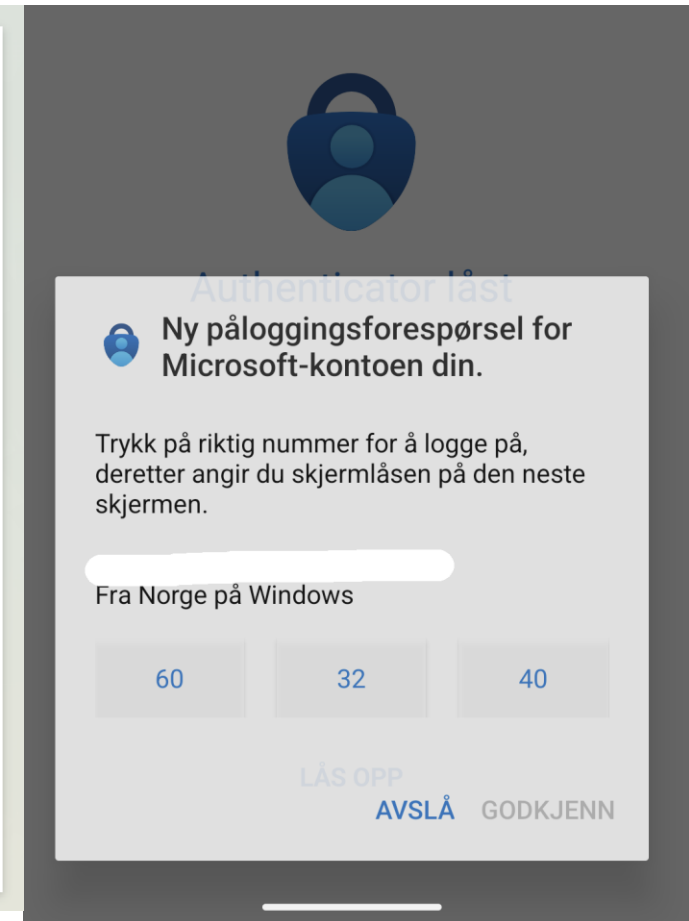
To-trinns pålogging

- Tilsvarer at du på døra di hjemme har 2 låser
 - Nøklene til de 2 låsene må ligge på ulike steder
 - Slik det er/var med bankbokser
- Passordet er 1.nøkkel. Mobilen (eller andre enheter) er 2. nøkkel
Eks: Bank-id. Der er den ekstra nøkkelen enten kodebrikke eller app på telefon

På PC



På telefon



Hvordan blir du forsøkt svindlet

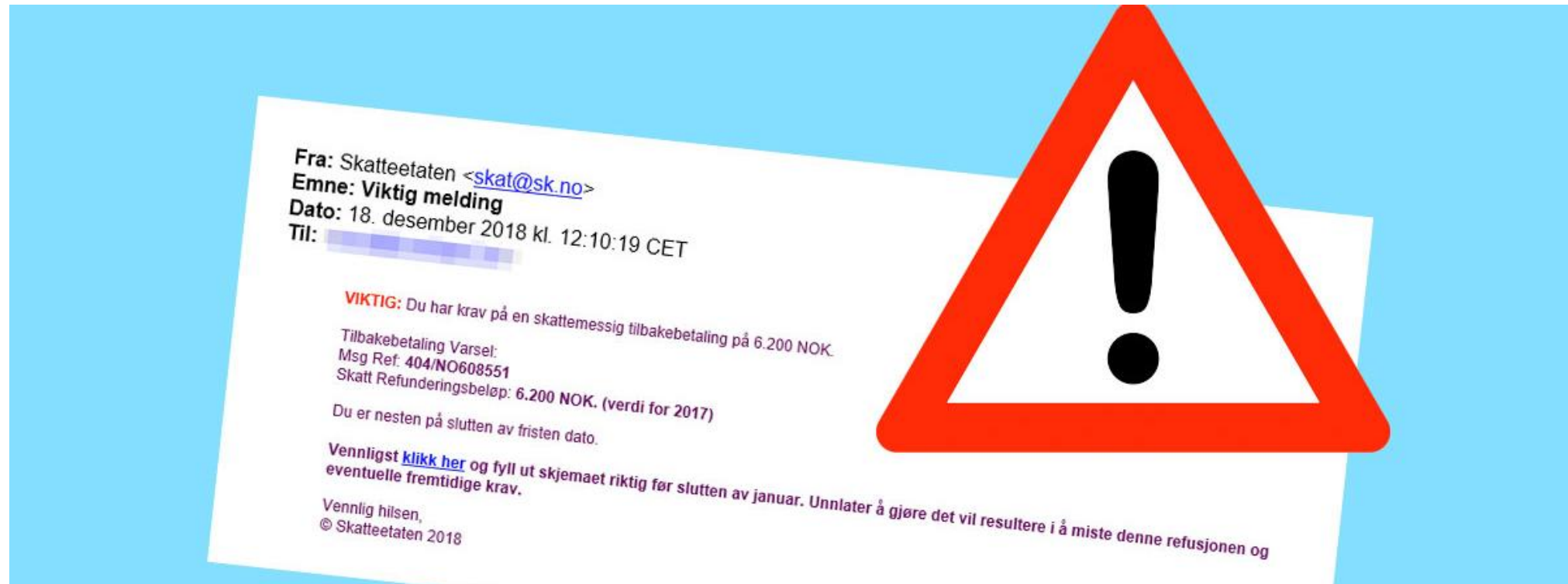
3 hovedmetoder:

- Fristelse
- Frykt
- Tillit



Fristelse

«Trykk her så kan du få masse penger»



Fra: [Svindlerens falske navn] <[falsk e-postadresse]>

Til: Deg

Kjære [Mottakerens navn],

Vi er glade for å informere deg om at du er den heldige vinneren av vår eksklusive premie! Du har blitt valgt ut blant tusenvis av deltakere til å motta en fantastisk gave verdt 10 000 NOK.

For å kreve premien din, vennligst følg disse enkle trinnene:

- 1.Klikk på lenken nedenfor for å bekrefte din identitet og fyll ut mottaksskjemaet.
- 2.Oppgi dine personlige opplysninger, inkludert navn, adresse og bankinformasjon, slik at vi kan overføre premien til deg.
- 3.Vent på bekreftelse fra vårt team, som vil kontakte deg innen 24 timer.

[Klikk her for å kreve premien din]

Vennligst merk at denne premien er tidsbegrenset, og du må handle raskt for å sikre at du mottar den. Ikke gå glipp av denne utrolige muligheten!

Med vennlig hilsen,

[Svindlerens navn]

Kundebehandler

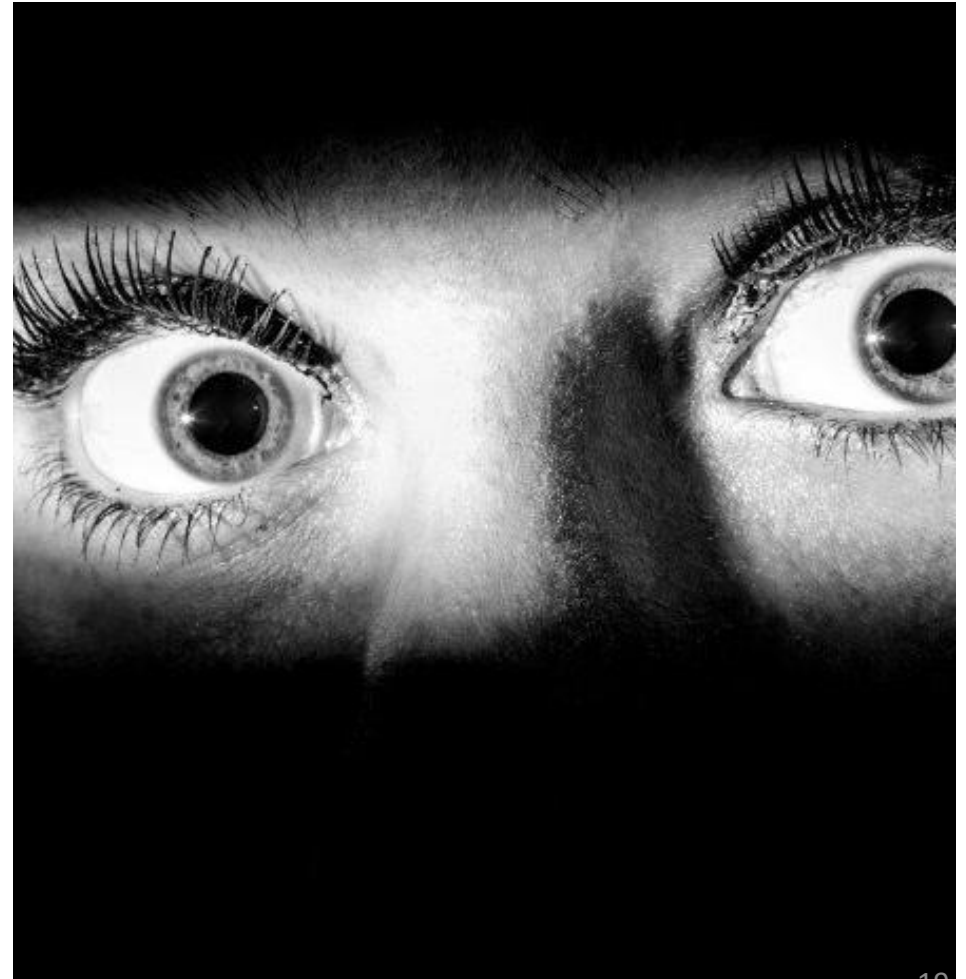
[Svindlerens falske firma]

Frykt

- Melding om at noe fryktelig vil skje
- Sier at du må gjøre noe veldig kjapt
- Typisk:
 - Oppringing om at noe er galt
 - Melding om at din enhet er infisert
 - Vi har filmet deg når du så på porno
 - Vi har tatt et kompromitterende bilde av deg

Hva bør du gjøre?

Stopp – Tenk – Ta det med ro, ikke stress



Emne: Viktig sikkerhetsvarsel: Kontoen din er kompromittert!

Fra: [Svindlerens navn] <[falsk e-postadresse]>

Til: [Mottakerens navn]

Kjære [Mottakerens navn],

Vi har oppdaget mistenkelig aktivitet på kontoen din, og det ser ut til at noen har fått uautorisert tilgang. For å beskytte dine personlige opplysninger og forhindre ytterligere skade, må du handle umiddelbart.

Hva du må gjøre:

- 1.Klikk på lenken nedenfor for å logge inn på kontoen din og bekrefte identiteten din.
- 2.Oppgi dine nåværende påloggingsopplysninger og opprett et nytt passord.
- 3.Bekreft dine sikkerhetsspørsmål og oppdater kontaktinformasjonen din.

[Klikk her for å sikre kontoen din]

Hvis du ikke følger disse trinnene innen 24 timer, risikerer du at kontoen din blir permanent låst, og du kan miste tilgang til alle dine data og midler.

Vi beklager eventuelle ulemper dette måtte medføre, men din sikkerhet er vår høyeste prioritet. Takk for at du samarbeider med oss for å beskytte kontoen din.

Med vennlig hilsen,

[Svindlerens navn]

Sikkerhetsavdelingen

[Svindlerens falske firma]

Tillit

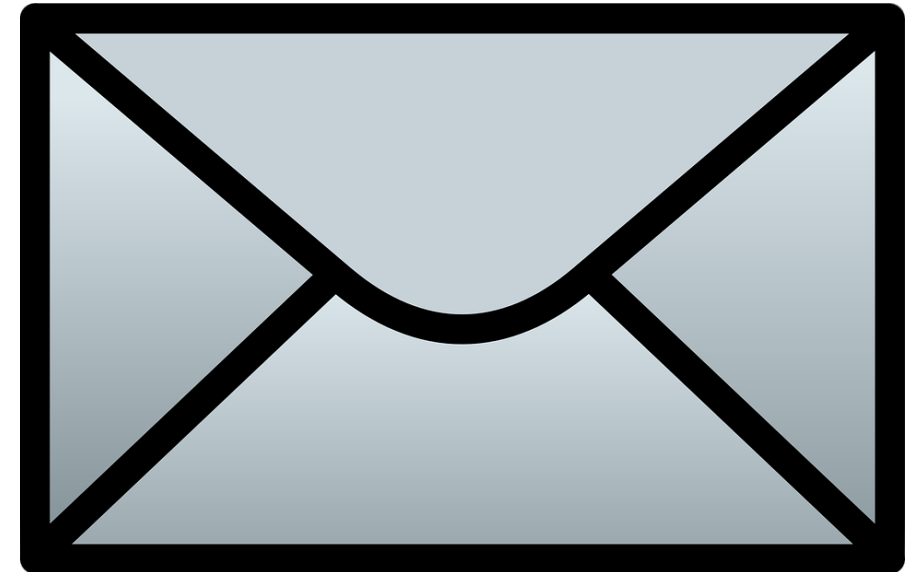
- Du får melding fra en du kjenner eller stoler på
- Du blir ringt opp av en du stoler på
- Du får «svært gode tilbud» på e-post

Svindleren vil spille på din følelse at du stoler på vedkommende. Noen kan bruke lang tid på å få deg til å tro at du kan stole på dem.



Tillit – Ulike varianter

- Olga-svindel
Ringer tilsynelatende fra banken eller politi
Ringer opp «eldre enslige damer»
- «Hei mamma»-svindel
Mor får melding om at sønn/datter har mistet telefon.
Send penger til nytt nummer
- Direktør-svindel
E-post som tilsynelatende er fra leder der du skal betale en regning
eller kjøpe gavekort
- Melding om pakke
Men du må betale litt for å få den
- Kjærlighetssvindel
Din «kjæreste» ber om penger





Tillit - Spoofing

- En svindler kan ringe deg og la det se ut som om det er en annen som ringer
- Du ser hvem som ringer det ser ut til å være et «hyggelig» telefonnr
- Innringer ser ut til å være Politiet, Posten e.l.
- De sier at noe er skjedd og at de skal hjelpe deg
- Er du usikker så be om at du ringer tilbake. Dette vil selvfølgelig svindleren ikke at du gjør

Tillit – Melding fra en «venn»

En du kjenner eller stoler på sender deg en melding

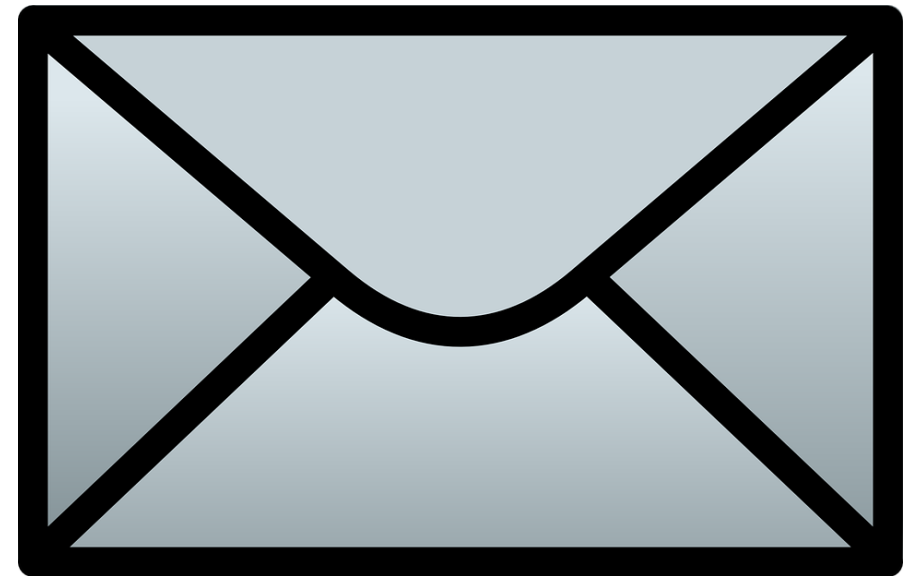
De sier at du skal gjøre noe

Og det haster gjerne

Eksempel: Du får en melding i Messenger fra en person på vennelisten. I meldingen blir du oppfordret til å delta i en konkurranse for to, hvor du må bekrefte din deltakelse overfor vennen din med en kode

Hva skal du gjøre og tenke?

- Er det naturlig at du får denne meldingen? Ber den deg om å gjøre noe uventet? F.eks. oppgi telefonnummer eller en kode
- Kontakt vedkommende i en annen kanal

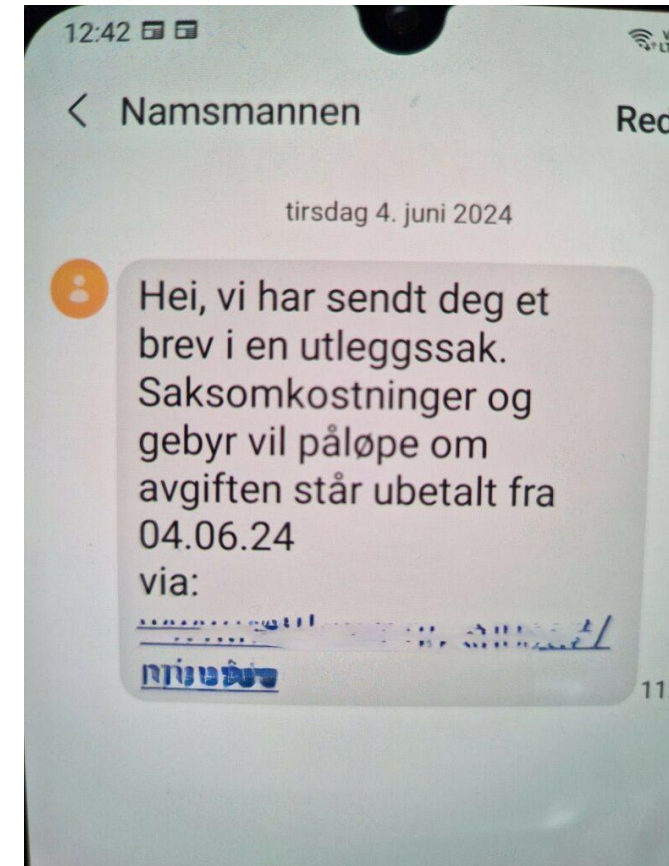


Tillit – Melding fra en institusjon

- Noe er utestående
- Du må gjøre noe
- Trykk på linken

Hva skal du gjøre?

- Stemmer det som står i meldingen?
 - Har du noe utestående, f.eks en ventende pakke
 - Haster det virkelig
 - Er det naturlig at avsender vil sende en slik melding
- Ikke trykk på linken
- Kontakt den som avsender utgir seg for å være



onsdag 15. jan. • 12:39

RCS-chat med +91 84803 88933

Postkontormelding:

Pakken din har ankommet vårt lager, men kan ikke sendes på grunn av feil adresse. Vennligst fyll inn riktig adresseinformasjon, så sender vi den til deg innen 24 timer.

<https://bit.ly/3ClfFjj?lfS=g2az845GTQ?gsl=OLRI4GLvcJ>

Klikk på linken ovenfor for å redigere den riktig.

Konto suspendert på grunn av ikke akseptert personvernpolicy

BANKID-NORWAY <a.th.en.arevi.n.g.ton@wix-forms.com>

til meg ▼

Vi håper denne meldingen finner deg vel.

Vi vil informere deg om at kontoen din er midlertidig suspendert fordi den nye personvernpolicyen for 2025 ikke er blitt akseptert. For å få tilgang til kontoen din igjen, vennligst følg trinnene nedenfor:

Logg inn på kontoen din

- Gå gjennom og godta den oppdaterte personvernpolicyen for 2025.
- Oppdater kontoinformasjonen din hvis nødvendig.
- Når policyen er akseptert og detaljene dine er oppdatert, vil kontoen din bli reaktivert umiddelbart.

Hvis du har problemer eller trenger hjelp, er du velkommen til å kontakte oss. Vi er her for å hjelpe!

Takk for din forståelse og samarbeid.
Med vennlig hilsen,

Org.no. 927 611 929
Biskop Gunnerus' gate 14,
0185 OSLO

Tillit – SMS fra bedrift

Du får en SMS «Vi holder på å klargjøre forsendelsen din. Hilsen Elkjøp. Er noe usikkert ring (et nummer)»

Du har ikke bestilt noe, så du ringer det oppgitte nummeret.

- En person sier «det er registrert 3 kjøp i ditt navn og faktura er på vei»
- Du sier «Dette må dere slette. Jeg har ikke bestilt»

Du blir så satt over til en annen person

- «Det er registrert 3 kjøp på deg. Vi kan slette, men du må bekrefte at du ønsker sletting via din Bank-id»
- 3 push-varsler fra bank-id dukker på din telefon. Ett for hvert beløp. Du godkjenner
- Du tror at alt er løst. Men du har nettopp overført penger til svindlere

Hvordan skal du tenke?

- Ikke ring oppgitt telefonnr. Ring det korrekte telefonnr til Elkjøp
- Ikke bekreft med bank-id når du ikke skal kjøpe noe

Tillit – Eksempel fra «Pay Pal»

- Du blir oppringt fra et norsk nummer
- Det er en innspilling av en person som sier at hun ringer fra PayPal
Hun snakker perfekt norsk
- Pay Pal har fått en kjøpsforespørsel på 2,99 Euro. Dette vil bli trukket fra din konto
- Hvis du vil kansellere, trykk 1. Hvis du vil kreve refusjon, trykk 2. Vil du snakke med en veileder, trykk 9
- Du vil bli satt over til en «veileder» uansett hva du velger
- Poenget er:
 - Å få snakke med deg
 - Å få deg til å tro at de skal hjelpe deg
 - Å få informasjon om deg eller få deg til å gå inn på din nettbank
 - Å fortelle at det haster

Eksempel på svindel fra Facebook

Oslo kollektivkart sitt innlegg

Oslo kollektivkart
Sponset · 🌐

🇳🇴 Den årlige kampanjen er tilbake
Reis gratis i hele seks måneder med Reisekort Travelcard 🔥
✅ Få vårt unike kort for kun 27,50 kr og glem alt om billettpriser 🚆🚊
⚠ Tilbudet gjelder frem til 11.09.2024.
For å få ditt nye personlige kort, følg lenken nedenfor 📌
<https://tinyurl.com/reisekort>



Oslo kollektivkart

Kian Bryan
Jeg ble kontaktet ganske raskt bokstavelig talt et par dager senere og mottok den i går, for prisen er det bare en gave, god jobb 🙌



1 d Liker Svar 6 🙌👍👍

Aimee Hawkins
Bestilt til søsteren min, mottatt på tre dager, takknemlig til regjeringen for dette initiativet 🙌



1 d Liker Svar 5 🙌👍👍

Aneta Slabá



1 d Liker Svar 4 🙌👍👍

Aneta Slabá
Jeg har brukt tjenesten din i ganske lang tid, fortsett å utvikle 🙌

1 d Liker Svar 3 🙌👍👍

Elvira Krüger
Tok et lite spørreskjema, generelt liker jeg tjenesten din med tanke på at jeg kjører mye

Eksempel på svindel e-post fra «Bank-id»

Varsling: Bekreft informasjonen din >

 BnkID <hola+compras@tiendanube.com>

til meg ▼



Siste varsel før stans av tjenester

Du må bekrefte kontoinformasjonen din :

I henhold til de nye gjeldende databeskyttelsesforskriftene, må våre kunder bekrefte informasjonen sin før fristen for å unngå avbrudd i deres netjtjenester.

- Frist : 14.10.2024

- Filreferanse : 95002920-669

Aktiver oppdatering

Dronning Eufemias gate 11

0150,OSLO

BnkID

Eksempel på svindel e-post. Direktørsvindel

(uten emne)

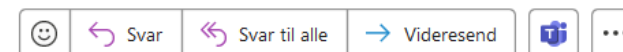


Hanni Petersen <hanni.petersen.seniornett@outlook.com>

Til ● Morten Bolstad

Oppbevaringspolicy Junk Email (30 dager)

Utløper 25.10.2024



ons. 25.09.2024 08:03

 Dette elementet utløper om 30 dager. Hvis du vil beholde elementet lenger, må du bruke en annen oppbevaringspolicy. Koblinger og annen funksjonalitet er deaktivert i denne meldingen. Flytt meldingen til innboksen for å aktivere funksjonaliteten. Vi konverterte denne meldingen til rent tekstformat.

hanni.petersen.seniornett@outlook.com ser ut til å ligne på noen som tidligere har sendt deg e-post, men som kanskje ikke er den personen. Finn ut hvorfor dette kan være en risiko
<<https://aka.ms/LearnAboutSenderIdentification>>

God morgen morten

Har du et minutt? Du må gjøre en oppgave for meg. Jeg kan ikke snakke i telefonen, jeg har en rekke møter, så jeg skriver bare tilbake her.

Med vennlig hilsen

Hanni Petersen

Generalsekretær



Tillit – svindel e-post

Hvordan unngå å bli lurt av svindel-epost

- Ikke svar på epost du ikke er sikker på er ekte
- Ikke trykk på lenke der du skal oppgi opplysninger
- Ikke oppgi e-postadressen din ukritisk til ulike nettsteder og nettjenester
- Ikke bruk funksjonen «meld deg av» fra ukjent avsender
- Vurder visningsnavn på f.eks. Finn.no (slik at svindlere ikke veldig enkelt kan resonere din e-postadresse)
- Bruk sunn fornuft



Sjekkliste ved mottak av e-post med lenke

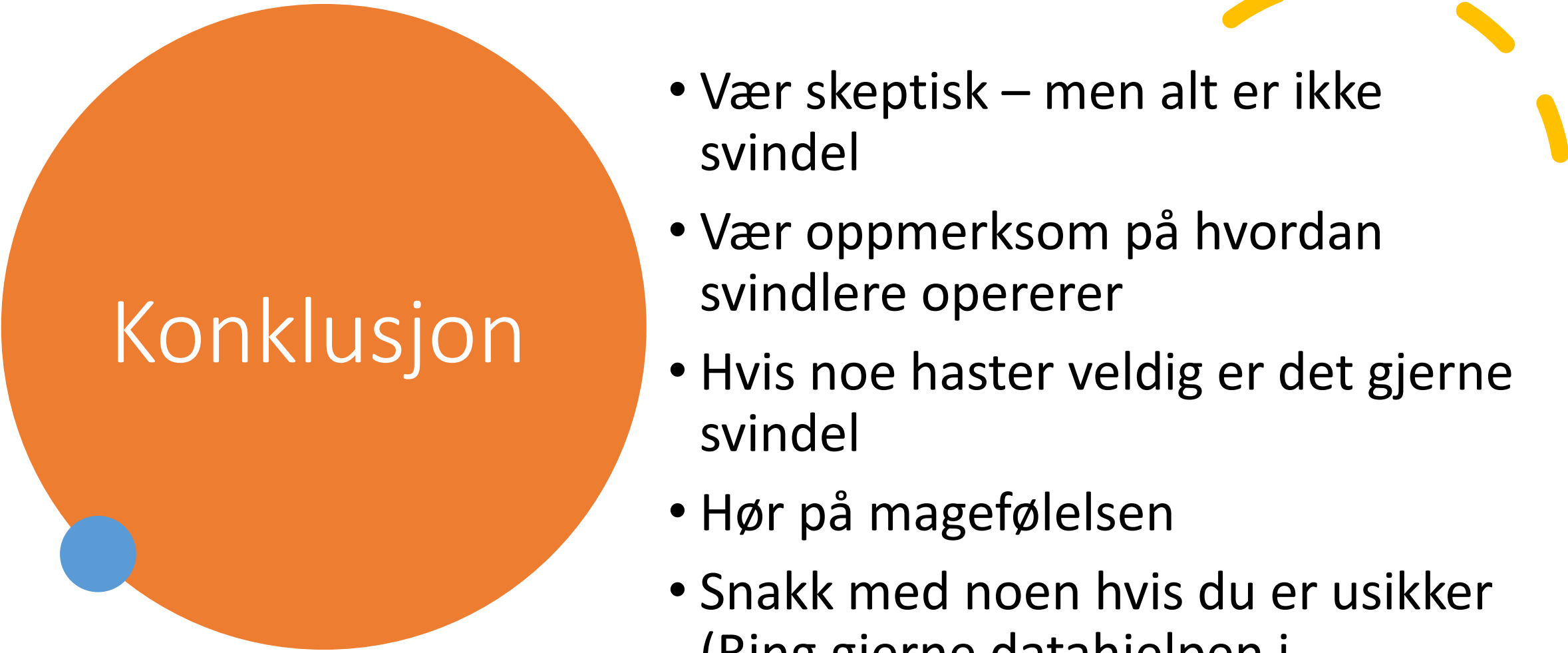
- Sjekk avsender-adresse
Sjekk spesielt mot feilstavelser
- Sjekk hvor lenken peker
- Er e-posten skrevet slik du forventer av «avsender»
- Prøver e-posten å stresse deg
«Det haster»
- Inneholder e-posten vedlegg
Vær skeptisk til disse
- Hvis du har klikket på lenken, sjekk hvilken nettadresse du er på.
Se spesielt etter nesten-korrekte ord
(f.eks: telenord istedenfor telenor)

Norsis tilbyr e-kurs «Beskytt dine digitale verdier»

Kurset lærer deg hva dine digitale verdier er og hvordan du kan beskytte verdiene.

Søk på Google «beskytt dine digitale verdier» og velg treffet på Norsis.

Der velger du *Kurs* og ser teksten *Vårt nye e-læringskurs heter [«Beskytt dine digitale verdier»](#)*. Trykk på lenken



Konklusjon

- Vær skeptisk – men alt er ikke svindel
- Vær oppmerksom på hvordan svindlere opererer
- Hvis noe haster veldig er det gjerne svindel
- Hør på magefølelsen
- Snakk med noen hvis du er usikker (Ring gjerne datahjelpen i Seniornett)

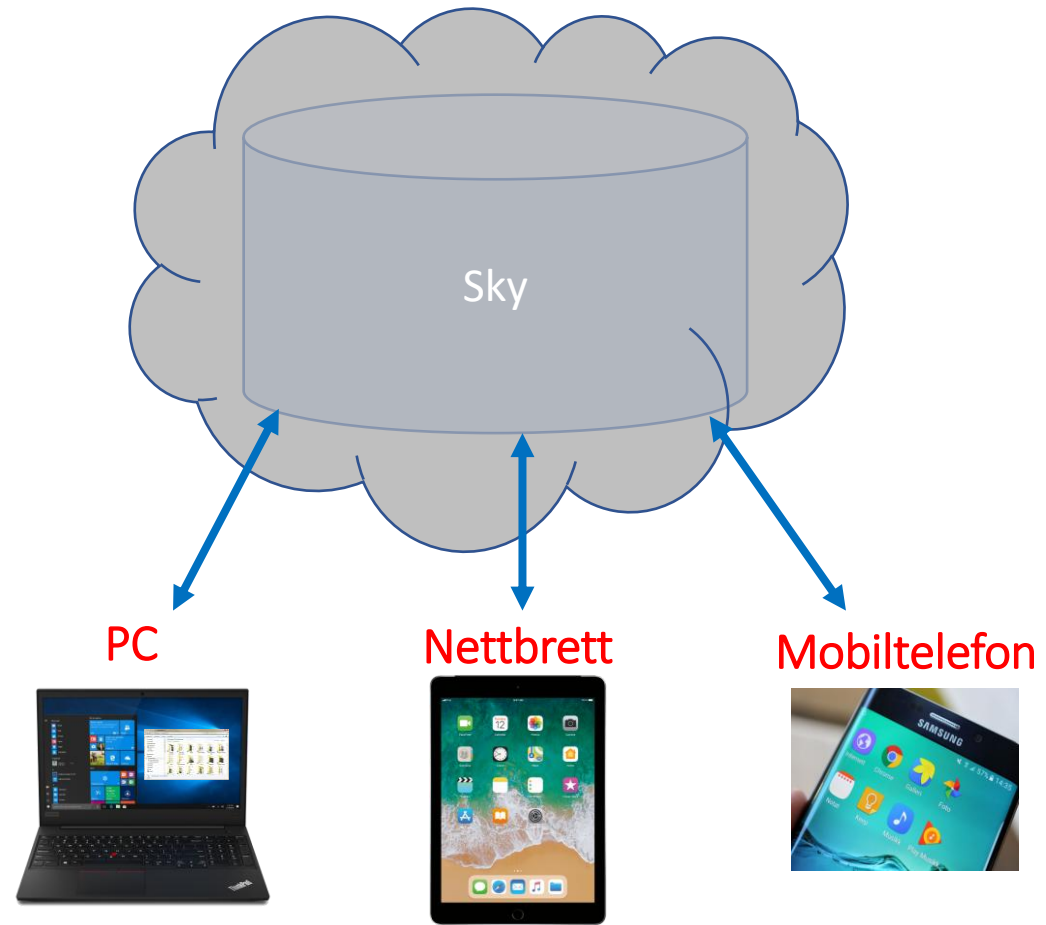
Sikre dine bilder og dokumenter

- Sørg for at de ikke blir borte
- Bildene og dokumentene skal være «nissen på lasset» når du bytter utstyr
- Svaret er: Skylagring



Hva er skylagring

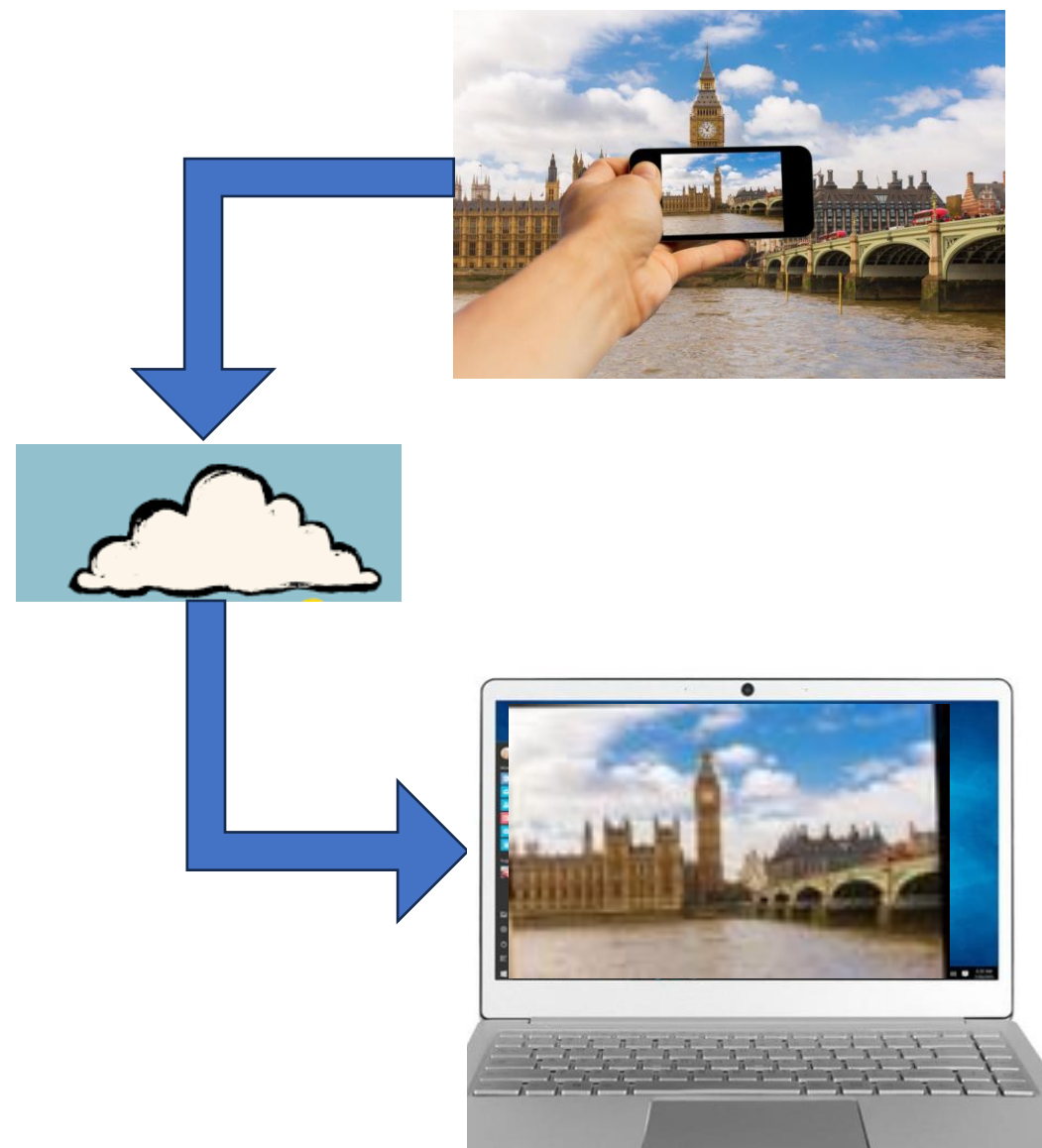
- *Skyen* er et datasenter som ligger et-eller-annet-sted i verden
- Den er tilgjengelig «over alt» og «alltid»
- Inneholder kopi av dine data (bilder, dokumenter)
- Kobles til dine enheter via autentisering (brukerid, passord, 2-faktor)
- Du må være koblet til Internett
Kan også kopiere asynkront
- Sørger for at dine data sendes til alle dine enheter



Hvordan virker det

Eksempel: Du har en mobiltelefon og en PC. Du har koblet begge til en skytjeneste

1. Du tar et bilde med mobilen
2. Bildet blir automatisk lastet opp i skyen (tar få sekunder, dersom du er koblet på nett)
3. Du slår på PC-en (eller nettbrettet) etterpå
Du logger deg på skytjenesten (Skjer normalt helt automatisk)
4. Du kan se bildet direkte på PC-en



Fordeler ved å bruke skylagring

- Du mister ikke filene/bildene dine selv om du mister/bytter enhet
- Du får automatisk sikkerhetskopi
- Enklere å redigere og organisere bilder på PC enn på telefon
- Lett å lage «album» via sky-apper (f.eks. Google foto, iCloud)
Manuelle og automatiske album
- Lett å søke opp bilder på dato, person, objekt mm
- Flere personer kan dele dokumenter/bilder

Ulemper med skylagring

- Du vet ikke hvor bildene/dokumentene dine faktisk lagres
- Hva hvis leverandøren går konkurs?
- Det koster, litt

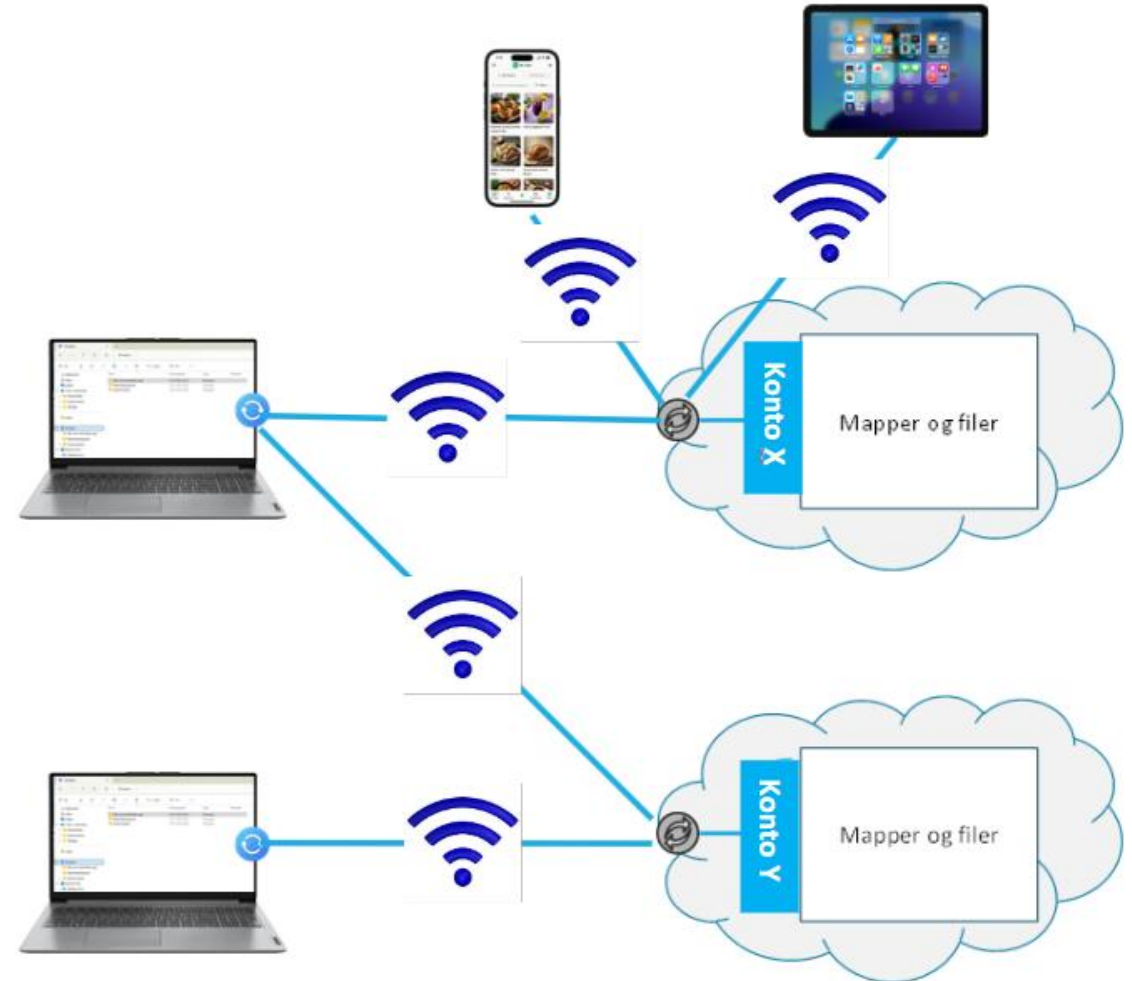


Eksempel på ulike bruksmåter

- En person kan ha **flere konti** som kan benyttes fra **samme PC**
- Flere enheter kan være koblet til **samme konto** **samtidig**

Eks:

- Flere familiemedlemmer på samme konto
- Flere familiemedlemmer på hver sin familiekonto
- En personlig konto og en jobb/skole-konto
- Flere konti for å bruke gratis lagringsplass eller for å skille ulike saksområder



Aktuelle leverandører

Skytjeneste	Leverandør	Gratis lagringsplass	Ekstra lagring (pr måned)
One Drive (MS 365)	Microsoft	5 GB	100 GB: 20 kr
Google Foto/Disk/Mail	Google	15 GB	100 GB: 24 kr / 2 TB: 125 kr
iCloud	Apple	5 GB	50 GB: 12 kr / 200 GB: 39 kr
Dropbox		2 GB	2 TB: ca 130 kr (10€)
Telenor Min sky	Telenor	Ubegrenset med telenor-abonnement	
Telia sky	Telia	Ubegrenset med Telia internett-abb	

Det finnes andre også. Dette er de vanligste for privatpersoner

Det er ikke noe i veien for å ha flere samtidig

Takk for meg!

**Ikke glem at du
kan melde deg
inn i
Seniornett.
Her og nå!**

