Sikker på nett

Hva skal man gjøre for å være sikker på nett – med PC, nettbrett eller mobil

Carl-Edward Joys
Seniornett Asker


Internett er som en urskog.
Full av skatter og ukjente ting
Men også full av skurker og farlige planter og dyr
Mennesket har vent seg til å leve i og av urskogen
Det må de også gjøre i en internettverden.

Nettvettregler

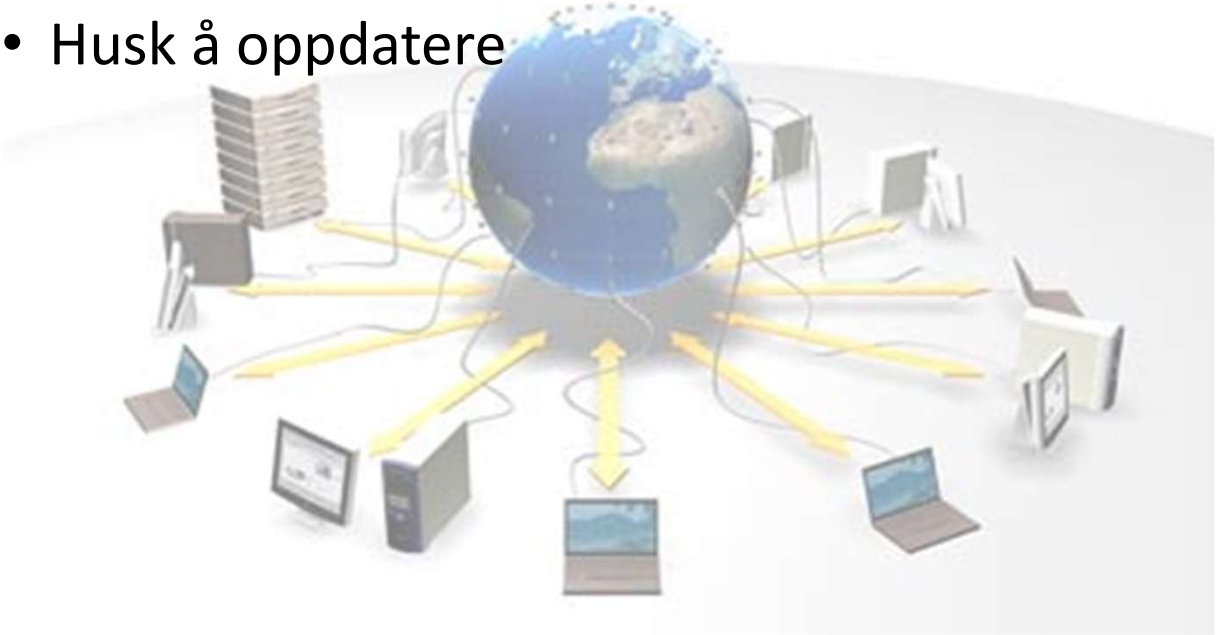
- Vi skal snakke om leveregler i Internettverdenen
  - Kalles også nettvettregler
- www.nettvett.no
- Andre sammenligninger:
  - Trafikkregler
  - Fjellvettregler

Basis

- Internett
- Terminaler
- Forbindelser
- Informasjons-givere
- E-post-servere
- Skylagring
- Søkemotorer
- Smart-hjem dingser

Hva galt kan skje?

- Maskinvaren din svikter
  - Tap av din private informasjon
  - Sikkerhetskopier er viktig
- Programvaren har feil/sikkerhetshull
  - Husk å oppdatere



Hva galt kan skje?

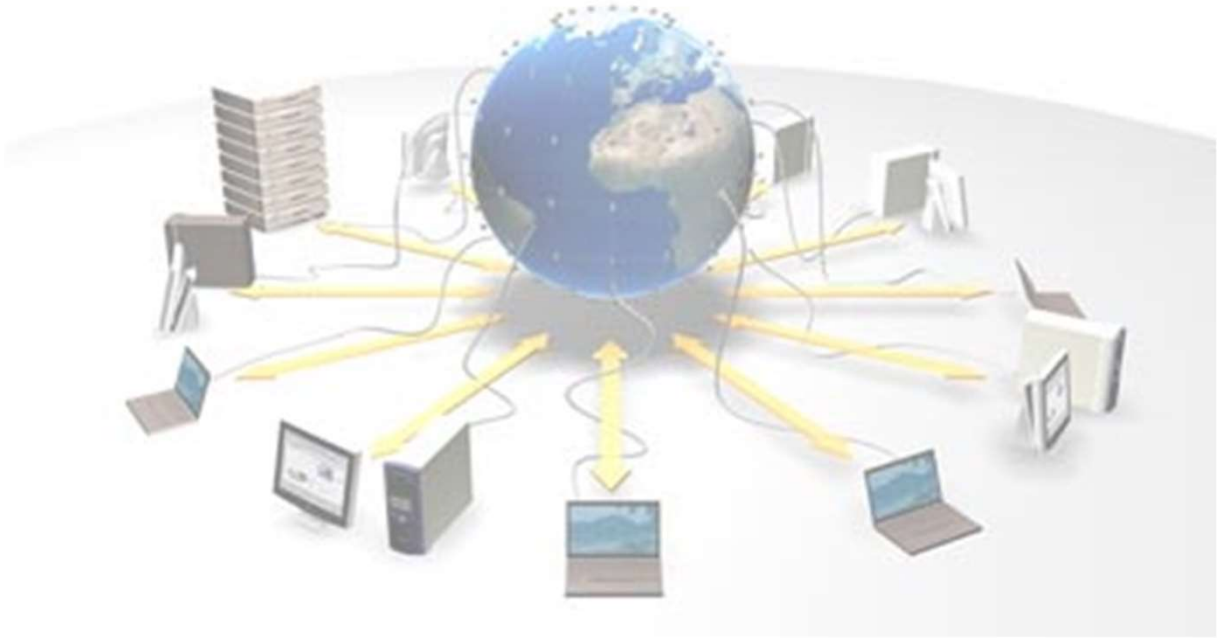
- Lytting på forbindelse for å finne passord, kontoopplysninger etc

Hva galt kan skje?

- Innføring av skadelig programvare på enheten din
  - Denne programvaren kan gjøre mye rart og få tilgang til mange opplysninger som så kan bli brukt videre

Hva galt kan skje?

- Noen kan stjele din informasjon som du har lagt igjen på nettet
  - Enten ved innbrudd hos den leverandøren du har valgt
  - Eller ved å logge seg på som deg (stjeling av identitet)



Hva galt kan skje?

- Du gjør noe dumt!
  - Dette er det vanligste – det er din oppførsel som er den største sikkerhetsrisikoen
    - Har passord klistret på bordet foran skjermen
    - Trykker på noe før du har tenkt deg om
    - Etc….

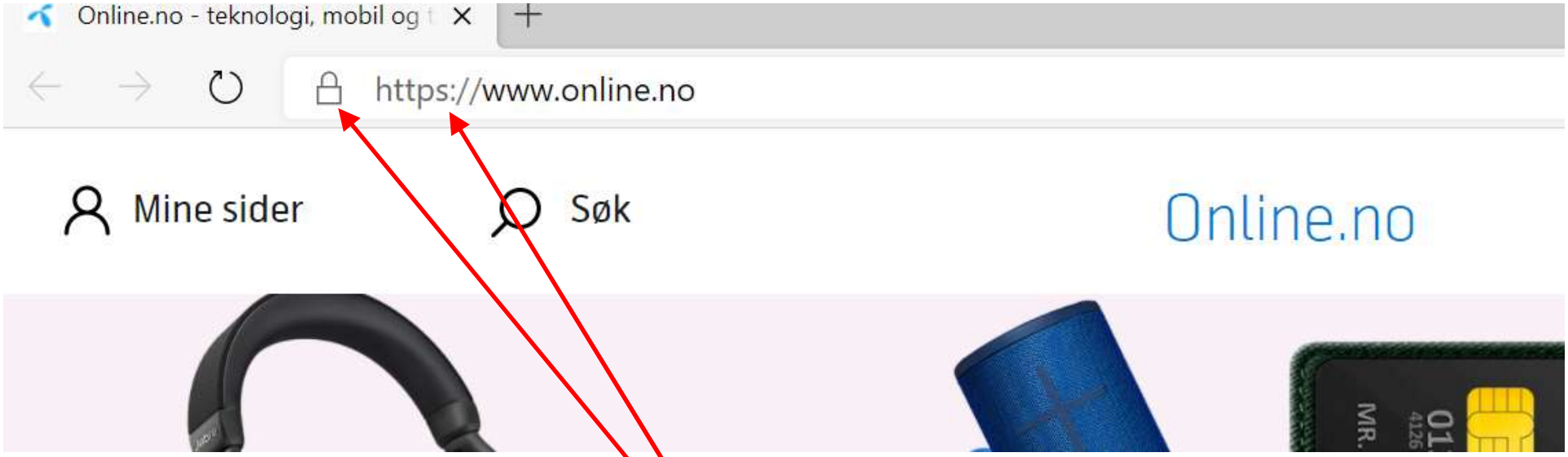
Hva galt kan skje?

- Lytting på forbindelse for å finne passord, kontoopplysninger etc
  - Forhindres ved kryptering av forbindelse,
  - Bruk VPN hvis man **må** bruke åpne WiFi-nett
    - Eller ikke logg deg på tjenester
  - To-trinns autentisering

Krypterte forbindelser

Hvordan ser man at man er på en kryptert forbindelse?

Nettlesereksempel



«s» i https: betyr kryptert forbindelse
Se også etter hengelåsen

Hva galt kan skje?

- Innføring av skadelig programvare på enheten din
  - Denne programvaren kan gjøre mye rart og få tilgang til mange opplysninger som så kan bli brukt videre
  - Virussjekker/Sikkerhetsprogrammer vil vanligvis finne disse og uskadeliggjøre dem
  - Vær spesielt varsom når du laster ned nye programmer at der ikke kommer noe haleheng.

Hva galt kan skje?

- Noen kan stjele din informasjon som du har lagt igjen på nettet
  - Enten ved innbrudd hos den leverandøren du har valgt
  - Eller ved å logge seg på som deg (stjeling av identitet)
  - Pass på passordene dine
  - Bruk to-trinns autentisering der du kan

Hva galt kan skje?

- Du gjør noe dumt!
  - Dette er det vanligste – det er din oppførsel som er den største sikkerhetsrisikoen
    - Har passord klistret på bordet foran skjermen
    - Trykker på noe før du har tenkt deg om
    - Etc….

Oppførsel

- Der finnes sikker oppførsel og usikker oppførsel
- Gode eksempler
  - Tenk før du klikker
- Dårlige eksempler
  - Ikke la andre bruke din datamaskin/nettbrett – sikre med passord for pålogging og inaktivitet
  - Ikke besøk suspekte nettsteder
    - Fra Hakkebakkeskogen:
      «Borti skogen er et revehi, der går aldri noen mus forbi»

Hva er sikkert og hva er ikke sikkert

- I utgangspunktet er alt usikkert, ingen terminaler er mer sikre enn andre.
- Det er din egen oppførsel som er nøkkelen til sikkerhet
- Dessuten kan du installere beskyttelsesmekanismer (virussjekker etc)
- Enheter som benyttes av flere er mer utsatt for risiko enn andre

Terminaler

- Alle terminaler som kan besøke Internett er utsatte, PC, Mac, nettbrett, smarttelefoner. Ingen er bedre enn andre.
- Beskyttelsesmekanismer
  - Virusprogrammer
  - Windows Defender (del av Windows 10)
  - Andre produkter
  - Hva gjør disse programmene?

Internett - lesing

- Internett lesing er relativt sikkert
- Så lenge man ikke svarer på opplysninger eller spørsmål er det ingen fare
- Men:
  - Sideeier kan lagre opplysninger om deg (Hvor du kommer fra (IP-adresse) og hvilke sider du har brukt)
  - Sideeier kan legge igjen informasjonskapsler (vanligvis ufarlige, men fjernes ofte av virussjekker)
  - Nedlastninger kan være farlige (eksempler nye drivere, dokumenter etc) fordi det kan være andre ting som blir hengt på. Virussjekker hjelper mot dette.

E-post

- E-post er ikke sikker
  - Du vet ikke hvem den kommer fra – det som står i adressefeltet behøver ikke være riktig
  - E-poster med vedlegg/lenker er en vanlig måte å lure folk på
    - Arv i Afrika
    - Tilbud som er for gode til å være sanne
  - De ender alltid med
    - Send informasjon om deg selv
    - Last ned fil, eller besøk nettsted

Hvordan kan vi oppdage

- Kommer e-post fra en du regelmessig kommuniserer med?
- Hvis du setter musepilen på en lenke – så viser den hvor du virkelig går videre, er det det samme som står i teksten?
- Er der språkfeil i e-posten - Suspekt

Eksempler


Faktura NO / 90402543

P

Posten <nets@server643831.nazwa.pl>

Til ca-ed-jo@online.no

Følg opp.

Service Posten.no Norway

Kjære kunde,

Posten informerer deg om at forsendelsen din NO / 90402543 fremdeles venter på instruksjoner fra deg.

Den blir levert så snart kostnadene er betalt.

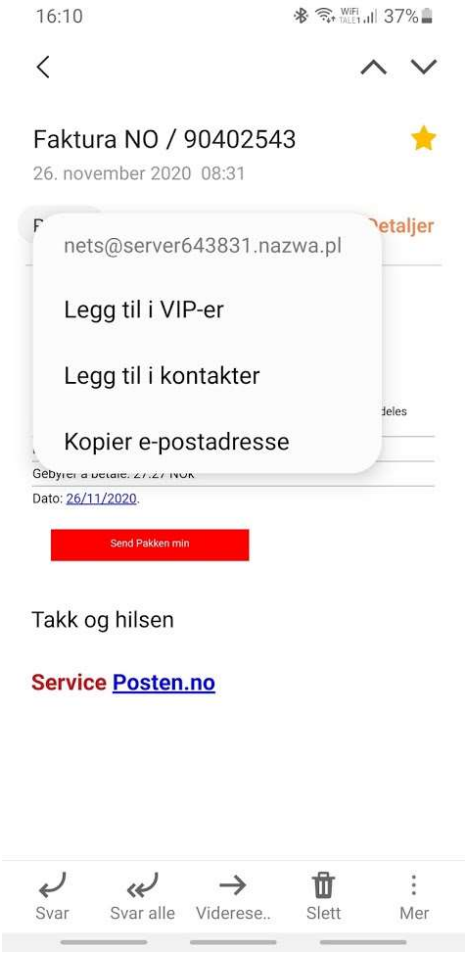
Gebyrer å betale: 27.27 NOk

Dato: 26/11/2020.

Send Pakken min

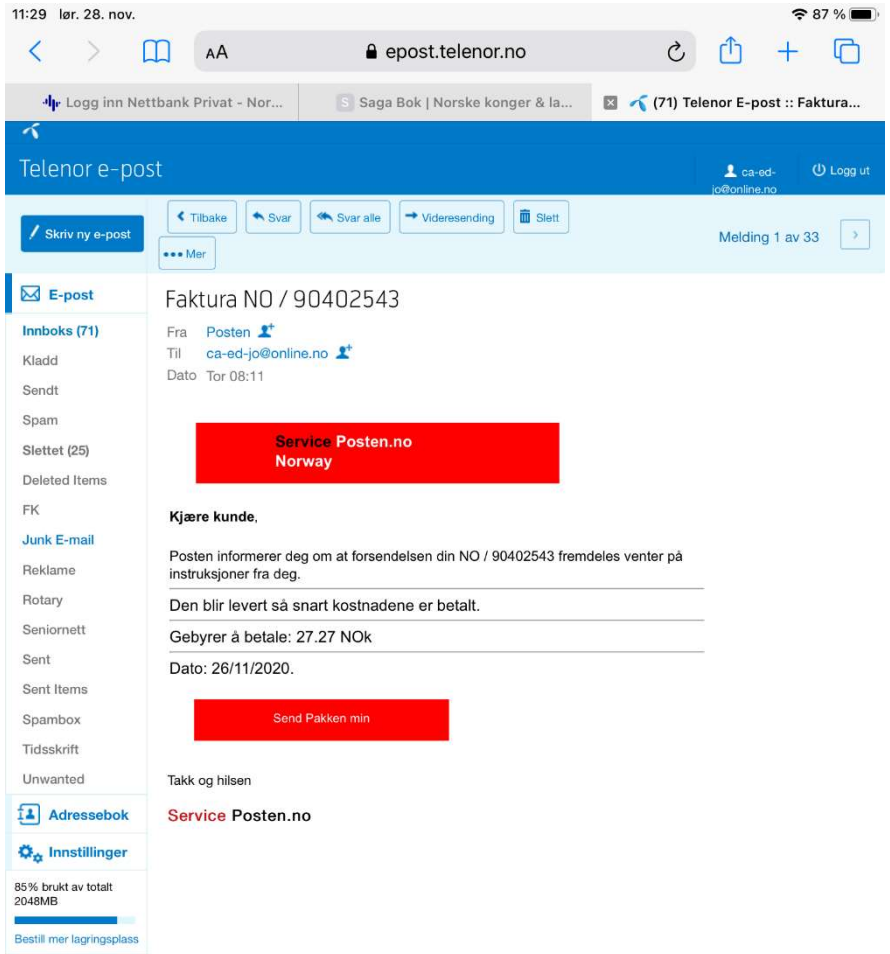
- Outlook
  - Legg merke til adressen ved siden av avsender

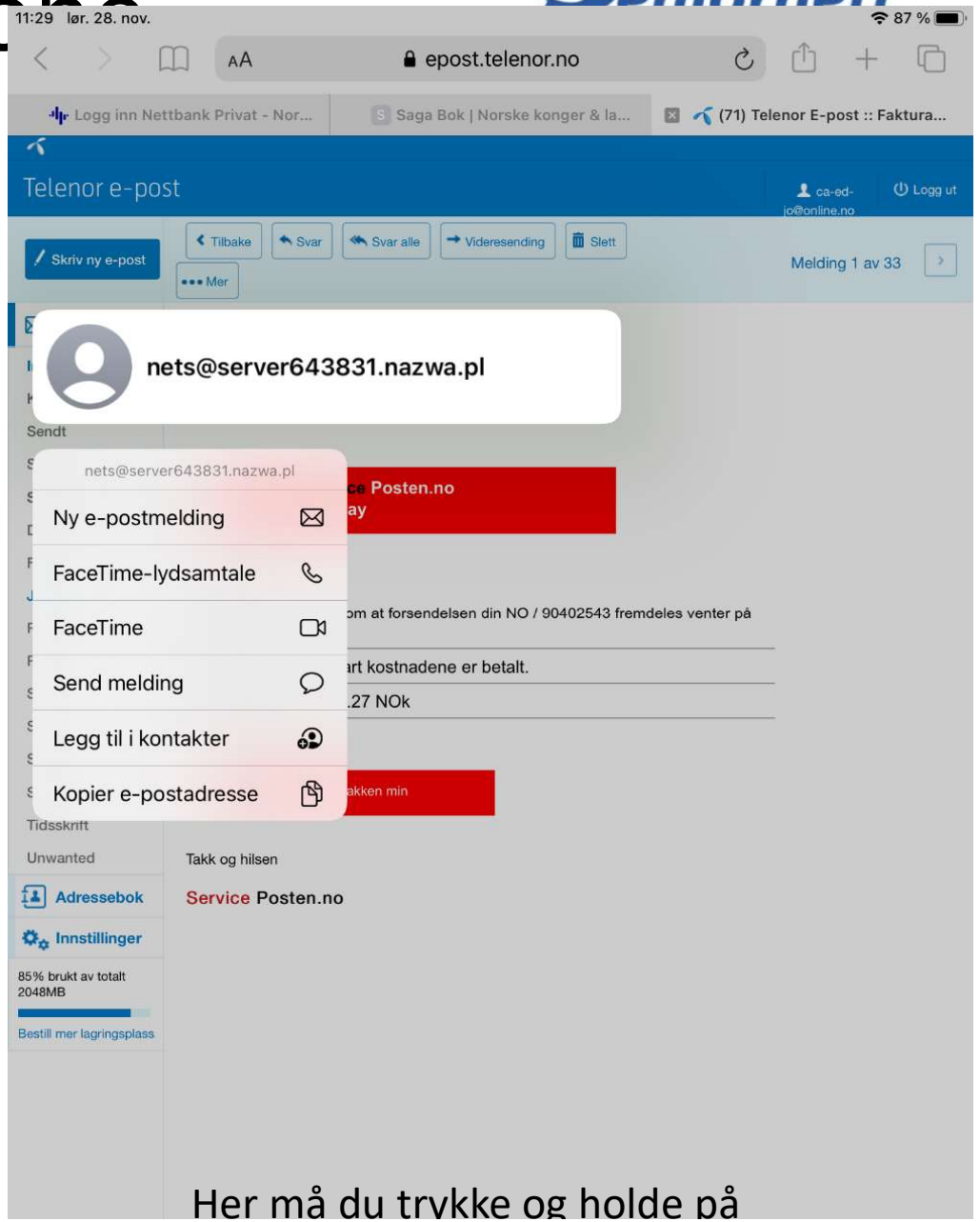
Eksempel – android



- Her må du trykke på «posten» og da først kommer adressen i polen opp

iPad/iPhone





Her må du trykke og holde på

Hva gjør du med suspekte e-poster

- Slett umiddelbart.

Hva gjør du hvis du gjorde noe galt

- Hvis du ser at du har lastet ned noe du ikke skulle gjort eller oppførselen til enheten blir gal – så gjør følgende
- 1. Koble enheten vekk fra nettet
- 2. Forsøk å finne ut hva som har skjedd ved å spørre andre, bruke en annen enhet til å sjekke opp etc

Ord og uttrykk

- Kryptering
- 2-faktor autentisering
- Åpne nettverk
- VPN (Virtual Private Network)
- Informasjonskapsler
- Virus/virussjekk
- Trojaner
- Phishing
- Ransomware

Ord og uttrykk

- For å unngå lytting
  - Kryptering
  - 2-faktor autentisering
  - Åpne nettverk
  - VPN (Virtual Private Network)
- Skadelig programvare
  - Virus
  - Trojaner
  - Ransomware (løsepengevirus)
- Informasjonskapsler
  - Vesentlig harmløse
- Phishing
  - For å få napp – (få deg til å gjøre dumme ting)

Sikre løsninger

- Nettbank
- Altinn – helse-norge
- Sikker e-post

- Alle disse bruker 2-faktor autentisering

Halvt sikre løsninger

- Handling på nett
  - Reise
  - Ting
  - Kjøp og salg
- Bruk kredittkort – da er det kreditkortfirmaet som har pengerisken hvis firmaet ikke leverer.

Mere opplysninger

- www.nettvett.no
- Nettvettreglene