IT sikkerhet

ASC

GJELDER DETTE MEG?

«Den som vil lese mine brev, se mine bilder kan bare gjøre det»

ASC

Dette gjelder alle med en enhet koblet til nettet!

Hva er farene?

- ID tyveri
- Løsepenger
- Lure andre i ditt navn
- ... Annet jeg ikke har tenkt på enda, men som kreative kriminelle sjeler pønsker ut fortløpende.

Store og små er utsatt

UTPRESSINGVARE

Cryptolocker har mutert. Schibsted, VG, Teknisk Ukeblad og digi.no ble rammet

Veldig mange opplever nå angrep. Her deler vi erfaringer og eksperter gir råd.

AV: MARIUS JØRGENRUD | PUBLISERT: 3. FEB. 2016 - 21:43

0

På ettermiddagen tirsdag gikk alarmen i redaksjonslokalene til Teknisk Ukeblad Media. Den fryktende Cryptolocker-skadevaren hadde slått til i bedriftens interne nettverk.

Leserne var aldri truet. Det er viktig å understreke.

Dette er en kjent skadevare som låser filene på infiserte datamaskiner med sterk kryptering. For deretter å kreve løsepenger.

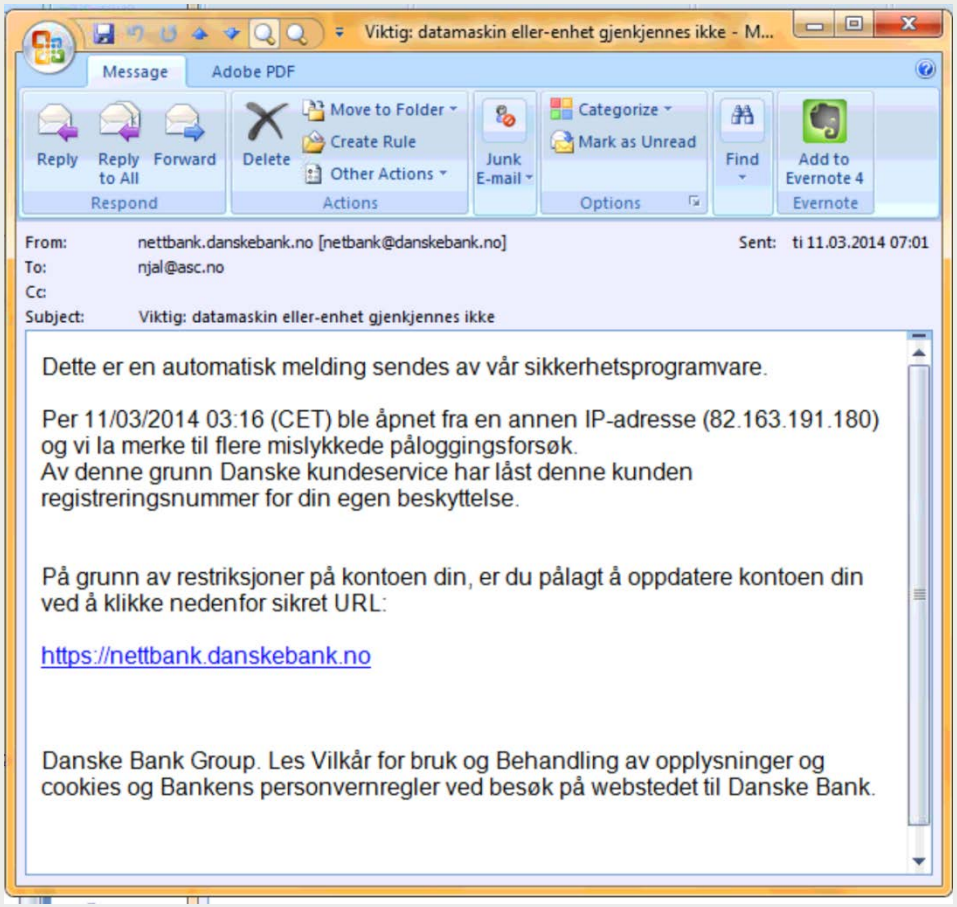
NEDTELLING: Etter at filene er kryptert blir skrivebordet på pc-en endret til en plakat med betalingsanvisning og nedtellingsur. Bildet er fra en eldre utgave av Cryptolocker omtalt i 2013. (Bilde: Sophos)

I vårt tilfelle kom én medarbeider i skade for å åpne et vedlegg, som utga seg for å være en hentemelding fra Posten Norge. Altså den samme skadevarekampanjen som har herjet mange

- **"Dette er en kjent skadevare som låser filene på infiserte datamaskiner med sterk kryptering. For deretter å kreve løsepenger.»**
- «I vårt tilfelle kom én medarbeider i skade for å åpne et vedlegg, som utga seg for å være en hentemelding fra Posten Norge»
- «Angripere sender epost som forsøker å lure mottakeren inn på en forfalsket nettside under postennorg.com, men domenet vil kunne variere. Det blir brukt norsk språk med relativt få skrivefeil. «Hentelappen» du kan laste ned er en zip-fil som inneholder skadevaren som en kjørbar fil.»

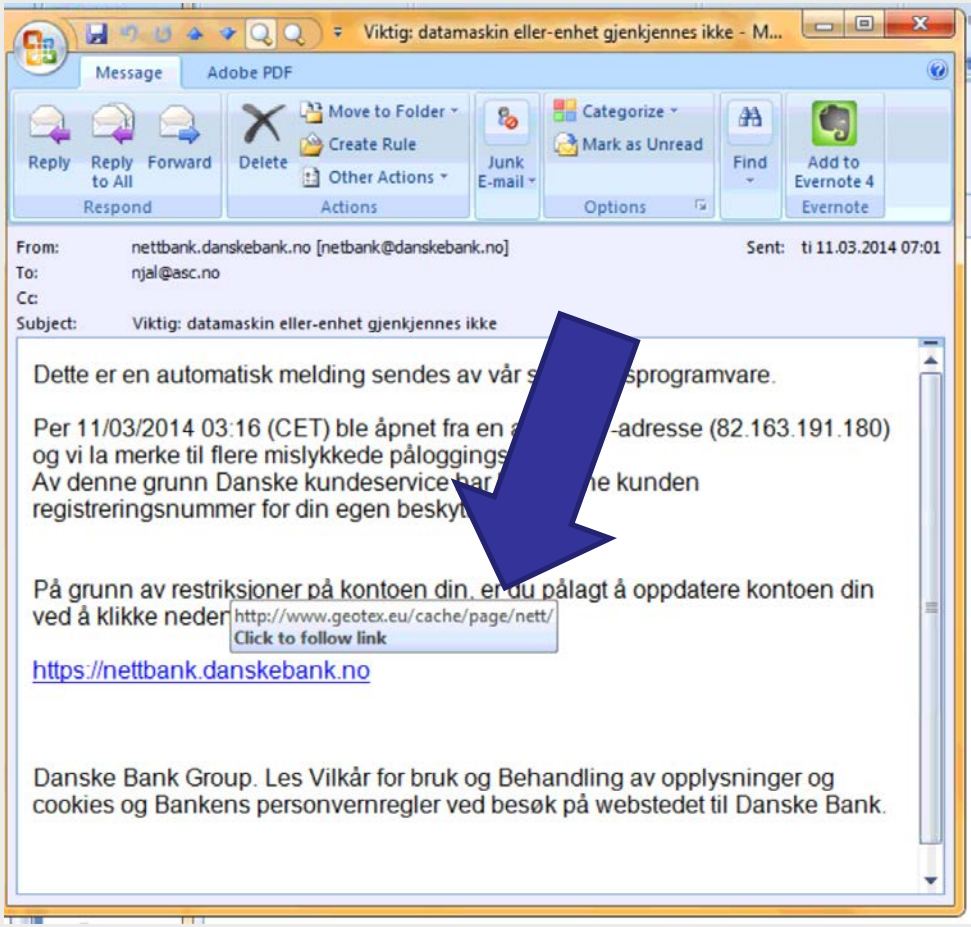
E-post med lenke ?

- Kjenner du avsender?
- Er avsender den de utgir seg for?
- Hva er lenken?
- Hva er BAK lenken?
- Hva ber de om?



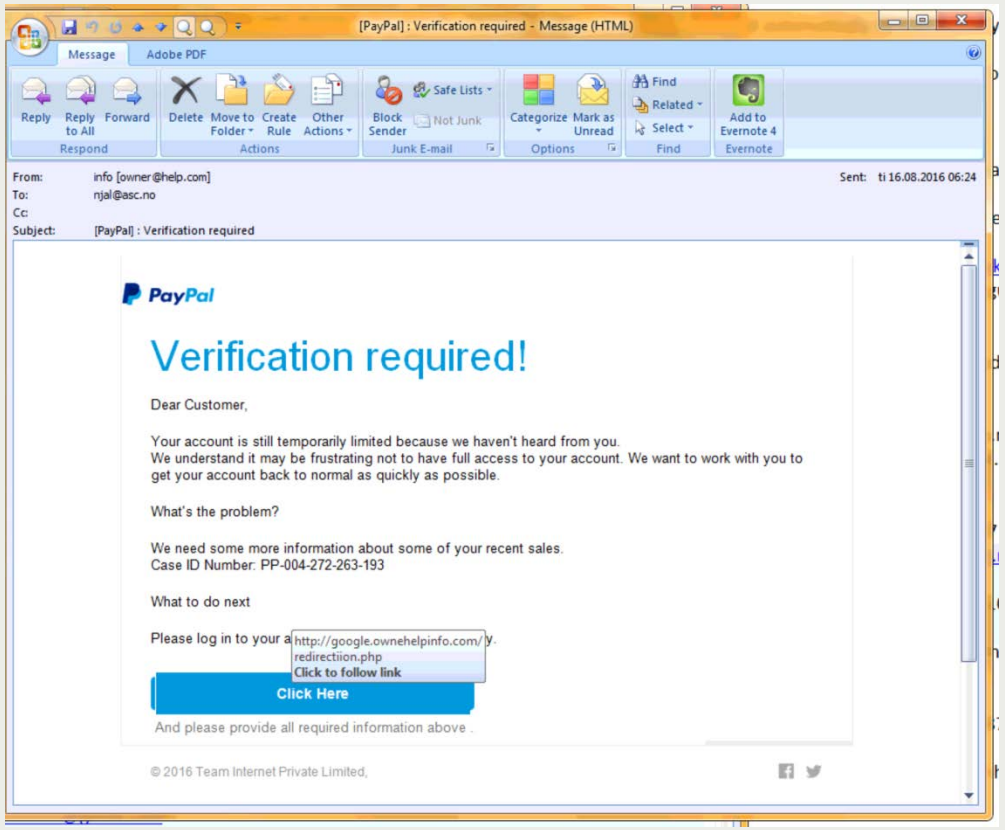
E-post med ukjent lenke

- Hold musen over lenken, så ser du hvor den faktisk går. Om dette ikke er likt, IKKE klikk!



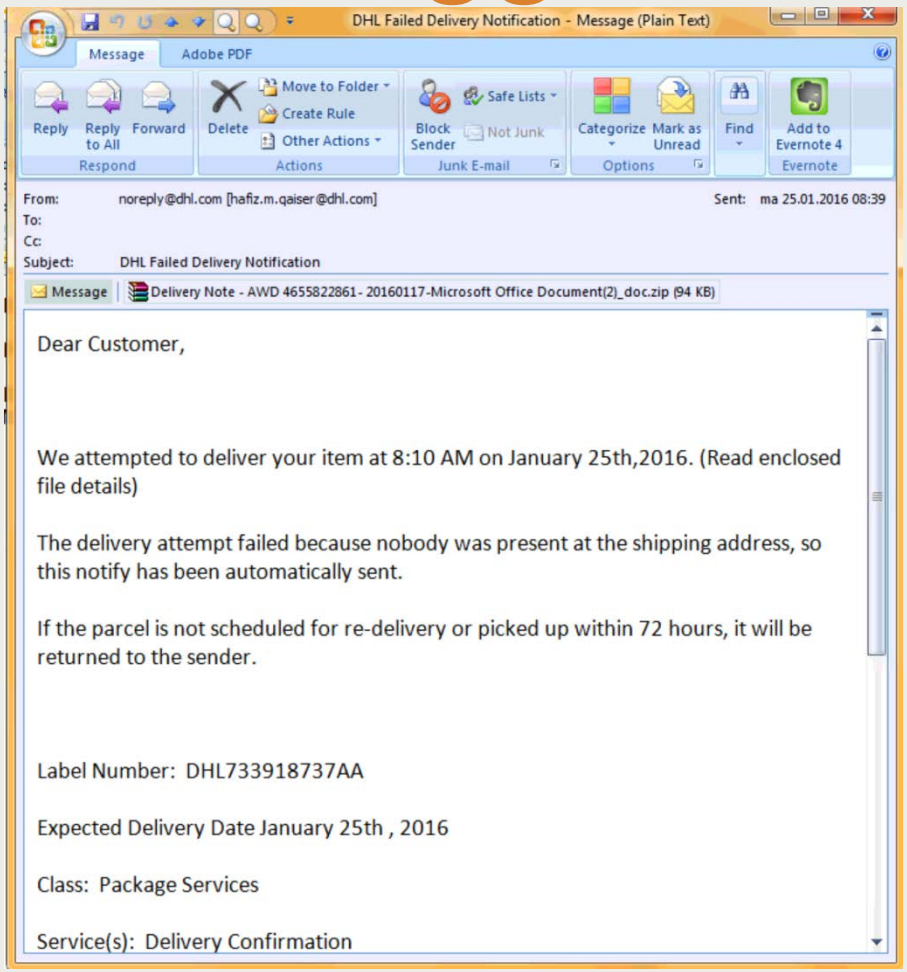
Gå inn på siden uavhengig av e-post lenken

- Om selskaper som Paypal vil ha bekreftelse, gå rett inn på siden, ikke klikk på lenken.



E-post med vedlegg

- Står det hva vedlegget er?
- Kjenner du avsender personlig?
- Hva er formatet?
- To formatter som ofte er trygge:
  - PDF
  - JPG
- Zip? NEI!
- Docx; Xlsx, Pptx ?
  - Kun om du er sikker; MEN, best å sjekke!



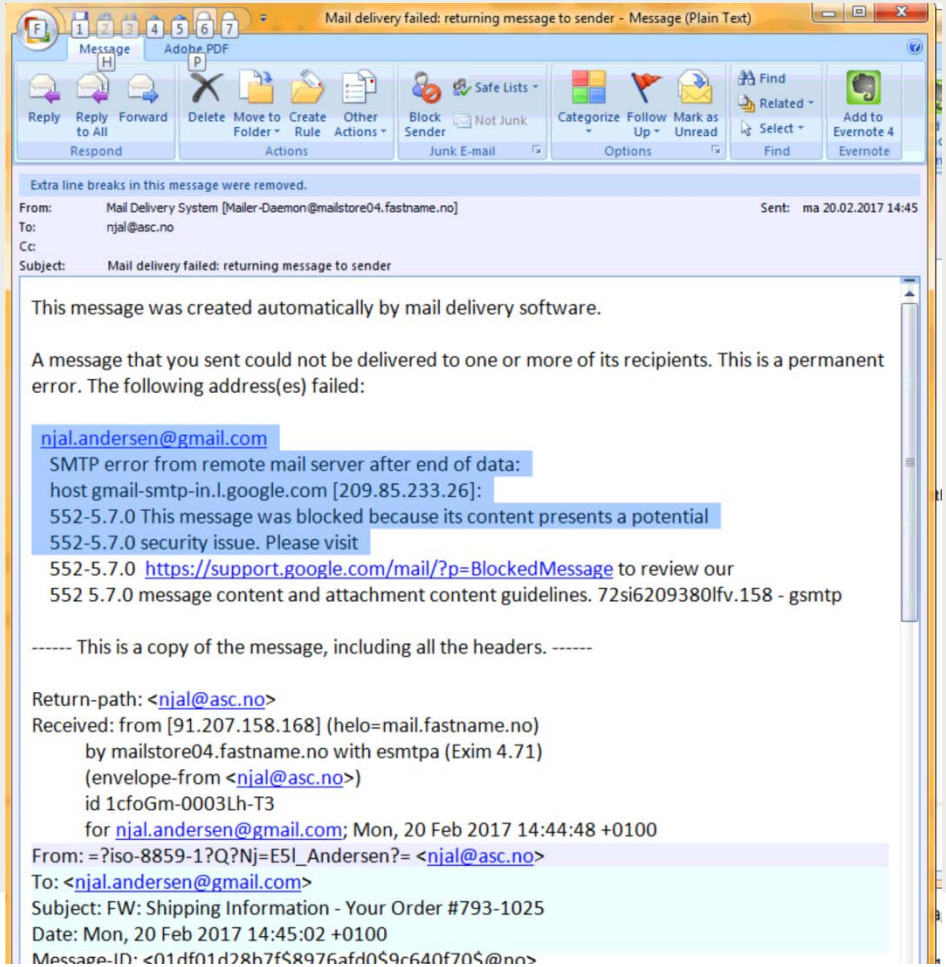
E-post fra en du kjenner.. med vedlegg

- Venners e-post kan hackes.
- Enhver kan sette avsender som de ønsker; så sjekk at innholdet er kjent også.

ASC

Videresend til en Gmail konto; blir den nektet: Slett den

- Er det virus, blir den nektet.
- (Google har svært oppdaterte filtre og viruskontroll)



ASC

Blir du utsatt for «løspengevirus»

Game over. You lost.

ASC

Da er du prisgitt det du gjorde FØR du ble infisert

Tenk Real Time backup.

ASC

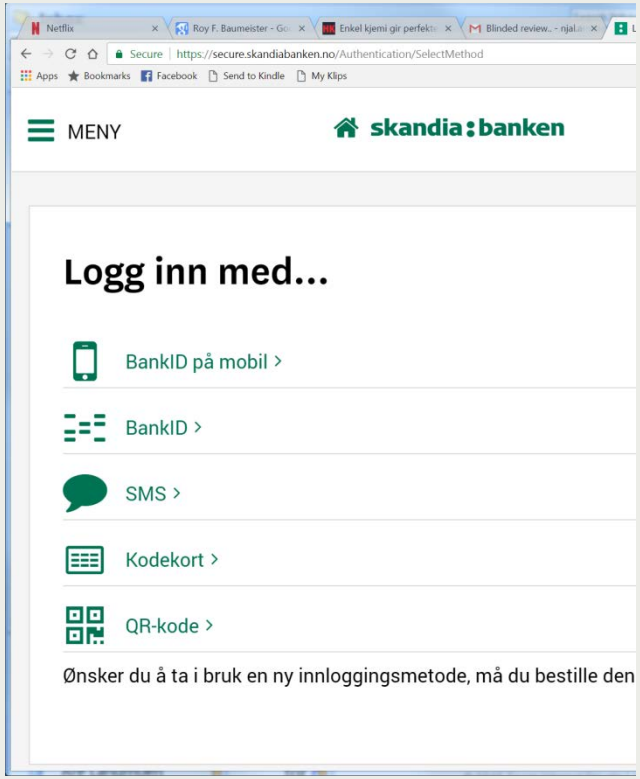
Ikke bare e-post...

- Konkurranser på Facebook og andre sider, mange med med flotte premier
- «IQ tester»
- Spill m.m.m.

→ Mye som er bra! Men vær SVÆRT var om du skal installere noe som helst.

Passord er de nye nøklene til det meste

- Nettbanker, det offentlige (Altinn m.fl.), Legesentre, Vipps m.fl.
  - Bruker SMS; BankID etc. fordi de vet de ikke kan stole på kunder for å ha gode og sikre passord.
  - Dette er relativt dyrt, så de færreste krever dette.



Hva er et godt passord?

Passord	Tid å hacke
123456789	25 nanosekunder
Liverpool	Instantly
Ark2005!	9 timer
«Njal er festlig»	330 milliarder år

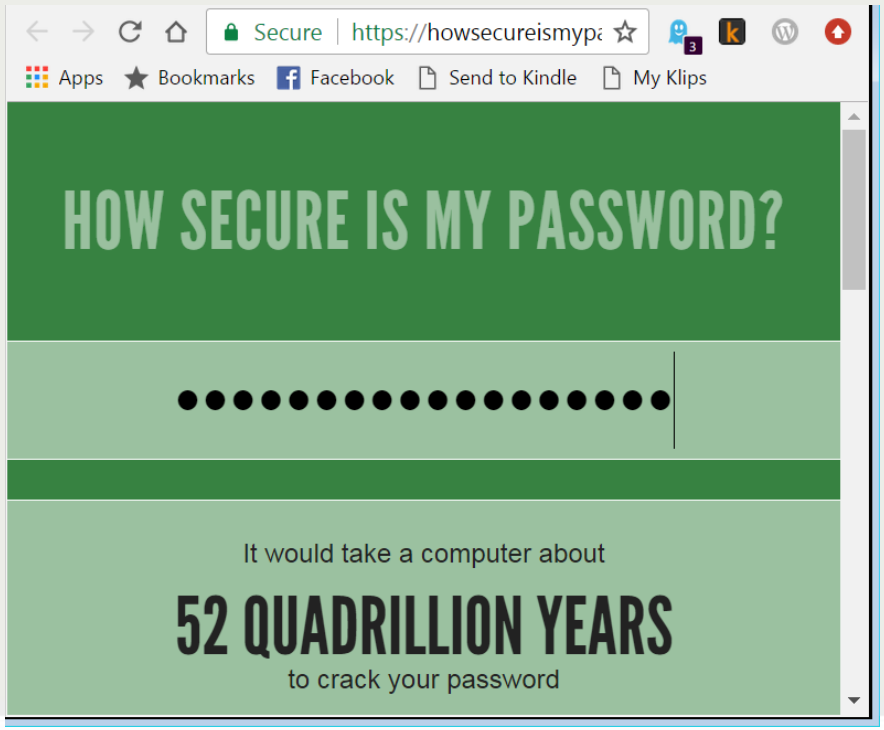
ASC

En setning er overlegent!

Passord

- «Njal skremmer meg!»

Time to crack



Hvor mange passord?

- Hva skjer om du har glemt et passord?

→ Nytt blir sendt til din e-post adresse.

Du må ha flere passord!

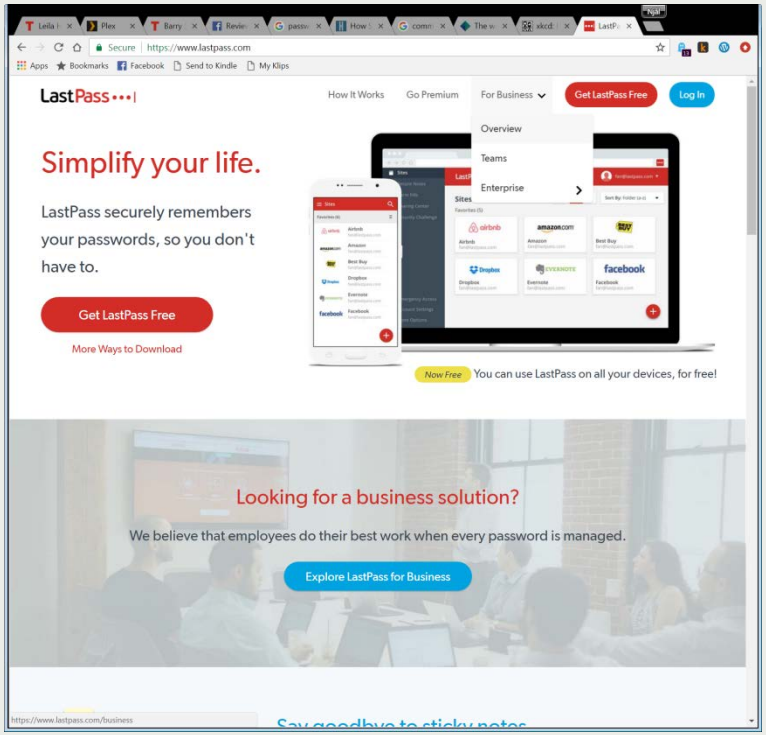
- Om en tjeneste blir hacket og passordet kommer på avveie, kan hackere få tilgang til alle konto med samme passord.
- Får de tilgang på e-post kontoen din, kan de få tilgang til neste alle andre også!

→Ha et EGET og SIKKERT passord for e-post!

→**BRUK 2 stegs passord** om mulig. F.eks. hos Gmail.

Gode råd

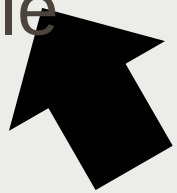
- TENK før du klikker
- Bruk sikre passord
- Ikke logg inn på offentlige maskiner, og gjør du det, IKKE lagre det



.. Fire klikk, så har jeg alle lagrede passord

- Dette gjelder både hjemme maskin og offentlige.
- Hvem har tilgang på din maskin hjemme?

- (Bilde er fjernet: men viser hvordan alle lagrede passord i nettleseren er tilgjengelig for alle som bruker maskinen!)



ASC

Gode råd

- TENK før du klikker
- Bruk sikre passord
- Ikke logg inn på offentlige maskiner, og gjør du det, IKKE lagre det
- Aller best: bruk tjeneste som Last pass
- Ha en god sky-basert backup, og bruk den! Dropbox; OneDrive etc.