

# Kom på nettet – uden at gå i nettet

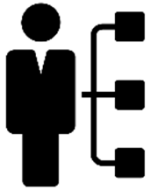
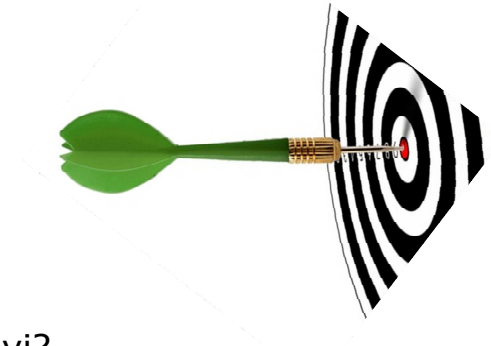
Lars Thomsen & Bjørn Mose

# DISCLAIMER



- Øjebliksbillede
- Så snart noget ligger fast, ændres det – eller
- Hvis noget er sikkert i dag så er det ikke nødvendigvis sikkert i morgen!

# Fokuspunkter



- Center for Cybersikkerhed – Hvem er vi?

- Hvad er det vi prøver at beskytte?

- Truslerne



- Vurdering af konsekvenser ved brug af nettet



- Truslerne fra din mailboks

- Sikker surfing



- Samarbejde med andre

- Råd til bedre sikkerhed

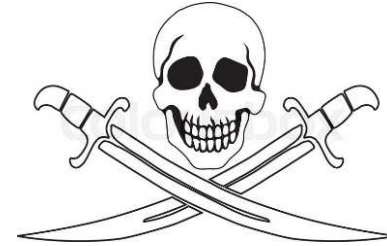
- Passwordsikkerhed

- Mobile enheder

# Hvad er det vi prøver at beskytte?

- Informationer
  - Tilgængelighed
  - Integritet
  - Fortrolighed





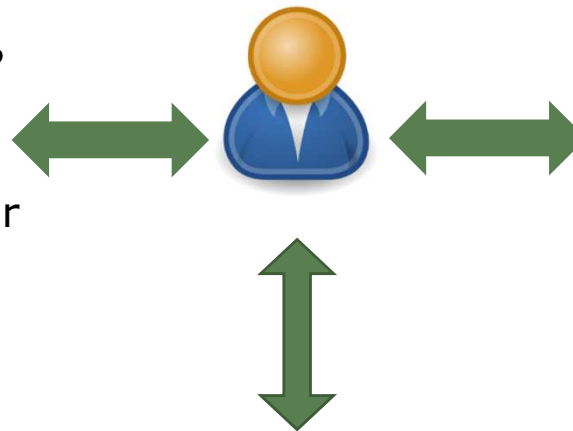
# Truslerne

- Udnyttelsen af de digitale muligheder påfører os risici
  - de skal vurderes
- Forskel på truslerne mod private, mod virksomheder, mod staten
- Typer af trusler
  - De menneskeskabte
    - Fejl
    - Med vilje; tjene penge, hugge informationer,
  - De ikke menneskeskabte

# Vurder konsekvensen ved brug af nettet

## Privat brug af internettet

- Hvad lægger jeg ud og hvor?
- Hvad tager jeg ned?
- Hvem giver jeg adgang?
- Hvad hvis uvedkommende får adgang?



## Arbejdsrelateret brug af internettet

- Hvad lægger jeg ud?
- Hvor lægger jeg det?
- Kan det misforstås/misbruges?
- Hvad får jeg med tilbage?

## Brug af foreningens it-plattform

- Hvem har adgang?
- Hvad hvis uvedkommende får adgang?



# Truslerne fra din mailboks

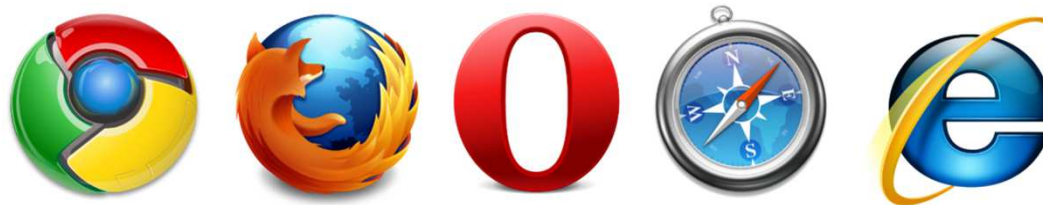


- Din mailboks er som udgangspunkt åben for alle indkommende mails!
- Virus og spam-filtre fanger meget, men ikke alt!
- Phishing og specielt spear phishing mails kan i dag være svære at undgå.
- Det dig som modtager, der i sidste ende kan/skal afgøre om en mail er falsk

## Derfor:

- Undgå om muligt at klikke på link i en mail - Brug "hoveddøren" i stedet
- Hvis mails er truende eller opfordre til hurtig handling – STOP og tænk!

# Sikker surfing



Du eksponerer dig selv og din organisation for en række trusler når anvender en browser:

- Hjemmesider kan indeholde malware, som du potentielt får når du besøger dem.
- Typosquatting, URL hijacking, Sting sites, falske URL'er er "fælder" som udnytter at du taster forkert i adresse-linjen i din browser.
- En grøn hængelås er ikke en garanti for at siden er sikker at besøge.



# Samarbejde med andre



- Centrale retningslinjer fra Ældresagen
  - Hvordan skal jeg håndtere de systemer jeg får adgang til?
  - Hvordan skal jeg håndtere de informationer jeg får adgang til?  
Også på print
- Andre samarbejdspartner; serviceleverandører
  - Hvilke aftaler forligger der og hvad kan jeg forvente?
  - Hvad bør jeg selv gøre?

# Råd til bedre sikkerhed – det basale

- God anvendelse password
- Opdater dine programmer
- Beskyt dine enheder mod malware
- Tag sikkerhedskopi
- Brug trådløse netværk på en sikker måde



# Passwordsikkerhed

- Brug gode passwords
- Brug Fler-faktor autentifikation
- Genbrug ikke dit password
  - Hjælp til håndtering af overflod af password
- Brug ikke standardpassword



# Det gode password

- Følgende passwordeksempel er lavet ved at tage de to første bogstaver, det første med stort, fra ordene i en sætning.

*Husk! Bestil 1000 liter olie til fyret = **Hu!Be1000L.OITiFy***

- I det næste eksempel er ordene enten lavet til forkortelser, erstattet af specialtegn, eller der er kun benyttet det første bogstav.

*Danmark blev nummer fire til europamesterskabet i fodbold i 1964  
= **DKb#4=EMif-64***

# Det gode password

- Andet bogstav i hvert ord er med stort, og der er med vilje lavet stavefejl.

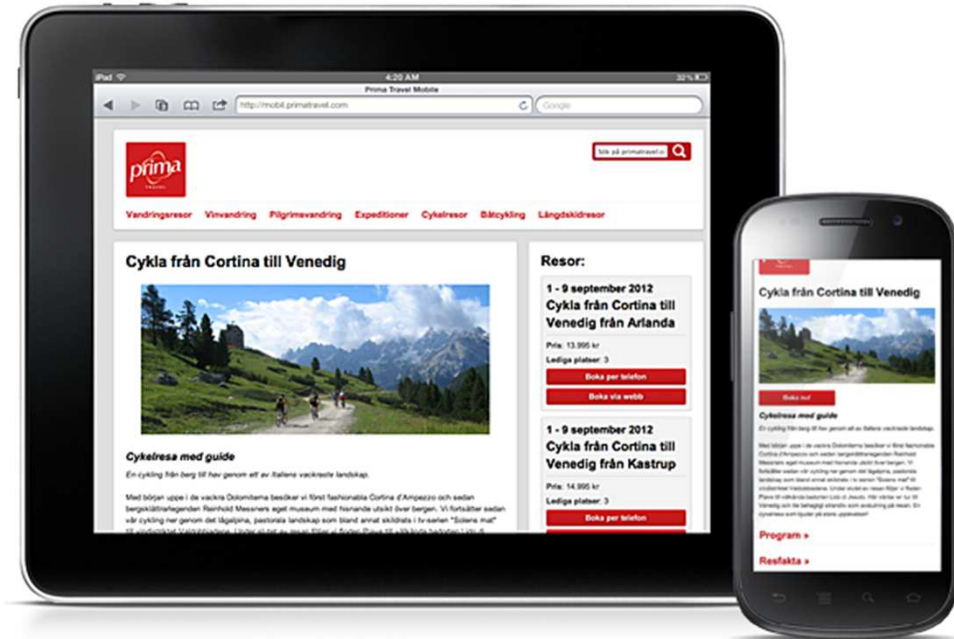
Eksempel: cykle motion stol paradys = **sYklemOtjonsTolpAradis**

- Sidste bogstav i hvert ord er med stort.

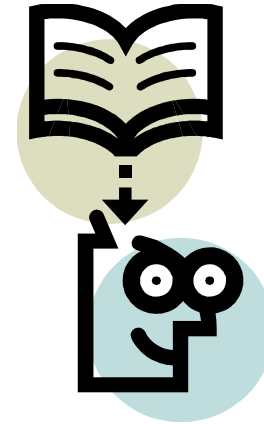
Eksempel: abrikos hospital zebra spark =  
**abrikoShospitaLzebrAspark**

# Mobile enheder

- Brug adgangskode
- Krypter enheden
- Opdater
- Luk låget
- Backup
- Brug Wi-Fi med omtanke
- Brug VPN
- Slå bluetooth fra
- Slå lokalitetstjenester fra



## Læs mere



Se publikationer på [Sikkerdigital.dk](https://sikkerdigital.dk)

Af CFCS egne publikationer vil vi gerne fremhæve:

- [Cyberforsvar der virker](#)
- [Passwordvejledning](#)
- [Reducér risikoen for ransomware](#)
- [Råd om sikkerhed på mobile enheder](#)
- [It-sikkerhed på rejsen](#)

