Hva er informasjonssikkerhet:

* CIA
  + CIA er forkortelse for «Konfidensielt (Confidentiality), Integritet (Integrity), Tilgjengelighet (Availability).
  + Vi oppnår konfidensielt ved å omforme data for å gjøre de sikre ved hjelp av kryptografi. Vi sjekker for tilgangs kontroll. Videre er det nødvendig med autentisitet for å sikre tilgang for kilder av rett person med de nødvendinge tilgang tillatelser. Dette kan vi videre oppnå ved hjelp av «To fase autentisitet» (IMSI).
  + Integritet handler om å unnvike uautoriserte endringer av data samtidig å ha data sikret i en «backUp». Man kan også gjøre krypteringer med «Checksum» for å sjekke integritet i de innkommende data.
  + Tilgjengelighet betyr å ha data tilgengelige for autorisert person til rett tid.
  + Drøfte: Data sikkerhet er nedfelt i EU lov om GDPR i 2018 der de som oppbevarer personalopplysninger må sikre tilgang til slike data, inklusive IP adresser.
  + CIA er viktig i forhold til phising, malware, network: sniffing, ARP spoofing, port scanning, session hijacking, DOS Attack, SQL Injection, XS Scripting.

Trusler mot personer:

* Største trusler:
  + De største trusler i dag er tyveri av identitet, personopplysninger, passord og annet informasjon av personlig karakter slik som bank informasjon og helseopplysninger. Videre er vi utsatt for overvåkning av våre data og web søk der selskaper prøver å påvirke våre oppfattinger, våre vaner, våre meninger og vår adferd. Noen steder fins det «social credit score» der innbyggene er utsatt for overvåkning av hva de har sakt, hva de har skrevet, hva de har gjort og hvor de har vært. Dette påvirker individets rettigheter og muligheter i samfunnet.
* Tiltak for å redusere risiko:
  + Vår data sikkerhet kan økes ved hjelp «A.A.A.»:
    - Ved autorisasjon som er ikke kompromittert.
    - Opprettholdelse av regler, tillatelser og sikkerhets mekanismer
    - Anonymitet, Proxy server, pseudonymer, oppdatering av programvare, VPN samt andre makansismer som holder vår identitet skult.
  + Videre «A.C.L.»:
    - Ved hjelp aksess kontroll av bruker gjennom autorisasjon, passord, filbeskyttelse og rolle hierarki som bestemmer tilgangsrettigheter.
  + Videre «Kryptografi»:
    - Vi sikrer våre komisaksjoner over sikrede kanaler slik som HTTPS, AES, RSA, Diffie-Hellman, EFS, Public Key Cryptatation, Block Chiffer, Tunneling og likende.
  + Fysisk sikring:
    - Vi sikrer våre data ved fysisk adgangskontroll slik som låsing av rom, ikke dirkbare låser/hengelåser (minimum nivå 4), ingen knus-bare vinduer, overvåkning, vekter sikkerhet/opplæring.