IN1020 – UKE 2

Datasikkerhet og datanettverk

av trondvq@uio.no

Plan for idag

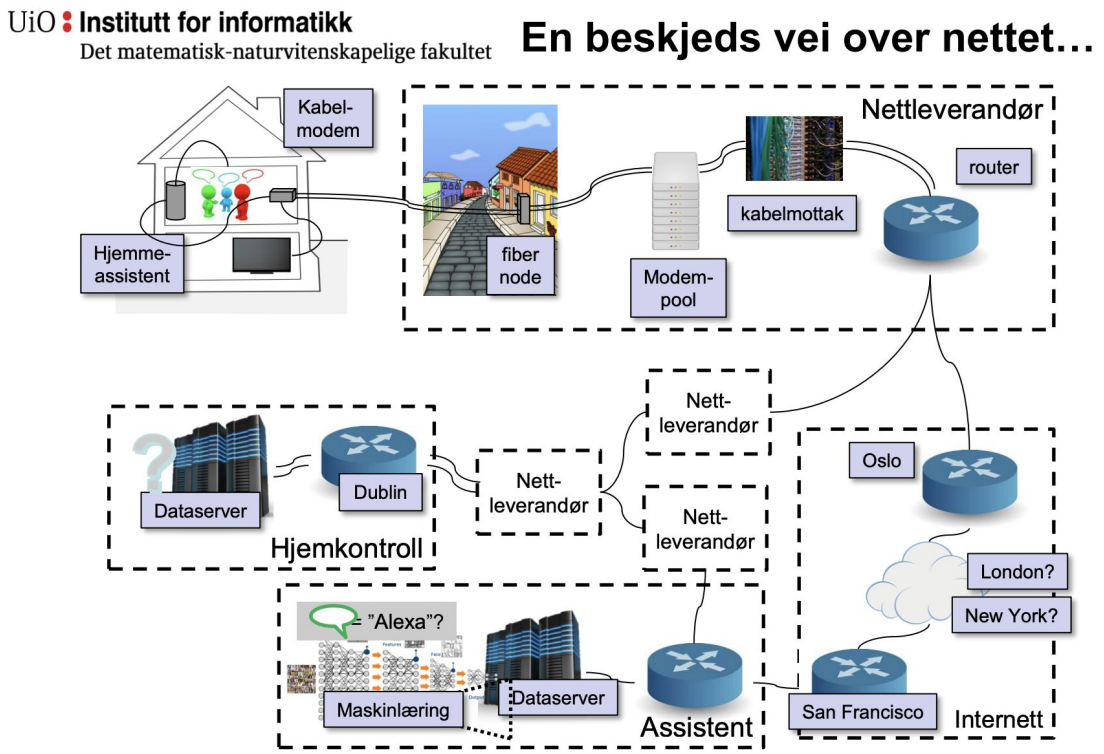
1. Repetisjon av pensum (litt lang)
2. Case-oppgave (Targeted Advertising)
3. Oblig/Ukesoppgave/Fri tid ☺️



Gyros!

Litt Datanettverk

Data**nettverk** – handler om å koble maskiner sammen.



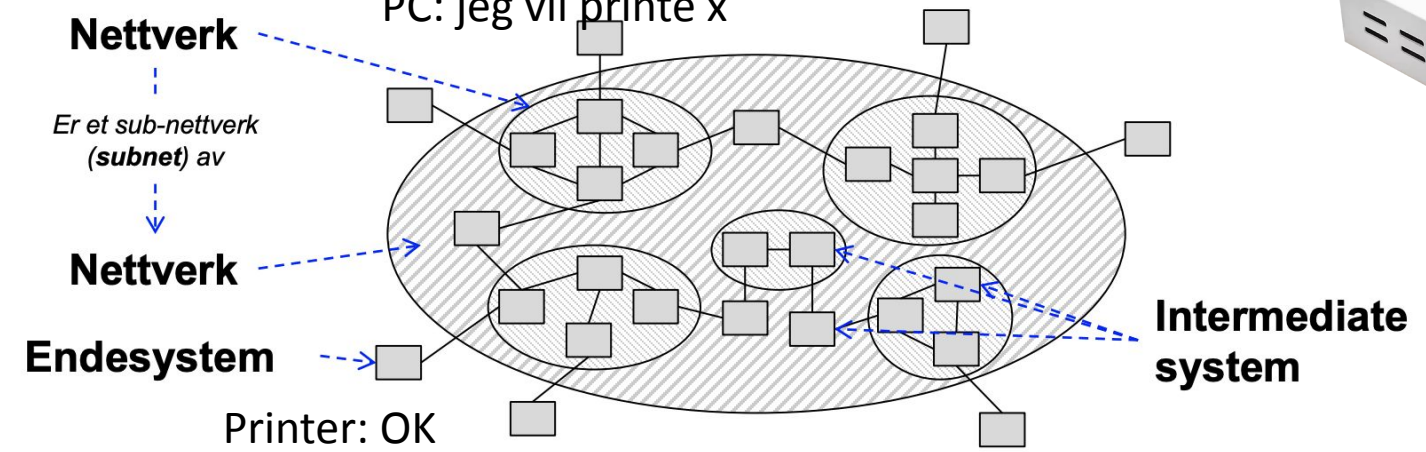
Komponenter i nettverk

- Tjenere (server)
  - Store datamaskiner som oppfyller forespørslene til klienter i nettverket.
  - Kjører programvaren vår. F.eks. Alexa.
- Klienter
  - Endebruker-system som sender forespørsler til tjenerne (oppretter forbindelse)
  - F.eks. PC-en du bruker
- Switcher
  - Enhet som kan koble noder sammen, en mellommann som videresender ting. Vet ikke helt hvor de skal sende de, men sender den i riktig retning. Dette får de vite via. MAC-adresser.
  - Hovedfunksjonen til en switch er å koble sammen endesystemer. Styrer datatrafikken mellom noder.
  - F.eks. switch
- Rutere
  - En enhet som videresender datapakker gjennom datanettverk. Vet hvor de skal.
  - F.eks. Wifi-ruteren hjemme
  - Hovedfunksjonen til en ruter er å koble to forskjellige nettverk sammen. Kan også oppføre seg som en switch.
  - Noen rutere har innebygd switch.

Komponentene i nettverket









Endesystemer:

- Endesystemer finnes helt ytterst i nettverket
- For eksempler: datamaskiner, mobiltelefoner, sensorer, skrivere

* Klient tjener

Intermediate system:

- For eksempel:
  - ruter, switch
  - gateway
  - repeater, bridge

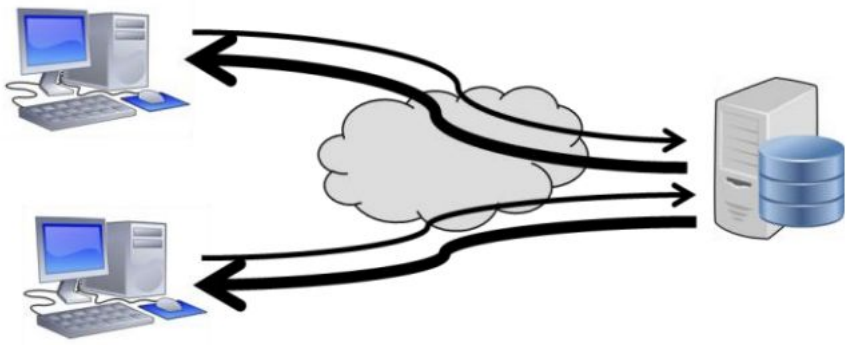


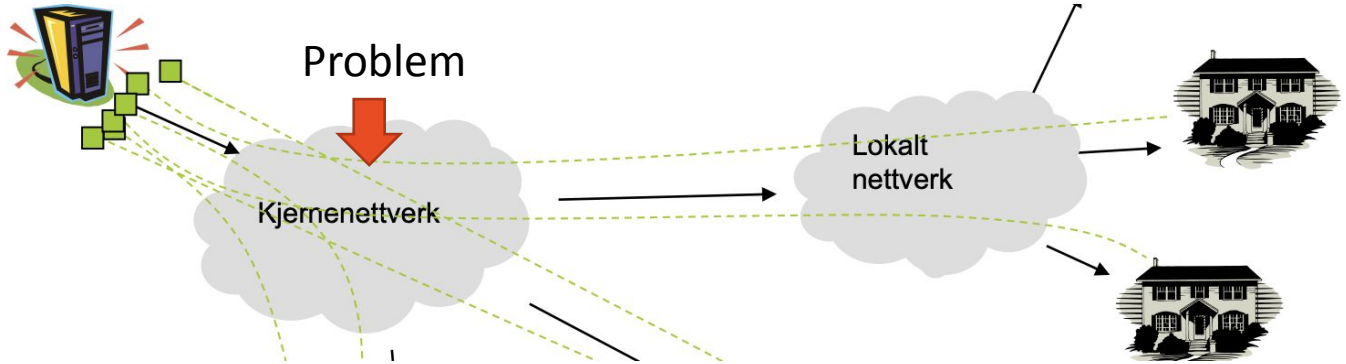
Aksessmodeller – måten man kommuniserer i datanettverket

Klient-tjener

- Klient ber om tjeneste -> oppretter forbindelse
- Tjenere leverer tjenesten - > svarer forespørsel
- Eksempel: Sjekke når bussen går via. Ruter-appen.

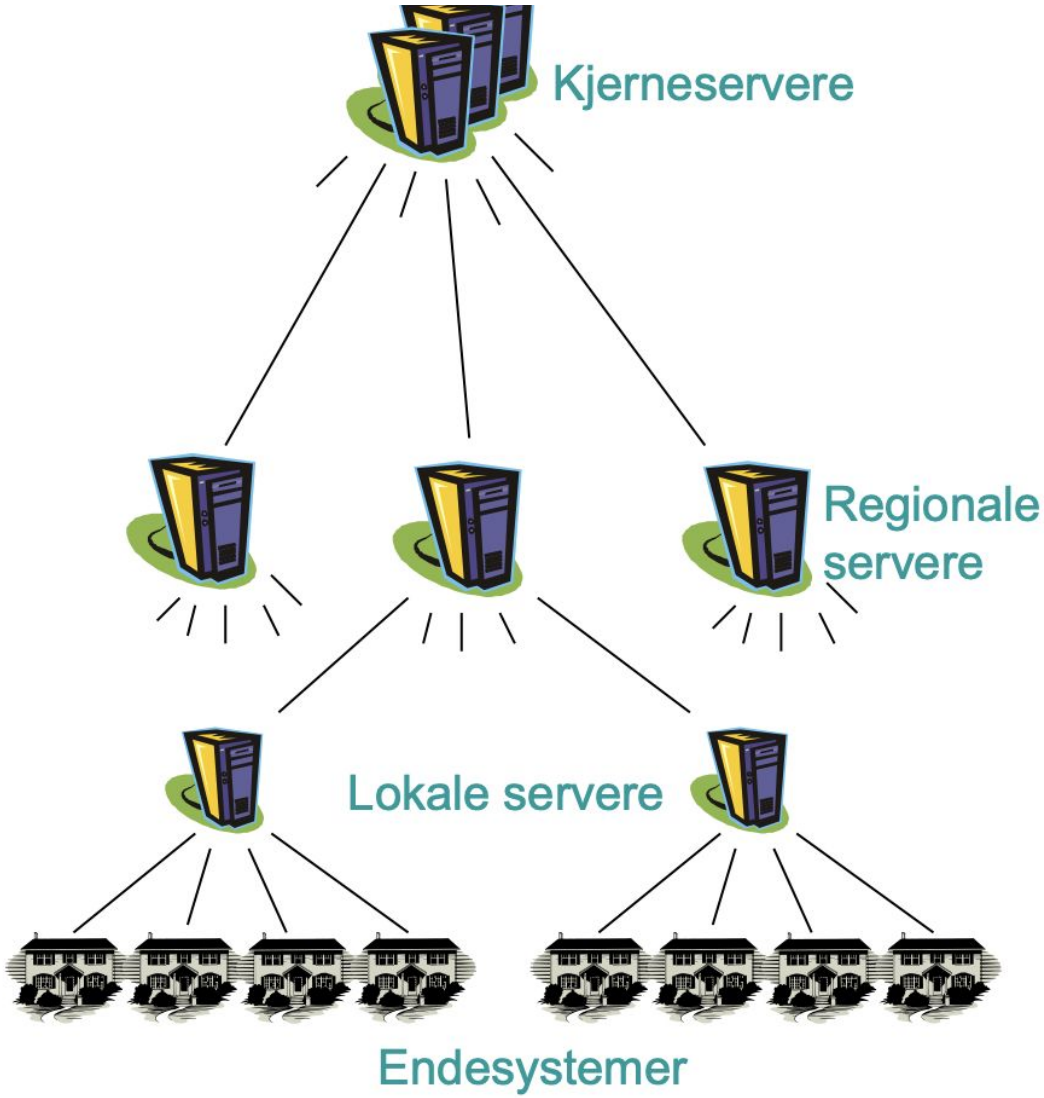
- Potensielt store kostnader med å få infrastrukturen skalerbar





Løsning: CDN (Content Distribution System)

- Deler dataen i en hierarkisk struktur
- Istedenfor at alt ligger et sted, blir kopier lagret rundt omkring.
- Populært innhold lagres nærmere sluttbrukere: f.eks. lokale tjenere(servere)
- Ikke så populære lagres på eller nære kjerneserveren: f.eks. Regionale tjenere(servere)
- Unngå flaskehals.
- Nyttig struktur hvis båndbredden er begrenset
    - F.eks. På flyet: kun noen nettsider er tilgjengelige.



Peer-to-peer (P2P)

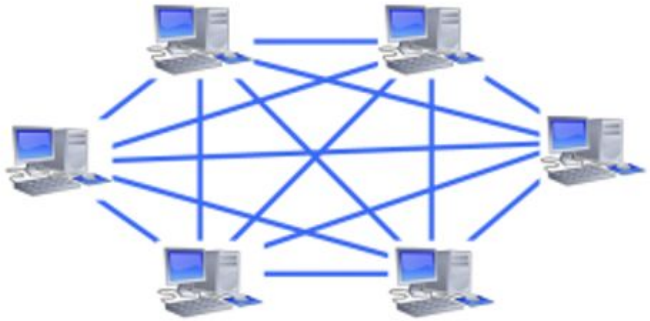
- Alle noder likeverdige
  - (kan være både klient og tjener)
- Alle noder kan nå hverandre
  - Sikkerhetsutfordringer
- Eierskapet er distribuert
  - Vanskelig å finne data
- Eksempler: Torrent, Napster

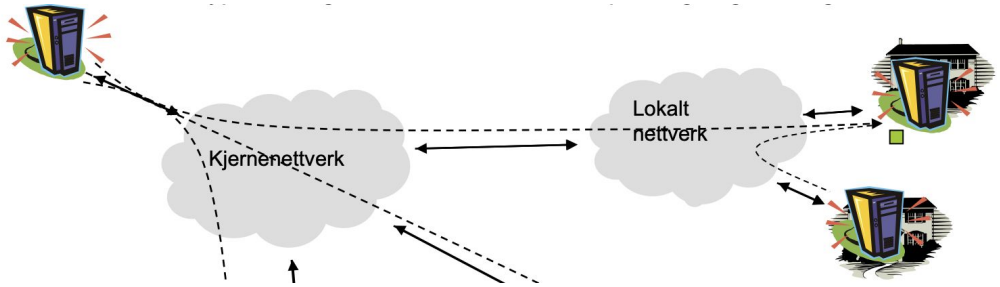
På flere måter likt CDN:

- Endesystemer kan være både klient og tjener
- Distribuert lagring
- Innholdet nærmere sluttbruker
- Begrenset lagring per endesystem

Men ulikt på noen punkter:

- Ingen klare roller på endesystemene
- Ikke noe hierarkisk forhold
- Klienter vet nødvendigvis ikke hvor innholdet er
  - Trenger protokoller for å «oppdage innhold»
- Endesystemer i et P2P nettverk kommer og går





Nettverkstopologier – Hvordan bygge nettverket

Punkt til punkt nettverk – kommunikasjon mellom to parter

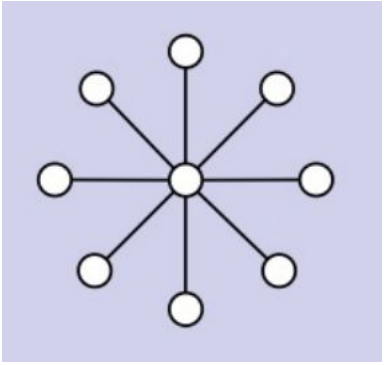
- Stjernetopologi – switchen/ruteren er i sentrum
  - Vanlig i hjemmenettverk
- Kan utvides til tretopologi
- Finnes flere som: Mesh,Ring,Torus etc.

Broadcast nettverk – alle koblet sammen

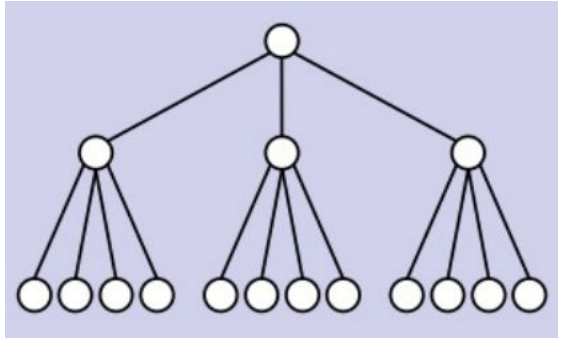
Kabel: Ethernet kabel

Radio: Wifi, Mobiltelefon: 4G, 3G.

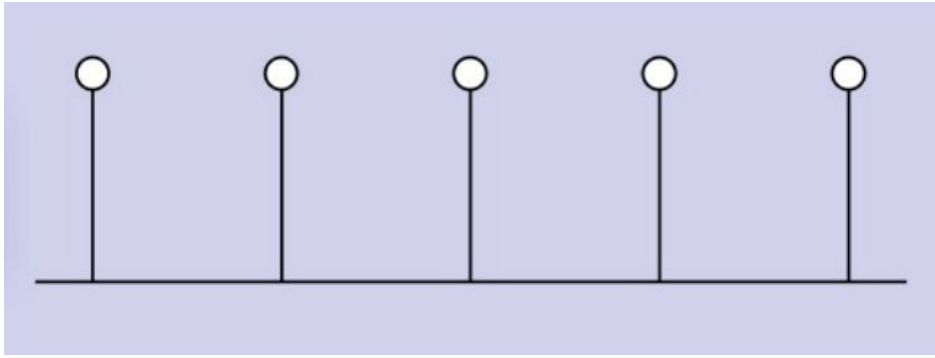
- Egenskaper:
- Når en node sender kan potensielt alle høre!
  F.eks. Når du bruker wifi på et shady hotel.
- Kan bli problemer hvis to noder sender samtidig
  - Sending bør koordineres…
- Feildeteksjon er viktig!



Stjerne



Tre



Nettverksprotokoller – et sett med regler

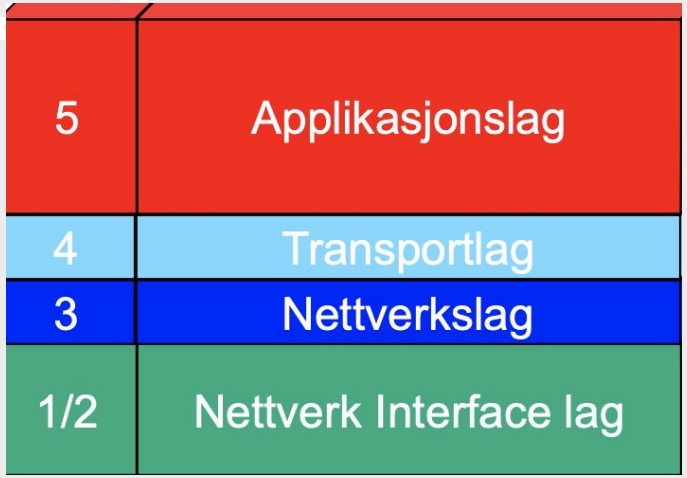
- Uten protokoller: ingen regler, hvor skal informasjonen sendes?
- En protokoll definerer strukturen på beskjeder sendt over et nettverk
- Eksempler på protokoller: TCP , UDP, IP
- Mange ting vi må ha regler over I nettverkskommunikasjon





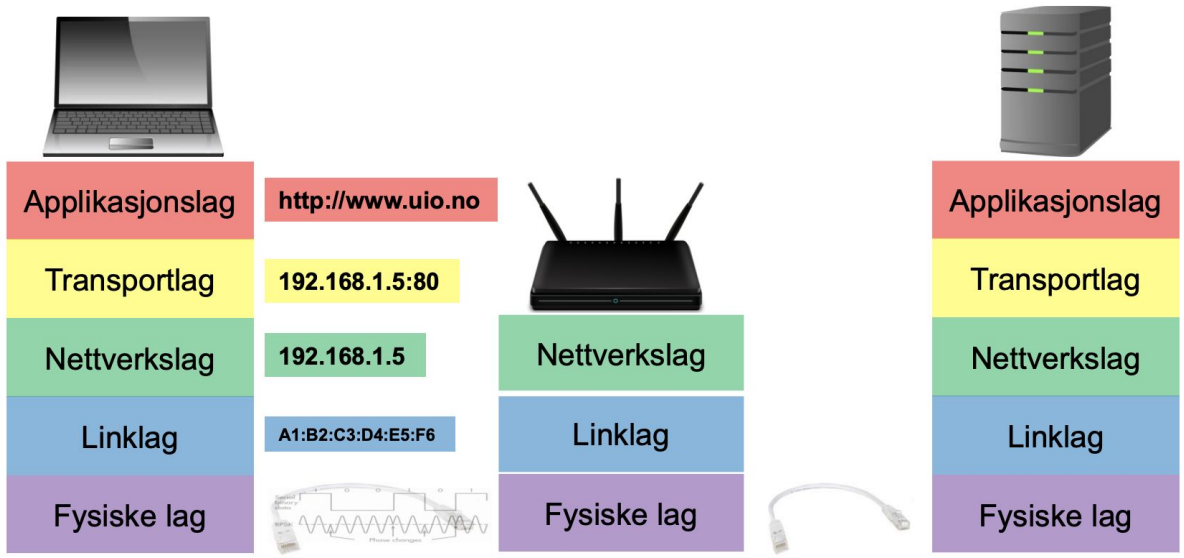
Løsning: Lagdeling

- Klar ansvarsfordeling
- Lagene kan byttes ut
- Kan utvikle lagene uavhengig
- Vi ser på femlags(eller fire)-modellen: TCP/IP-modellen
  - En modell for nettverkskommunikasjon



Litt om lagene

	Lag	Funksjon
5	**Applikasjon**	Applikasjonsrelaterte tjenester (**HTTP**, **Mail**)
4	**Transport**	Kobler sammen systemene ende-til-ende (**TCP/UDP**)
3	**Nettverk**	Sende data fra ende-til-ende systemer (**IP**)
2	**Link**	Pålitelig overføring mellom to noder (**LAN/WiFi**)
1	**Fysisk**	Sender bit ut på mediet (kablet eller trådløst)



Litt om datasikkerhet

Autentisering - Tilgangskontroll

Autentisitet vs. **Autentisering**

Autentisitet = Hvor sikre er vi på at noe/noen er den/det de utgir seg for å være

- Sikkerhetsmål

Autentisering = Å bekrefte en hevdet identitet.

- Sikkerhetstiltak
- Flere typer: Brukerautentisering, Systemautentisering, Organisasjonsautentisering, Autentisering av dataopprinnelse.
- Autentiseringsfaktorer= noe du vet, noe du er eller noe du har.
  - Vet: Passord, er: Ansikt, har: Kodebrikke.
  - Fler-faktor: flere faktorer kombinert. F.eks. Passord + mobiltelefon.

Tilgangskontroll

- Tilgangskontroll = Autentisering + Autorisering
  - Autorisering: å spesifisere tilgangsrettigheter til dataressurser
- Tilgangskontroll innebærer å sjekke om et subjekt har tilgang til å utføre en ønsket handling på et objekt, etter forhåndsdefinerte regler»
    - F.eks. Anne vil lese innholdet i en fil

Targeted Advertising

Gå på: https://adssettings.google.com/authenticated eller søk opp “google ad settings”.

1. Hva synes dere om dette?
2. Hvilke innvirkninger har dette på personvern?
3. Hvilke trusler finnes det ved bruk av slik teknologi?
4. Hvilke sikkerhetstiltak kan man foreta for å unngå at dataen ender opp I feil hender?
5. Denne dataen lagres ofte på google servere. Hva er spesielt viktig da?

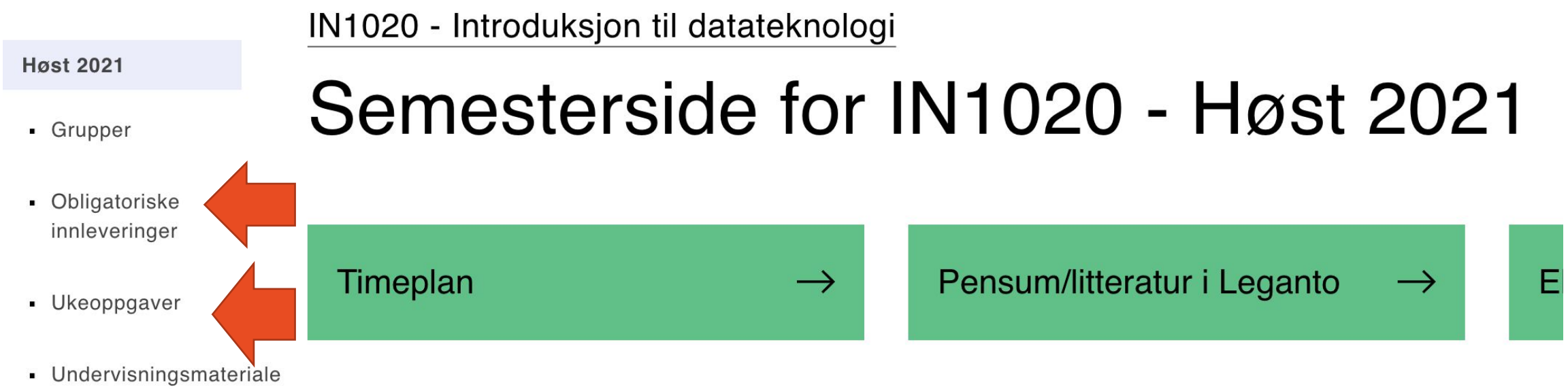
Har passordet ditt blitt lekket?

https://haveibeenpwned.com

https://haveibeenpwned.com/Passwords

Oblig/ Ukesoppgave/Fri tid

- Gå på semester siden
- Jobb sammen! (2-3 per)
- Første oblig frist 15.9.



Spørsmål?

Kontakt informasjon:

- trondvq@uio.no
- studieinfo@ifi.uio.no
- Mattermost: mattermost.uio.no
- Discord: https://discord.gg/5jUpWjkQew

