

UiO : Institutt for informatikk

Hvordan hackes vi?

(og hvordan unngå å bli rammet)

IN1020 – Introduksjon til datateknologi
26.08.2026

Kristin Skar
kritisk@ifi.uio.no

Datateknologi og sikkerhet

Tema for tema:

1. Datasikkerhet - Er det så viktig da? (19. aug)
2. Å innfri sikkerhetsmål: Autorisert og uautorisert tilgang (21. aug)
3. **Hvordan hackes vi? Trusselaktører og angrepsvektorer (26. aug)**
4. Kryptografi – nøkkelen til (fungerende) digital samhandling (9.sept)
5. Trygg infrastruktur og sikre datasystemer (18.sept)
6. Å skape trygge digitale tjenester krever innsats (23.sept)

I dag: Hvordan hackes vi?

Ressurser:

- Forelesning 26.08.26
- Ukeoppgaver og pensumlitteratur:
  - Jøsang: Kap 2, 11.7, 13.1-13.5

Nøkkelord:

- Trusselaktør
- Angrepsvektor
- Skadevare
- Sikkerhetstiltak
- Sikker datalagring
- Applikasjonssikkeret:
  - SQL-injeksjon
  - XSS
- Sosial manipulasjon

Repetisjon

- **Entitet**: Noe med en fysisk, juridisk eller prosessuell eksistens.
- **Identitet**: *Representasjonen* av en entitet.
- **Autentisering**: Å *verifisere* en påstått identitet.
- **Autorisering**: Å *spesifisere* tilgangsrettigheter.
- **Tilgangskontroll**: Å *håndheve* tilgangsrettigheter.

- Kan sammen *entitet* har flere ulike *identiteter*?



Trusselaktører - oversikt

	Trusselaktør	Motivasjon
1)	Stater og statssponsede organisasjoner	→ Geopolitiske interesser
2)	Cyberkriminelle organisasjoner	→ Økonomisk vinning
3)	Hacktivister	→ Ideologiske interesser
4)	Terroristorganisasjoner	→ Voldelige ideologiske interesser
5)	Spenningssøkende amatørhackere	→ Ønske om spenning og anerkjennelse
6)	Utro tjenere i virksomheter	→ Misnøye, økonomisk vinning, eller ideologi

Hackere er (stort sett) ute etter:

Hva:

- Tilgang til informasjon
- Endre/forfalske informasjon
- Utilgjengeliggjøre informasjon

Hvordan:

- ID-tyveri
- Utnytte sårbarheter i programvare/systemer/infrastruktur
- Få noen til å gi deg det du vil ha

Angrepsvektor: Hvordan hackes datasystemer?



Definisjoner

- (Digital) sårbarhet: En feil, mangel eller svakhet i et IT-system som gjør at det kan utnyttes (angrep gjennomføres).
- Nulldags-sårbarhet: Sårbarhet som noen har kunnskap om, *før* produsenten/leverandøren eller brukerne av systemet/programvaren kjenner til den.
- Sårbarhetsflate: Summen av (de potensielle) sårbarhetene i et system som kan nås og utnyttes av en angriper.
- Skadevare: Samlebetegnelse på programvare som har som mål å gjøre skade.
- Angrepsvektor: Metoden en angriper bruker for å utføre et angrep på en datamaskin, et nettverk eller et datasystem

Et utvalg av typer skadevare:

 Løsepengevirus	Kjennetegnes ved at det krypterer kritiske data på offerets IT-systemer, slik at data og applikasjoner ikke fungerer og blir utilgjengelige.
 Dataorm	Skadevare som på egenhånd er i stand til å spre seg og finne nye ofre.
 Trojaner	Skadevare som utgir seg for å være et nyttig program.
 Bakdør	En ubeskyttet og ukjent åpning inn i et datasystem, laget av en angriper.
 Spionvare	Programvare for å spionere på en bruker i håp om å få tak i f.eks. informasjon, passord, kontoinformasjon.
 Tastelogger (Keylogger)	Et program, eller en enhet som er koblet til tastatur eller maskin, og som lagrer eller videresender alle tastetrykk. En variant av spionvare.
Rootkit	Skadevare som endrer eller erstatter funksjoner i OS eller applikasjoner, med mål å ta kontroll over en maskin eller et system.
Exploit	Et program, en sekvens med data, eller en oppskrift på hvordan en sårbarhet kan utnyttes.

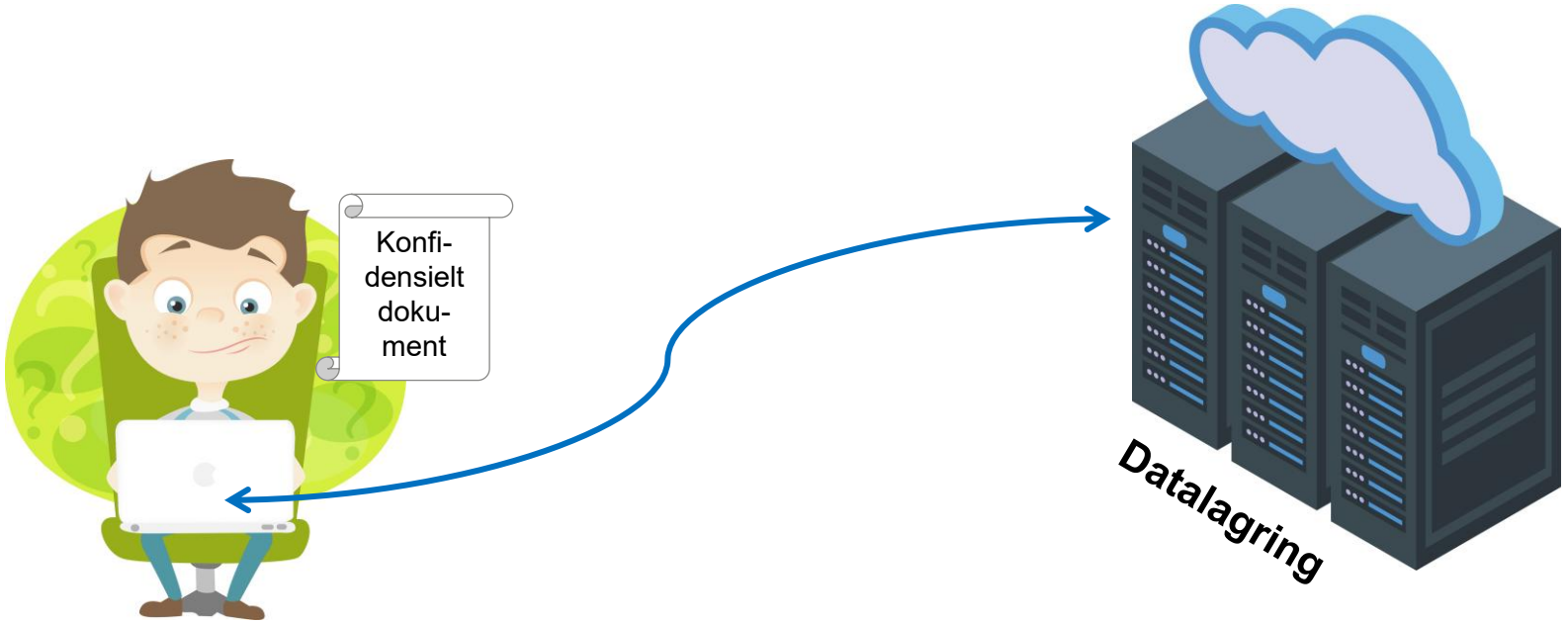
(Gruppene er til dels overlappende, og ikke alltid presist definert.)

Sikkerhetstiltak: Ivareta sikkerhetsmål





Øvelse: Angrepsvektorer? Sikkerhetstiltak?



Hvordan ivareta sikkerhetsmål? Innføre *sikkerhetstiltak*

For alle *datatilstander*

- Lagring
- Overføring
- Bruk

I ulike *faser* (av et IT-system)

- Forebyggende
- Detekterende
- Korrigerende (gjenopprettende)









Beskytte *lagret* informasjon







Beskytte informasjon under lagring

- Riktig tilgangsautorisasjon og tilgangskontroll for lagrede data understøtter konfidensialitet og integritet:
  - Bare entiteter som skal ha tilgang innvilges tilgang.
- Å kryptere lagrede data understøtte konfidensialitet:
  - Sørger for at informasjon er uleselig/uforståelig for utenforstående.
  - *Eksempel: Laptop mistes/stjeles, datainnbrudd på server/tjener der data lagres*.
- Sikkerhetskopiering for å ta vare på informasjon over tid:
  - Bidra til økt tilgjengelighet ved å være i stand til å gjenopprette systemer og data ved uønskede hendelser som endrer eller sletter informasjon.
  - *Eksempel: Angrep med løsepengevirus, datainnbrudd der informasjon er slettet eller endret.*
- Gode retningslinjer for avhending av data:
  - Hvordan kvitte seg med fysiske enheter som inneholder data, uten å potensielt lekke data?

Planlegg for katastrofe…

Raskest mulig back in business:

- Ha sikkerhetskopier
- Og kanskje *redundante* systemer



Angrepsvektor: Sårbare systemer eller applikasjoner

Applikasjonsprogramvare:



Applikasjonssikkerhet

Systemprogramvare:



Systemsikkerhet

Kjennetegn ved applikasjoner

Svært ofte:

- Dialog med bruker(e)
- Behandler input fra bruker(e)
- I bakkant av applikasjonen benyttes en *database* for lagring av informasjon.

- Egenskapene utnyttes av hackere.

Eksempel: SQL injisering

Eksempel: Tabellen «Bruker»:

BrukerId	Brukernavn	Passord	Fornavn	Etternavn	Kredittkort #
1001	anneh	ewtgfst45yh	Anne	Hansen	1609983275417533
1002	pederaa	67efg3ndfa	Peder	Aas	4586890148239766

Eksempel på brukerdialog:

Oppgi brukernavn: anneh Oppgi passord: xyxyxy OR 1=1

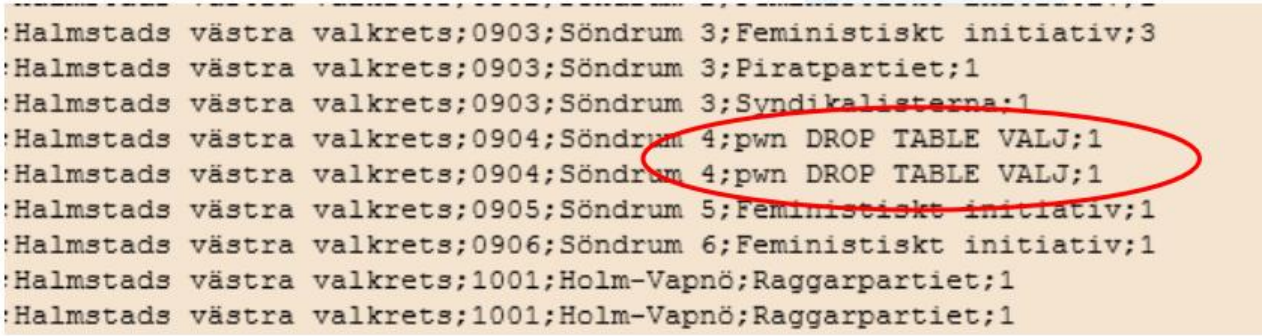
Dette kan resultere i følgende gyldige SQL-setning:

```
SELECT * FROM Bruker
WHERE Brukernavn = anneh and Passord = xyxyxy  OR 1=1;
```

- For den interesserte (Computerphile): https://www.youtube.com/watch?v=ciNHn38EyRc

Svensk valgsabotasje ☺

«Hacking swedish election with pen and paper»:



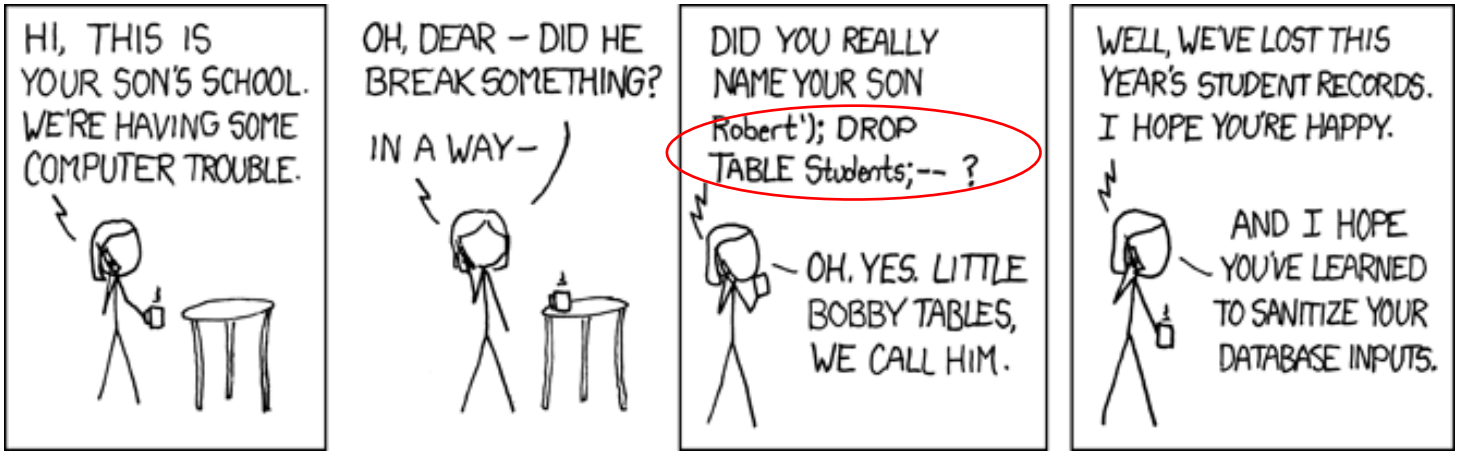
```
:Halmstads västra valkrets;0903;Söndrum 3;Feministiskt initiativ;3
:Halmstads västra valkrets;0903;Söndrum 3;Piratpartiet;1
:Halmstads västra valkrets;0903;Söndrum 3;Syndikalisterna;1
:Halmstads västra valkrets;0904;Söndrum 4;pwn DROP TABLE VALJ;1
:Halmstads västra valkrets;0904;Söndrum 4;pwn DROP TABLE VALJ;1
:Halmstads västra valkrets;0905;Söndrum 5;Feministiskt initiativ;1
:Halmstads västra valkrets;0906;Söndrum 6;Feministiskt initiativ;1
:Halmstads västra valkrets;1001;Holm-Vapnö;Raggarpartiet;1
:Halmstads västra valkrets;1001;Holm-Vapnö;Raggarpartiet;1
```

Forsøk på sabotasje ved å slette data/tabeller:

SELECT * FROM Brukere WHERE Brukernavn = anneh; DROP TABLE Valg;

- Mer info: https://www.wired.co.uk/article/sweden-election-hack

Nerde-humor: «Exploits of a Mom»



Kilde: https://xkcd.com/327/

Eksempel: Cross Site Scripting (XSS)



1. Angriper plasserer ondsinnede kode på en webside, kamuflert som innhold fra en bruker. Lagres på web-tjeneren.



2. Intetanende bruker besøker websiden, og ondsinnet kode sendes tilbake til brukeren med innholdet.



3. Angriperen tar kontroll over brukerens maskin og/eller data via den injiserte koden.

- For den interesserte (Computerphile): https://www.youtube.com/watch?v=T1QEs3mdJoc

Sikre applikasjoner

Design og utvikling med tanke på trygg bruk:

- I designfasen:
  - ✓ Kartlegge potensielle trusler.
  - ✓ Identifisere tiltak som kan iverksettes for å motvirke truslene.
- I programmeringsfasen:
  - ✓ Unngå å skape eller tilrettelegge for sårbarheter.
- I produksjonsfasen:
  - ✓ Holde all *programvare* oppdatert.

Oppgave 2

Konfidensialitet

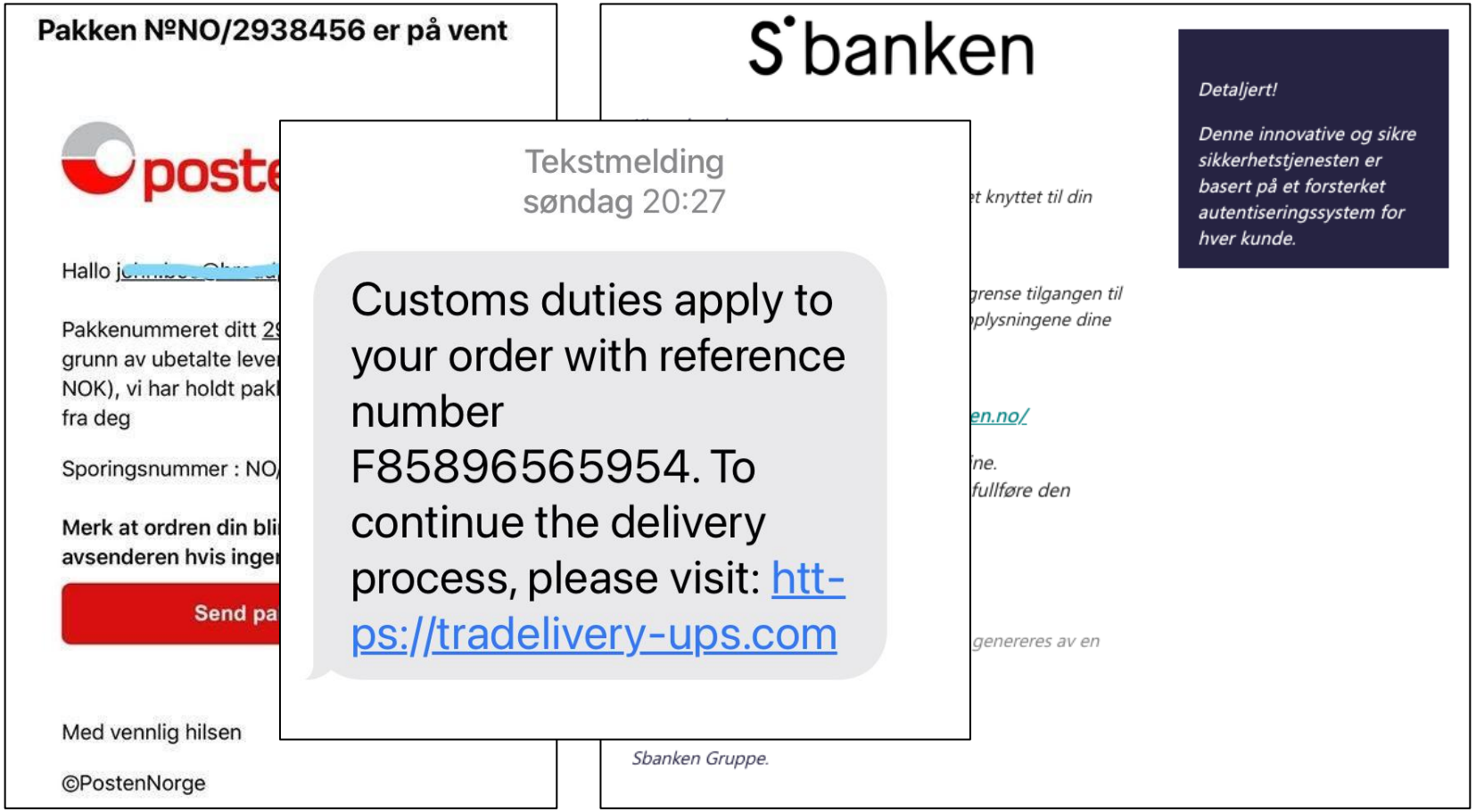
Konfidensialitet for persondata er et sentralt krav i norsk personvernlovgivning. Hvilke av følgende sikkerhetstiltak kan bidra til konfidensialitet for persondata i et IT-system:

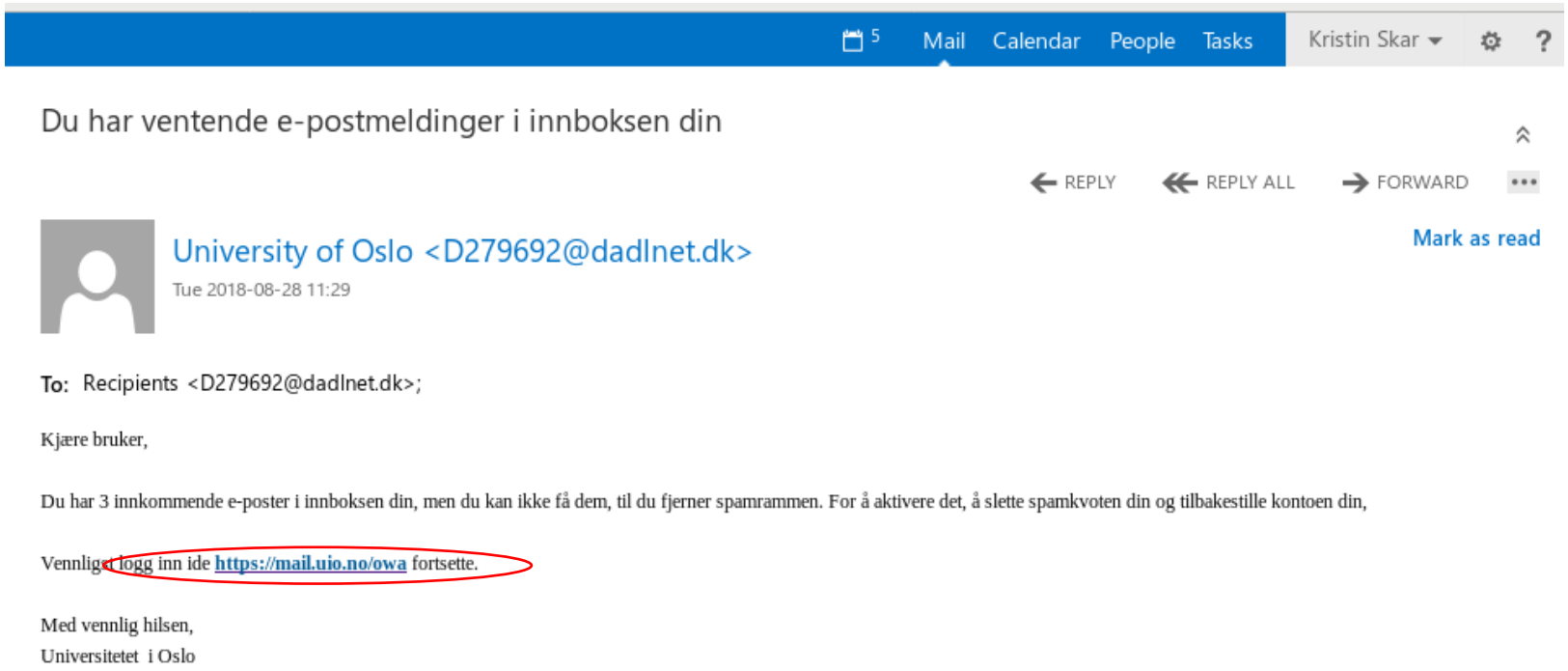
Velg ett eller flere alternativer

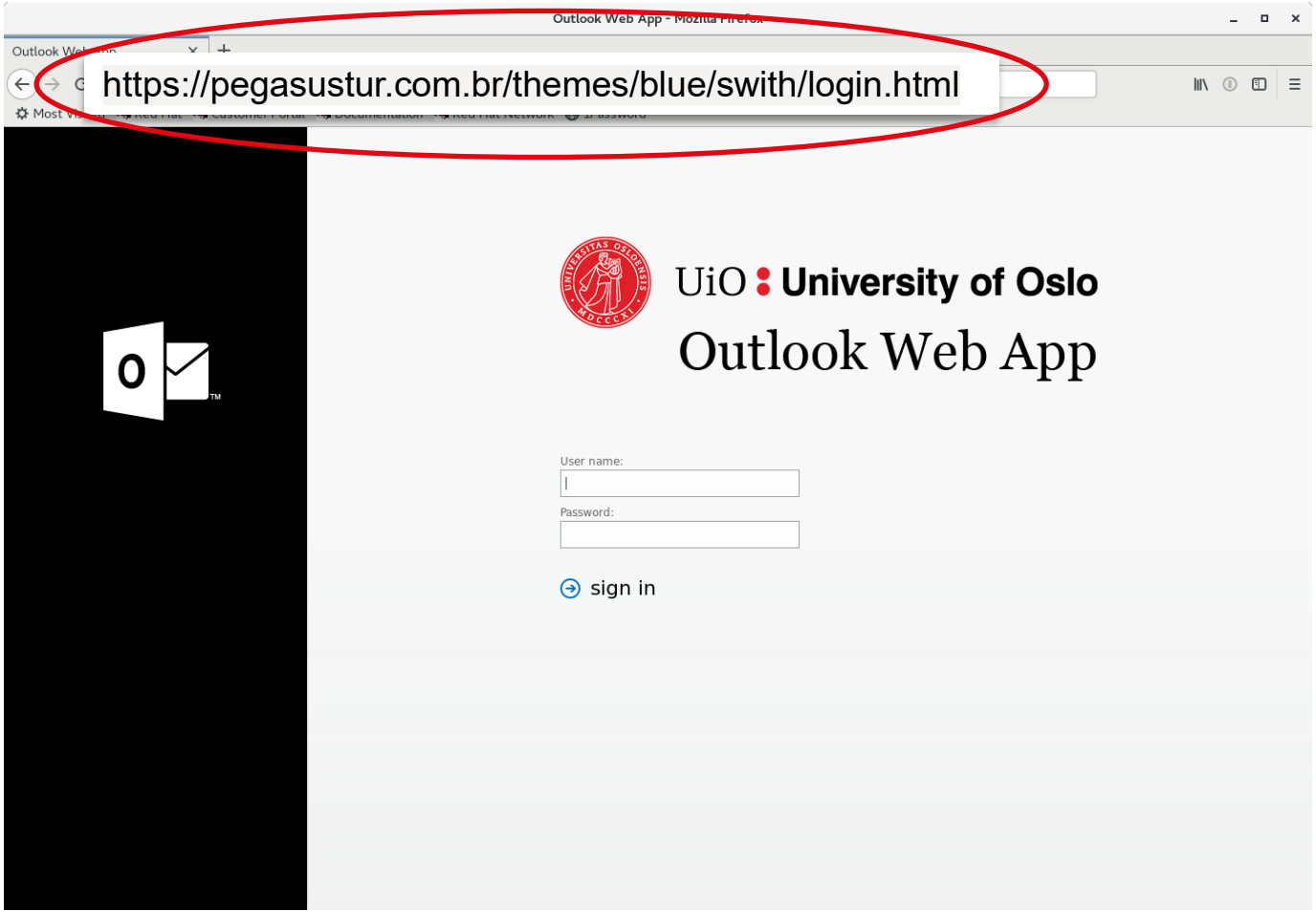
- ❑ Kryptere alle data som lagres
- ❑ Autentisere alle brukere av IT-systemet
- ❑ Sikkerhetskopiere alle data
- ❑ Innføre tilgangskontroll til IT-systemet
- ❑ Ha gode rutiner for gjenoppretting av data



Utgjør du og jeg en trussel?


Pakken NºNO/2938456 er på vent
Hallo j
Pakkenummeret ditt 2
grunn av ubetalte leve
NOK), vi har holdt pak
fra deg
Sporingsnummer : NO
Merk at ordren din bli
avsenderen hvis inge
Send pa
Med vennlig hilsen
©PostenNorge
Tekstmelding
søndag 20:27
Customs duties apply to your order with reference number F85896565954. To continue the delivery process, please visit: htt-ps://tradelivery-ups.com
S banken
Detaljert!
Denne innovative og sikre sikkerhetstjenesten er basert på et forsterket autentiseringssystem for hver kunde.
et knyttet til din
grense tilgangen til
plysningene dine
en.no/
ine.
fullføre den
genereres av en
Sbanken Gruppe.


5 Mail Calendar People Tasks Kristin Skar
Du har ventende e-postmeldinger i innboksen din
REPLY REPLY ALL FORWARD
University of Oslo <D279692@dadlnet.dk>
Tue 2018-08-28 11:29
Mark as read
To: Recipients <D279692@dadlnet.dk>;
Kjære bruker,
Du har 3 innkommende e-poster i innboksen din, men du kan ikke få dem, til du fjerner spamrammen. For å aktivere det, å slette spamkvoten din og tilbakestille kontoen din,
Vennligst logg inn ide https://mail.uio.no/owa fortsette.
Med vennlig hilsen,
Universitetet i Oslo


Outlook Web App - Mozilla Firefox
https://pegasustur.com.br/themes/blue/swith/login.html
UiO : University of Oslo
Outlook Web App
User name:
Password:
sign in

Bedragere lurte ansatt til å utbetale en halv milliard kroner

- Oslo-politiet har samarbeidet med FBI
- Ingen pågrepet så langt

Politiet på bar bakke i Norfund-saken: 100 millioner borte etter digitalt angrep

Norfund bekrefter å ha tapt store summer i en avansert, digital svindel. Politiet har etterforsket saken i det skjulte.

UiT svindlet for 12 millioner

UiT betalte ut 12 millioner kroner til det som viste seg å være svindel. Pengene gikk til det som så ut som en faktura for en røntgenmaskin.

Etterbørs Musikk

Utenlandske «direktørsvindlere» stjal 770.000 kroner fra festspillene i Nord-Norge

Med falske epostadresser og god norsk klarte svindlere å få festspillene i Nord-Norge til å overføre store summer til kontoer i England og Tyrkia.

NTB
Publisert: 20.09.2017 – 06:38 Oppdatert: 20.09.2017 – 07:33

Vanskeligere og vanskeligere å ikke la seg lure.

Deepfakes utnytter kunstig intelligens for å lage videoer og lydinnhold det er svært vanskelig å avsløre som falskt.





Men; Du er også en viktig forsvarsmekanisme.

Mennesker utnyttes (også digitalt):

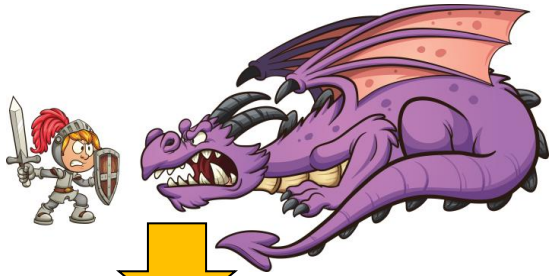
- Offer for svindelangrep
- Utpressing/overtalelser



«Sikkerhetskultur»

(God eller dårlig?)

Oppsummering: Helhet er nødvendig



Sikkerhet i applikasjonsprogramvare er ikke sikrere enn sikkerheten i datamaskinen den kjører på.

Sikkerhet i datamaskinen avhenger av sikkerhet i systemprogramvare, datamaskinens oppstartsprosess og maskinvare.



Læringsmål

- Kjenne til de viktigste typene *trusselaktører,* og hva de potensielt er ute etter.
- Vite hva *angrepsvektor* er, og kjenne til de vanligste typene.
- Kjenne til et utvalg *skadevare* som er gjennomgått i forelesning.
- Vite hva et *sikkerhetstiltak* er, hvordan de gjerne kategoriseres, og sammenhengen mellom sikkerhetsmål og sikkerhetstiltak.
- Kjenne begrepet *applikasjonssikkerhet*, og kjenne til angrepsvektorene SQL-injeksjon og XSS.
- Forstå *menneskelig faktor* som reell sårbarhet.
- Sikre datasystemer: Aldri sikrere enn det svakeste ledd.

Lenkesamling (ikke pensum)

- **Ressurser på nett:**
  - Nasjonal sikkerhetsmyndighet (NSM): https://nsm.no
  - NorSIS (Norsk senter for informasjonssikring): https://norsis.no
  - Datattilsynet: https://datatilsynet.no
  - NSR (Nærlingslivets sikkerhetsråd): https://www.nsr-org.no/
- **Lesestoff**
  - Nordmenn og digital sikkerhetskultur: https://norsis.no/publikasjoner/
  - PSTs nasjonale trusselvurdering: https://www.pst.no/trusselbilde/norsk-trusselvurdering/nasjonal-trusselvurdering-2026/
  - NSMs digitale risikobilde: https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2026
  - Mørketallsundersøkelsen: https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen

Takk for i dag!

mn.uio.no/ifi

