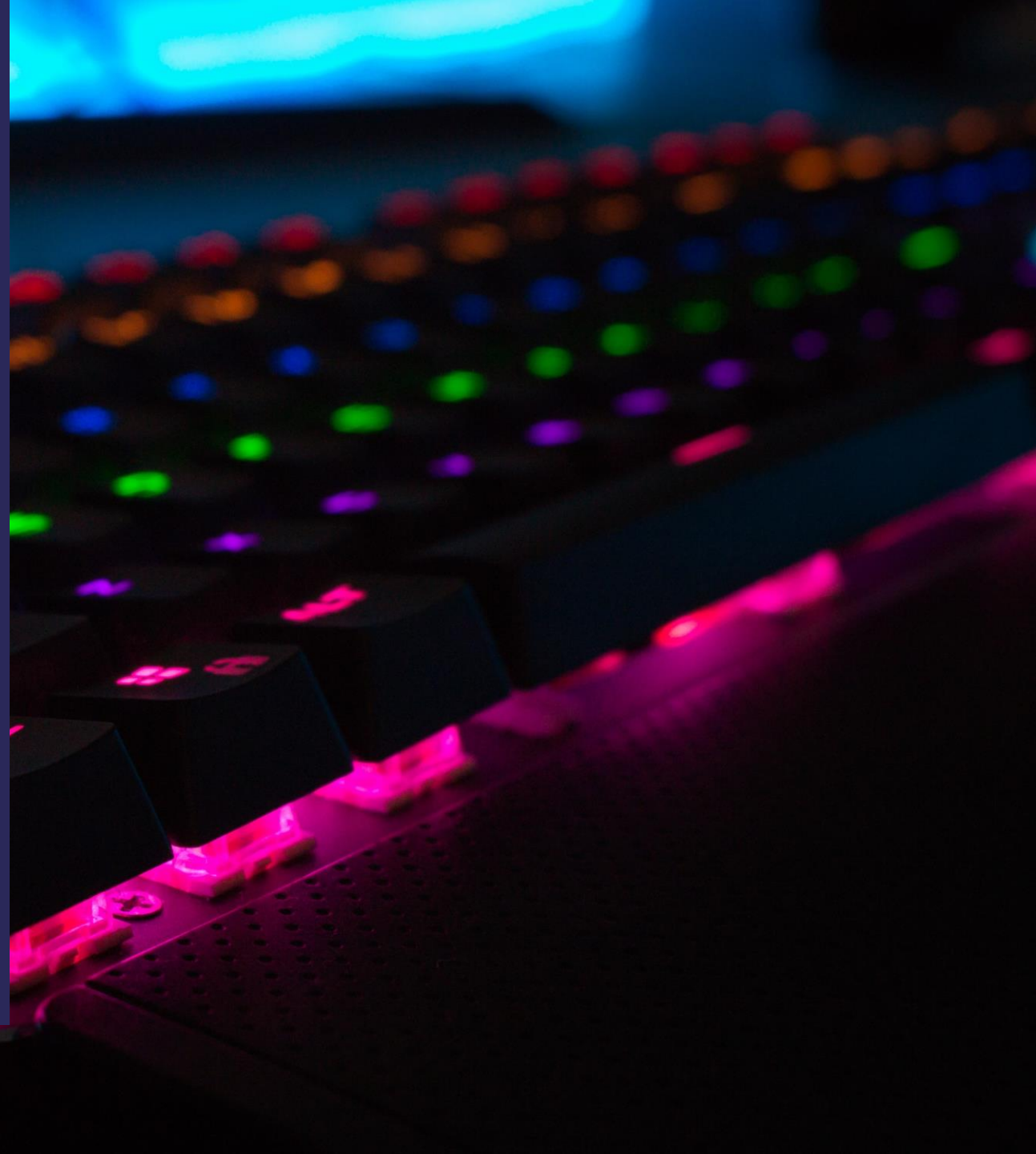
Oslo

Forum for informasjonssikkerhet og personvern

Onsdag 30. november

Sendingen starter 09:00



Program

09:00 - 09:05	**Velkommen og introduksjon til dagens program**
09:05 - 09:15	**Hva skjer på personvernområdet?** Maryke Silalahi Nuth
09:15 - 09:25	**Hva skjer på informasjonssikkerhetsområdet?** Åsmund Skomedal
09:25 - 09:40	**IDA – Tilgangsstyring** Camilla Ruud og Ida Marie Haukland fra UKE
09:40 - 09:50	**Pause til å fylle kaffekoppen**
09:50 - 10:30	**Personvernkommisjonens NOU** Haakon Hertzberg fra NAV og Personvernkommisjonen
10:30 - 10:50	**Sikkerhetsmåneden og Phishingøvelsen** Cecilie Bergh
10:50 - 11:00	**Avslutning**

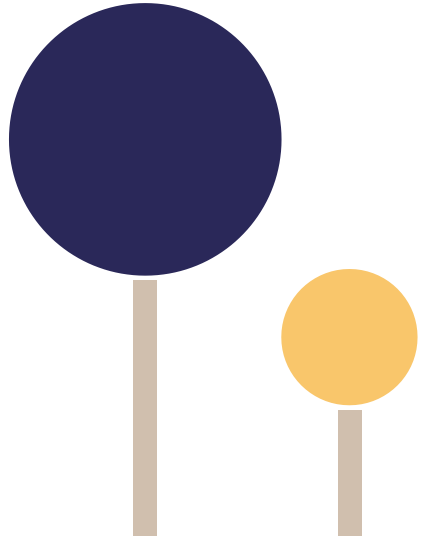
Hva skjer på personvernområdet?

Maryke S. Nuth
Fagsjef personvern
maryke.nuth@byr.oslo.kommune.no

Forum for informasjonssikkerhet og personvern
29. nov 2022

Status behandlingsoversikt

- Opplæring er godt i gang i november (avsluttes 30.11)
  - ekstra opplæring kommer
  - kun nøkkelpersoner (PKO, ISK, PISK eller IKT-hovedkontakt)
  - tilgangsstyring gjennom PRK
- Brev til alle virksomheter
  - Fra UKE datert 26. juni
  - Fra FIN/ISI datert 16. november
- Pågående arbeid med veileder for Behandlingsoversikten
- Oppdatering av intranett kommer!



Personvernverktøy lansert i 2022

Verktøy

Retningslinjer

- Kameraovervåking
- Apper
- Deling til forskningsformål
- Deling til statistikkformål
- Bruk av film og foto
- Sosiale medier
- Adressesperre (informasjon)

Andre verktøy

- Oppdaterte maler for personvernvurderinger
- Huskeliste for etablering av Facebook

Vurderinger

- Klassifisering av informasjon (som en del av OSIS)
- Behandling av personopplysninger ved sykdom hos ansatt (gjenbruk fra ISIs e-post til BRE)
- Personopplysninger om døde (grunnet forespørsel fra Gravferdsetaten)
- Overføring til tredjeland og Schrems II-dommen (gjenbruk fra brev til UKE 2021)
- Bruk av sosiale medier (et vedlegg til KS veileder for SoMe)

Dokumentene ligger på felles intranett for Oslo kommune om personvern

Fokusområder i 2023

Verktøy:

- Veileder
  - Retting og sletting
- Maler
  - Databehandleravtaler
  - Personvernerklæringer
- Huskeliste
  - Avvikshåndtering og avvikskultur

Temaer:

- Behandlingsansvar
- Den registrertes rettigheter
- Den registrertes friheter (frihetspakke)
- Personopplysninger til ansatte (arbeidslivpakke)

Planlagte kurs 2023

- Grunnleggende personvern
  - februar og september(på Teams)
- Databehandleravtaler
  - Q2
- Personvern i prosjekter
  - Q4

Bruk av maler for personvernvurderinger:

- Nybegynner
  - mars og september
- Viderekomne
  - mai og november

Sektorkontakt

	BLK	NOE	KIF	FIN	BYU	MOS	OVK	AIS	HEI	BYD
Sektorkontakt	Siri P. Johansen			Brit Røthe			Linda M. Knutsen	Siril Jonassen		Linda M. Knutsen

- Hovedtyngde i sektormøter har vært strategisk valgte fokusområder for 6-mnd av ganger f. eks. avvik

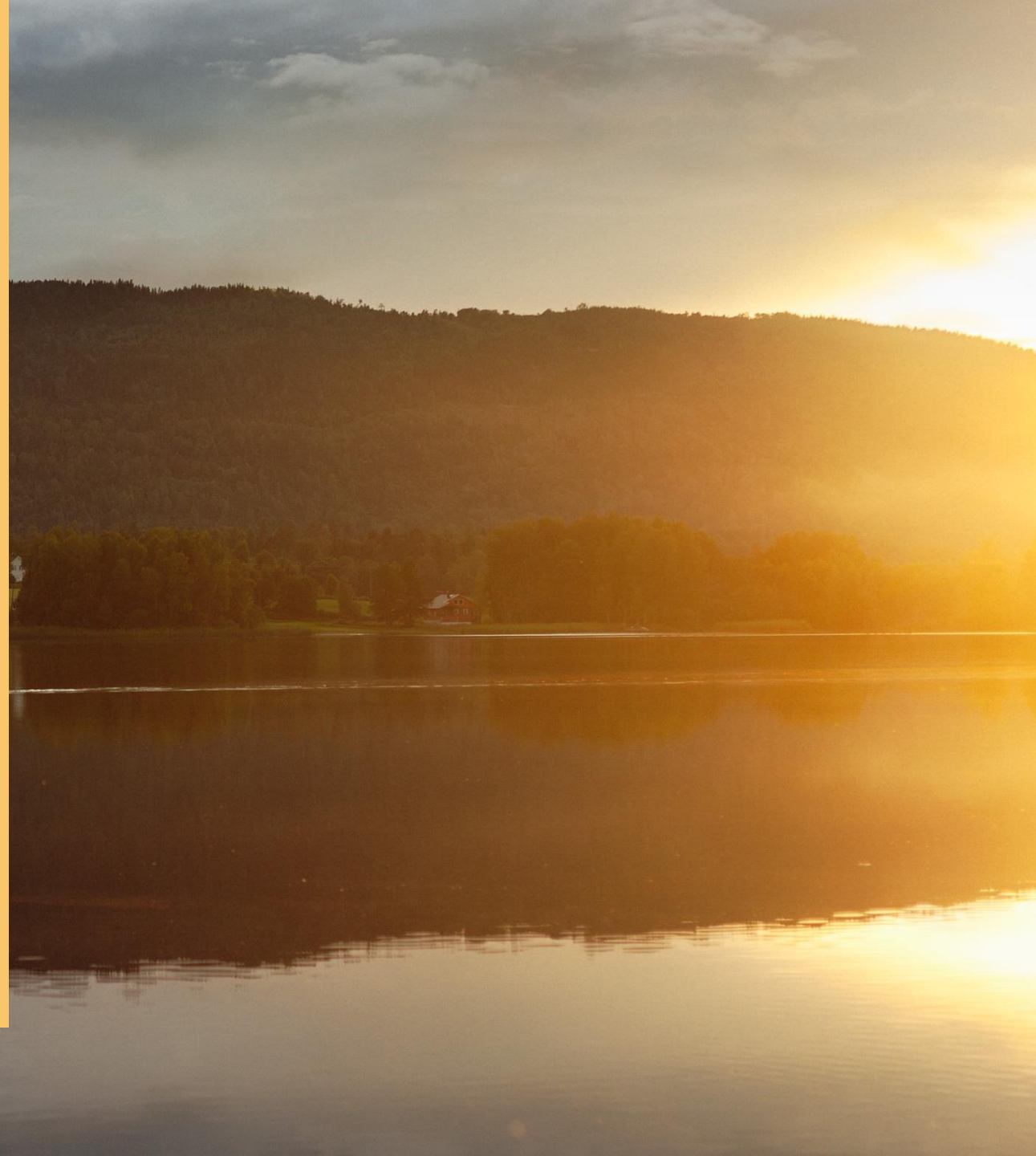
Oslo

Informasjonssikkerhet

Hva skjer innen området …

30. november 2022

Åsmund Skomedal
Informasjonssikkerhetssjef
asmund.skomedal@byr.oslo.kommune.no



Trusselbildet – Q4 2022

NSM – Nasjonalt Digitalt Risikobilde 2022 [oktober]

- særlig tre samfunnsområder har vært utsatt det siste året:
  - Teknologibedrifter - forskning og utvikling - offentlige forvaltningsorganer
- politisk motiverte tjenestenektangrep
  - En mye brukt angrepsmetode fra pro-russiske aktører mot en rekke NATO-land
  - NSM gikk i mai ut og ba virksomheter påse at de var i stand til å motstå denne typen cyberangrep
- Ingen endring i «Sikkerhetspulsen» = 2

ncsc.gov.uk - årlig trussel-rapport [september]

- peker på fire statlige aktører:
  - Russland; ønsker å ramme operasjonelle kapabiliteter i Ukraina, EU og NATO
  - Kina og Iran; ca som før
  - *Nord-Korea*; økonomisk motivert bruk av løsepengevirus og tyveri

Trusselbildet – Q4 2022 (ii)

EU - ENISA Threat Landscape 2022 [fra oktober]

- **Null-dags sårbarheter**
  er en viktig ressurs som trussel-aktørene benytter for å nå sine mål
- **En ny bølge av hacktivisme er observert** etter starten av krigen i Ukraina
- **DDoS angrep blir større og med komplekse; de beveger seg mot mobilnett og IoT for å benytte ressursene der til cyberkrigføring**
- **AI-støtte for desinformasjon og «deepfakes»**;
  større utbredelse av «bots» som opptrer som personer kan ødelegge varslings- og kommentarregler og samhandling i samfunnet ved å oversvømme offentlige etater med falskt innhold og kommentarer

Nyhetsbildet [24. nov. 2022]

Falske oppringinger fra banker: «Spoofing-as-a-Service»

- Oppringninger 10 mill. i 2022
- Potensielle offer 200.000
- Antatt fortjeneste 500 mill. [NOK]

The Guardian

100 people arrested in UK's biggest fraud investigation

Scotland Yard shuts down iSpoof website, which helped scammers steal using fake bank phone calls

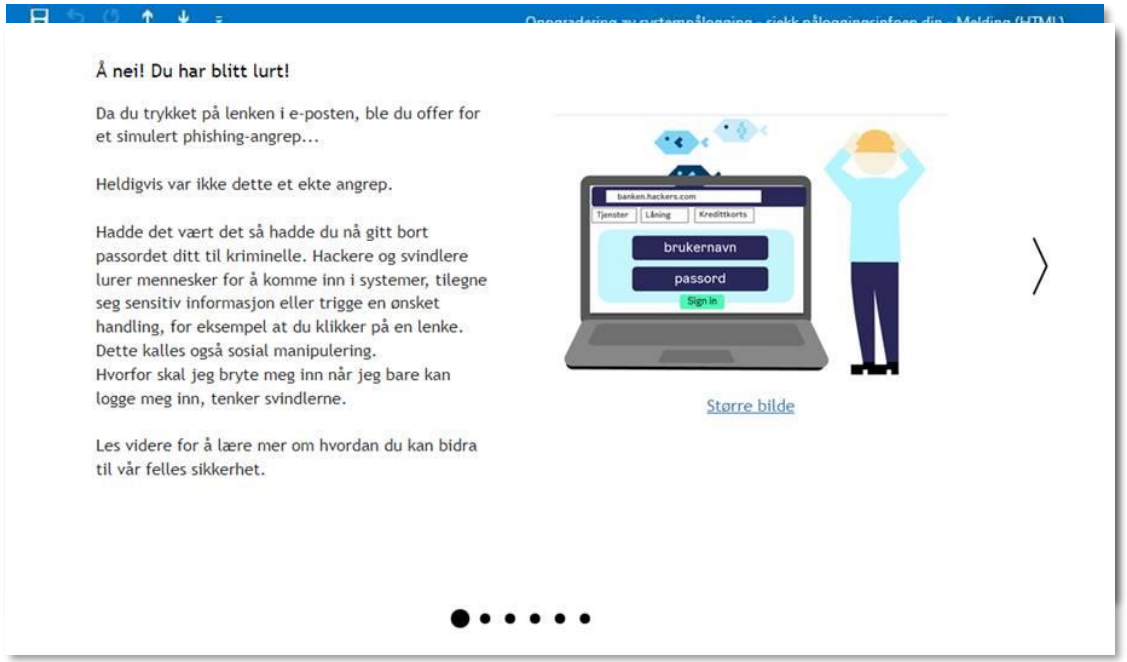
Scammers tricked victims into handing over money or giving them access to their bank accounts. Photograph: Dominic Lipinski/PA

More than 100 people have been arrested in the UK's biggest ever fraud operation, which brought down a website police describe as a "one-stop spoofing shop" used by scammers to steal tens of millions of pounds from Britons via fake bank phone calls.

It is estimated that more than 200,000 potential victims were targeted via the iSpoof fraud website, which was taken down this week by Scotland Yard's cybercrime unit with the help of the authorities in the US and Ukraine.

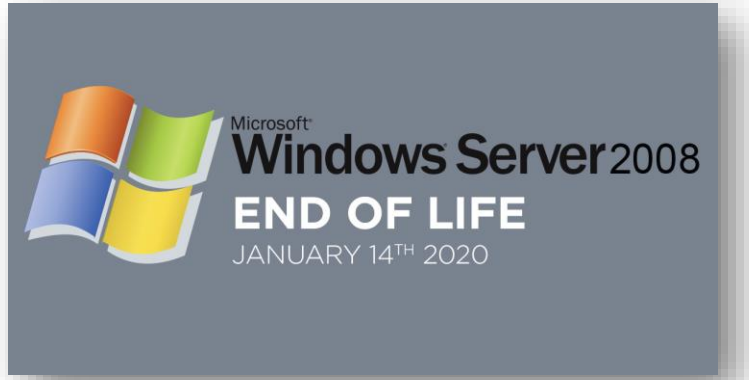
Felles IKT-plattform (i) - Hvor sårbare er vi ?

Phishingøvelse for alle på felles ikt-plattform



Test av passord

Utdaterte IT-systemer



Felles IKT-plattform (ii) - passord

- **Revisjon av passordreglene**
  - **Ikke** bytte hver tredje måned ☺
  - **Lenger** passord; min 14-16 karakterer
  - Ikke krav til tall eller spesialtegn
  - Rulles ut i Q1 2023
  - På sikt; åpne opp for (mer) to-faktor autentisering

- **Oppfølging av svake passord**
  - CSIRT gjør en skanning hver måned
  - Vurderer å dele statistikk fra hver sektor med egen byrådsavdelingen

Foto: irpp.org, Creativ

Oslo

Oslo kommunes nye verktøy for sikker tilgangsstyring heter IDA

Hvorfor trenger vi IDA?

Informasjonssikkerhetsforum, 30.11.22

Ida Marie Haukland og Camilla Ruud (UKE)

Oslo kommune får et nytt verktøy for sikker tilgangsstyring - IDA

- Dagens løsning for tilgangsstyring: Person- og ressurskatalogen (PRK)
- IDA vil på sikt erstatte dagens løsning for tilgangsstyring i PRK
- IDA = identitetsadministrasjon

- Sikker tilgangsstyring
= overholdelse av regelverk

Det er leders ansvar at ansatte har riktige tilganger

- Arbeidsoppgaver *kan* delegeres
- Ansvar kan *ikke* delegeres

Hva betyr sikker tilgangsstyring?

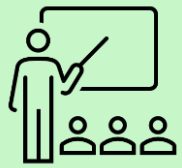
Riktig individ

Får tilgang til riktige ressurser/systemer

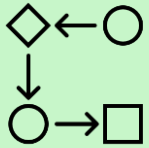
Til riktig tidspunkt

Av de rette årsaker

Behov for å forsterke...



Kunnskap om risiko og utfordringene knyttet til tilgangsstyring blant ledere



Skriftlige rutiner og prosedyrer

Holdninger og adferd (endringsledelse)

Forsterke fellesskapsfølelsen (én kommune)

Fordeler for deg, og for oss som kommune

Leder

Et verktøy for å ta og etterleve ansvaret

Ansatte

Enkel oversikt og intuitivt å søke om tilganger

Oslo kommune

Oslo

Enklere og mer effektiv tilgangsstyring, etterlevelse av lovverk

Oppdrag fra Byrådsavdeling for Finans

- Ivareta sikker tilgangsstyring i Oslo kommune i tråd med gjeldende lovverk og krav til informasjonssikkerhet.
- Sikre at alle virksomheter kan bruke den nye sentrale løsningen, inkludert virksomheter som driftes utenfor felles IKT plattform.
- Kommunens målbilde er ett felles verktøy, som brukes i alle kommunens virksomheter for brukeradministrasjon og tilgangsstyring på alle kommunens IKT-plattformer.

Hva går vi fra og til?

Fra

1. Svakheter i dagens løsning for tilgangsstyring, både på sikkerhet og brukervennlighet/funksjonalitet
2. Manglende felles, sentral prosess for tilgangsstyring
3. Lav bevissthet rundt tilgangskontroll (tilfeldige tilgang), kopiering av tilganger fra en «lik» person
4. Ingen automatisk sletting av brukere ved fratredelse

Til

1. Riktig person får riktig tilgang til systemer til riktig tidspunkt av de rette årsakene, også eksterne konsulenter
2. Selvbetjeningsportal for forespørsel/bestilling av IKT tilganger med innebygd godkjenningssløyfe via leder
3. Enkel og god oversikt over tilganger som søkes om og tilganger som gis
4. Automatisk deaktivering og sletting av en bruker ved fratredelse

Hva er gevinstene for virksomhetene?

- Ivaretar lover, regler og informasjonssikkerhet
- Bedre kontroll – compliance GDPR
- Enklere og mer effektiv tilgangsstyring
  - Automatisert stenging av tilganger når arbeidsforhold opphører
  - Mindre manuelt arbeid med å gi og avslutte tilganger
- HR-systemet er master for person- og organisasjonsdata (slipper å registrere nyansatt i PRK, registreres kun i HR-systemet)
- Oversikt over alle brukergrupper inkludert eksterne som ikke lønnes av Oslo kommune (gir bedre oversikt og mulighet for sluttdato)

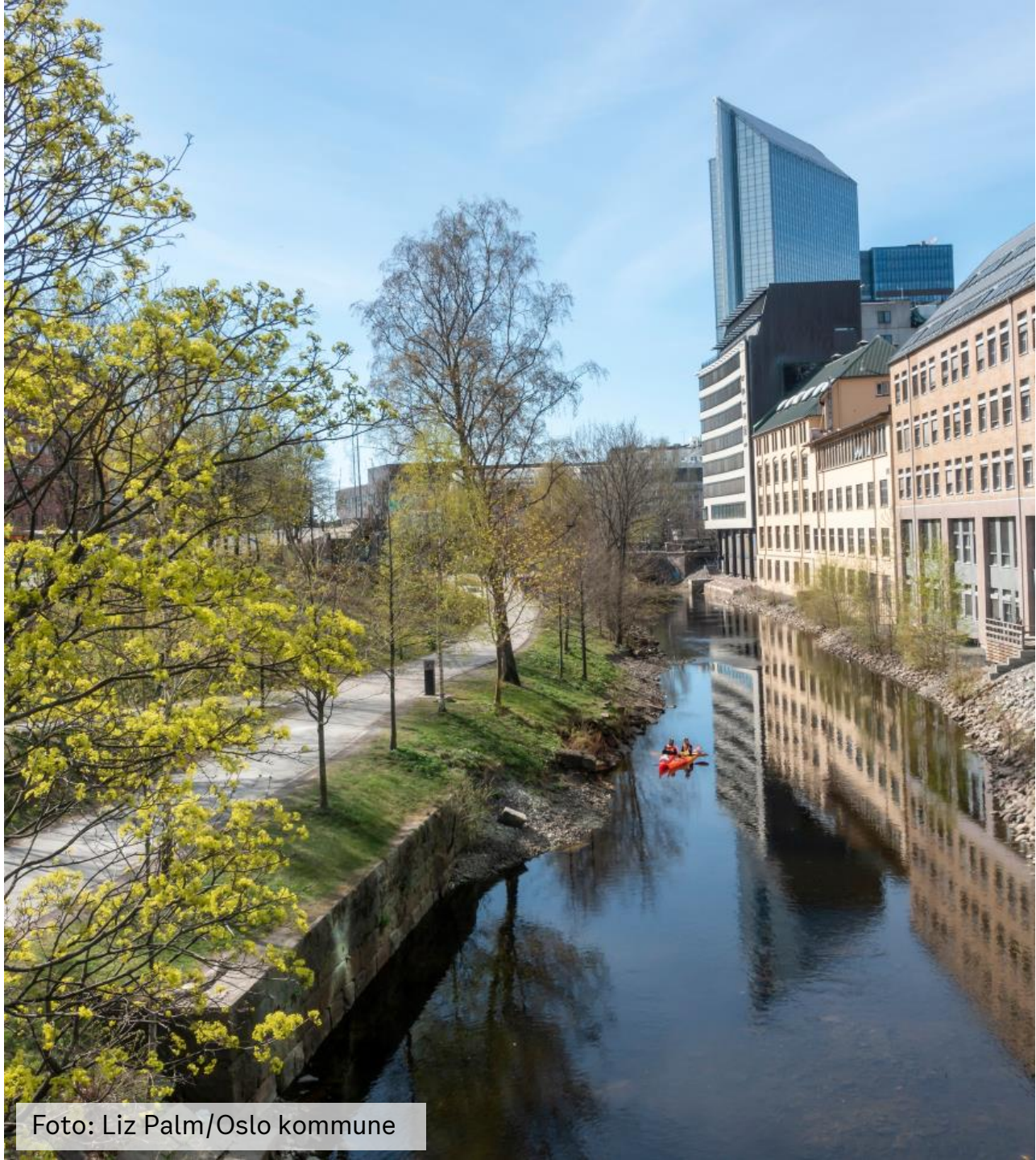


Foto: Liz Palm/Oslo kommune

Når får virksomhetene tilgang til IDA?

- Implementering starter høsten 2023
- Trinnvis innføring
- Plan i bevegelse

Ditt personvern
- vårt felles ansvar

Tid for en personvernpolitikk

30. november 2022

Haakon Hertzberg

Om rapporten

- 2 år.
- 242 sider.
- 140 anbefalinger og tiltak.
- Kommisjonen står samlet bak anbefalingene, med unntak av én dissens.

Mandatet

- Offentlig forvaltning
- Justis
- Skole- og barnehagesektoren
- Forbruker

Medlemmene

- John Arne Moen (leder)
- Ingvild Næss (nestleder)
- Haakon Hertzberg
- Jill Walker Rettberg (frem til mars 2021)
- Tor-Aksel Busch
- Marianne Høyer
- Dag Wiese Schartum
- Trine Skei Grande
- Finn Lützow-Holm Myrstad
- Helge Veum
- Toril Nag
- Trude Haugli
- Brita Ytre-Arne (fra juni 2021)
- Oddhild Aasberg
- Catharina Nes (sekretariatsleder)
- Janne Kummeneje Loen
- Ailo Ravn Krogh

Om arbeidet

- 18 plenumsmøter, de fleste digitale.
- Tre innspillsseminarer om sentrale tema.
- Seks eksterne utredninger.
- Fått innspill fra barn og unge.
- Løpende kontakt med andre utvalg og ekspertgrupper.

Hovedtemaene

Del 1: Hva er personvern, rettslig rammeverk og teknologiske drivkrefter

Del 2: Personvernets situasjon og utfordringer innen utvalgte sektorer

- Personvern i den digitale forvaltningen
- Personvern i justissektoren
- Personvern i skolen og barnehagen
- Forbrukernes personvern

Del 3: Andre områder kommisjonen har arbeidet med

- Regelkompleksitet og nasjonalt handlingsrom
- Teknologi i personvernets tjeneste
- Åpenhet
- Veiledning, tilsyn og klage

Hovedkonklusjoner – personvern på dagsorden

- Samfunnsgevinstene av digitaliseringen er store.
- Digitaliseringen skjer på bekostning av personvernet.
- Personvern ikke bare et individuelt anliggende – en kollektiv og solidarisk verdi.
- Teknologi avgjørende for å oppnå et bedre personvern.

Hovedkonklusjon: Tid for nasjonal personvernpolitikk

- Føringer for digitaliseringen av samfunnet.
- En nasjonal personvernpolitikk må:
  - ha som overordnet mål å sørge for reell ivaretakelse av personvernet.
  - se personvernet i et helhetlig perspektiv.
  - innebære grundige risikovurderinger.
  - ha særlig oppmerksomhet på sårbare grupper, herunder barn og unge.
  - inkludere en tydelig utenrikspolitisk rolle.
  - utnytte det nasjonale handlingsrommet for regulering.
  - fremme personvernvennlig innovasjon.
  - innebære at offentlig sektor går foran.
  - forutsette et solid kunnskaps- og kompetansegrunnlag.
  - forutsette åpenhet rundt behandling av personopplysninger.
  - forutsette effektiv håndheving.
- Regjeringen bør legge frem en personvernpolitisk redegjørelse for Stortinget årlig, forankret i gjeldende personvernpolitikk.

Personvern i den digitale forvaltningen

- Fragmentert tilnærming til personvern.
- Utilstrekkelig kompetanse og ressurser.
- Manglende vurdering av personvernkonsekvenser.
- Uklare roller og ansvar, spesielt knyttet til deling av personopplysninger.

Personvern i den digitale forvaltningen – anbefalinger

- Tiltak med stor innvirkning på innbyggernes personvern bør hjemles i lov, i stedet for å forskriftsfestes.
- Nødvendig å få på plass en forståelig og anvendelig veileder for vurdering av personvernkonsekvenser i lov- og forskriftsarbeid.
- Veilederen om lovteknikk- og lovforberedelse («lovteknikkheftet») bør oppdateres.
- Vurderinger av viderebruk bør være grundige og offentlig tilgjengelige.
- Nødvendig å utvikle standarder for deling av personopplysninger.
- Profilering for å avdekke ulovligheter alltid bør sees som en inngripende behandling som krever solid hjemmel i lov.

Personvern i den digitale forvaltningen – anbefalinger

Offentlige aktører og store teknologiselskaper

- Sosiale medier bør ikke brukes i konkret enkeltsaksbehandling.
- Viktig at det gjøres både personvern- og datastrategiske vurderinger når det offentlige benytter tjenester fra store teknologiselskaper.
- Offentlig forvaltning må tilgjengeliggjøre informasjon til innbyggerne i digitale løsninger uten at personopplysninger samles inn og brukes av kommersielle aktører til kommersielle formål, som for eksempel til å bygge og berike profiler eller deles med tredjeparter.

Personvern i justissektoren

- Alvorlige personvernkrenkelser = kriminalitetsbekjempelse må vike.
- Mangler ved vurderinger av personvernkonsekvenser i lov- og forskriftsarbeider.
- Behov for vurdering av personvernkonsekvenser av politiets metoder.
- Behov for styrking av personvernkompetanse i sektoren.

Personvern i justissektoren

- Utvalg for å utrede metodebruken i justissektoren.
- Vurdere behov for å utvide dagens domstolskontroll av politiets tiltak.
- Tillegg i straffeprosessloven § 170a for å sikre vurdering av at den samlede bruken av ulike etterforskningsmetoder ikke blir et uforholdsmessig inngrep.
- Generelt forbud mot bruk av ansiktsgjenkjenning og annen biometrisk fjernidentifikasjon i offentlige rom.
- Norske myndigheter bør innhente erfaringer fra andre land om ordninger for å filtrere bort overskuddsinformasjon ved beslag av digitale lagringsenheter og vurdere å etablere en lignende ordning.
- Ved masseinnsamling av personopplysninger for nærmere angitte formål, er det viktig at metoder for dataseparasjon følges for å sikre at data kun benyttes til formål lovgiver har vurdert det nødvendig for.

Personvern i skole og barnehage

- Mangel på personvernressurser og kompetanse.

Personvern i skole og barnehage – anbefalinger

- Sentral testing og veiledning.
- Forhandlingsstøtte og -ledelse.
- Behov for en nasjonal tjenestekatalog er stort.
- Statlige myndigheter må ta initiativ til å utarbeide en personvernnorm.
- Bruke offentlig innkjøp aktivt og ved behov investere i nye løsninger.

Veiledning, tilsyn og klage

- Stort behov for veiledning.
- Ofte uklarhet.

Veiledning, tilsyn og klage – anbefalinger

- Opprette tilsynsmyndigheter på europeisk nivå med myndighet og ansvar for å sørge for effektiv håndhevelse av personvernregelverket overfor de globale plattformaktørene, tilsvarende bestemmelsene som er inntatt i Digital Markets Act.
- Styrke Datatilsynet.
- Andre tilsynsmyndigheter med ansvarsområder som har stor og direkte betydning for ivaretakelse av personvern bør veilede.
- Systematisk arbeid for å styrke sektortilsynenes arbeid med personvernregelverket, og for å klargjøre hjemlene for utøvelse av myndighet.
- Tydelige rammer for henholdsvis veiledning og tilsyn i Datatilsynet.

Neste skritt: Høring

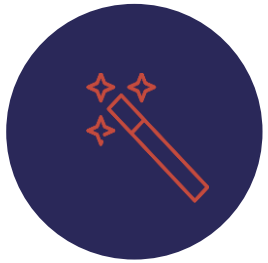
Oslo

Oppsummering og tilbakemeldinger

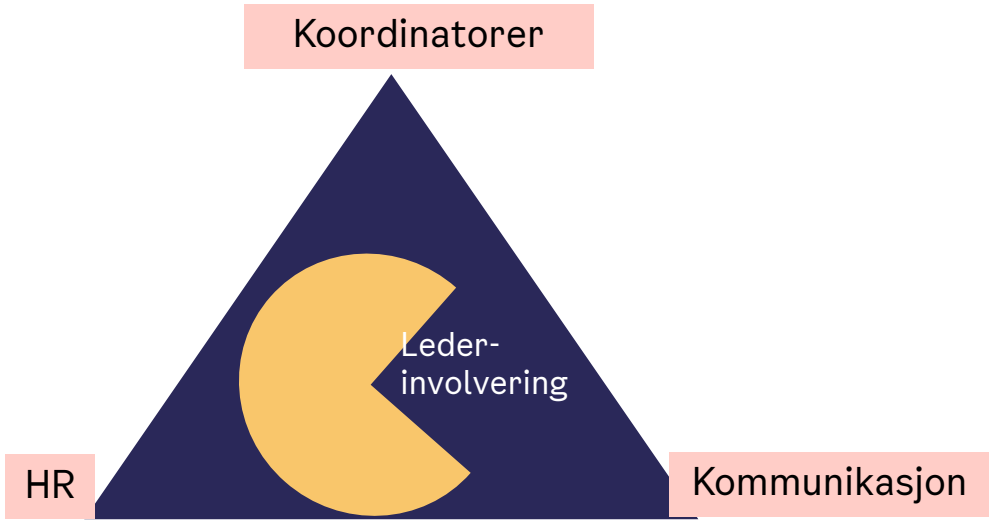
Sikkerhetsmåneden 2022
Phishingøvelsen

Sikkerhetsmåneden 2022 - løfte involvering og engasjement i virksomhetene – **klarte vi det?**

- Mål
  - Flere aktiviteter i virksomhetene
  - Flere gjennomfører e-læringene



- Grep
  - Involvere og jobbe med koordinatorene i virksomhetene over tid
  - Flere perspektiver på budskapene og til ulike målgrupper
  - Laget verktøy til bruk i virksomhetene
  - Jobbet med UKE om å ta i bruk Kompetansemodulen



- Samarbeid mellom faggrupper i virksomheten
  - Lederinvolvering!

Uketemaer

Uke 40

Tilgang og verdier

«Jeg likte særlig presiseringen og fokuset på at kommunens data har en verdi»

«Hvis jeg må trekke noe frem er det dette med hvilke verdier vi ønsker å beskytte.»

Uke 41

Trusselbildet og kontinuitet i tjenestene våre

«Det har vært veldig mange bra foredrag med veldig aktuelle temaer. Jeg har lært enda mer om hva jeg gjør for å sjekke e-poster mot eventuell phishing og hvordan jeg skal rapportere videre.»

Uke 42

Demokrati – personvern og sikkerhet

«veldig bra at det settes av tid til presentasjon av dette temaet.»

Uke 43

#sikkerhetheleåret!

Alle temaer er viktige, men kunne tenkt meg å høre mer om sikkerhetskultur.

Som ISK var jeg på workshop om beredskap, sånne praktiske øvelser føler jeg gir veldig mye utbytte på kort tid, samtidig som det hjelper å snakke på tvers av bydeler/etater om slikt for å se problemstillinger som man ofte ikke tenker på i eget hus. Gjerne noe tilsvarende, men med invitasjon til ledere i tillegg.

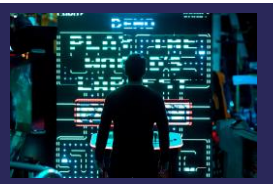
Oslo

Temaer og virkemidler

Uke 40

Tilgang og verdier

Uke 41



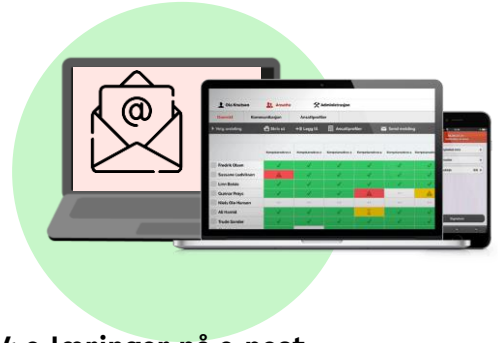
Trusselbildet og kontinuitet i tjenestene våre

Uke 42

Demokrati – personvern og sikkerhet

Uke 43

#sikkerhetheleåret!



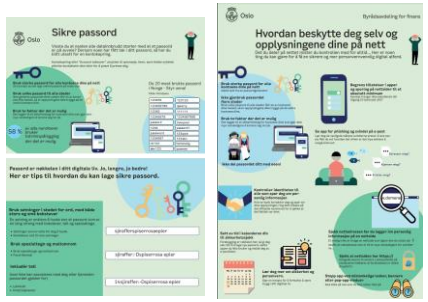
4 e-læringer på e-post

2 kompetanseplaner i Kompetansemodulen

- *Sikkerhetsmåneden 2022*
- *Sikkerhetsmåneden 2022 for ledere.*

Samtalekort med veiledning og dilemmaer til bruk i grupper

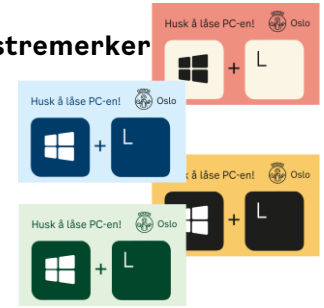
- Om å låse PC
- Om å ikke dele tilganger
- Om digital svindel
- Om behandling av personopplysninger
- Om avvikskultur



One-pager/flyer

- Sikker pålogging
- Sikrere på nett

Klistremerker

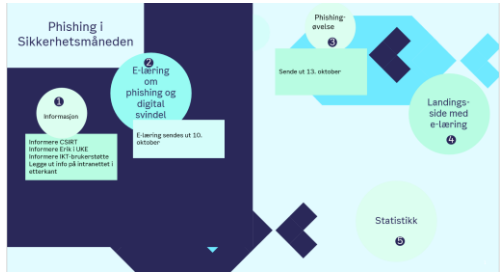


Sjokolade

Låseskjerm

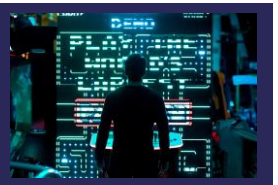
- Uke 40: Takk for at du låser PC'en din
- Uke 41:
- Uke 42:Takk for at du melder i fra
- Uke 43: Takk for at du lager sterke passord

Phishingøvelse



Opptak fra seminar/foredrag

Uke 41



Trusselbildet og kontinuitet i tjenestene våre

185 unike i sendingen

645 unike seere

Tirsdag 11. oktober
Foredrag: 60 min
På Workplace

Tim Talk med Origo: Martin Albert-Hoff

Sårbarhet i verdikjeden: Bakdøren du ikke visste at du har laget i ditt produkt

IKT-ansatte
Arkitekter
Utviklere
Sikkerhetsfolk

75 i Rådhuset
162 digitale

Onsdag 12. oktober
Seminar, heldags
Hybrid

Under angrep! Alle systemer er nede!
Eksterne foredragsholdere

Koordinatorer
Ledere
Fagfolk/faglig interesserte

305 deltakere

Torsdag 13. oktober
Foredrag: 60 min
På Teams

Trusselbildet og beredskap på 1-2-3: CSIRT i UKE

Alle

Vurderinger

	Tirsdag 11. oktober	Onsdag 12. oktober	Torsdag 13. oktober
Seminaret som helhet:		4.58	4.06
Faglig nivå i seminaret i forhold til forventningene i forkant:		4.62	4.08

Kommentarer og tilbakemeldinger

«Det var også et spennende foredrag om sikkerhet i regi av en etat i kommunen - som blant annet omhandlet spionasje mellom USA og Russland - med en foredragsholder som hadde forsvarsbakgrunn. Spennende, annerledes og lærerikt.»

«Dette er det beste seminaret jeg har deltatt på noensinne i Oslo kommune. Det var veldig gøy å få følge med på hvordan et hackerangrep ser ut og fungerer. Det faglige innholdet var bra og høyt, men allikevel lettforståelig for en som ikke er veldig teknisk»

«(...) et slikt informasjonsmøte om sikkerhet er viktig og bør gjennomføres oftere og mer regelmessig i Oslo kommune»

Uke 42

Demokrati – personvern og sikkerhet

225 unike i sendingen

756 unike seere

Tirsdag 19. oktober
Foredrag: 60 min
På Workplace

Tim Talk med Origo: Hjelp – jeg har klikka!

Alle

301 påmeldte:
- 34 koordinatorer
- 32 ledere
- 225 annen rolle

Onsdag 20. oktober
Seminar, 120 min
På Teams

240 deltakere

Er dine personopplysninger til salgs?
Intern og ekstern foredragsholdere

Koordinatorer

Ledere

Fagfolk/faglig interesserte

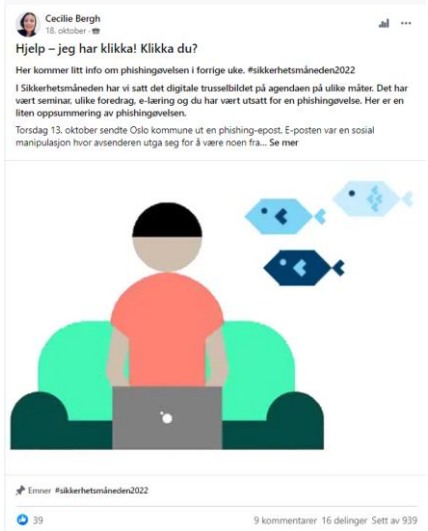
Torsdag 21. oktober
Foredrag: 60 min
På Teams

252 deltakere

Personvern og kommunikasjon via sosiale medier
Intern og ekstern foredragsholdere

Kommunika-sjonsfolk

Vurderinger



Seminaret som helhet:	**4.15**
Faglig nivå i seminaret i forhold til forventningene i forkant:	**4.20**

Seminaret som helhet:	**3.23**
Faglig nivå i seminaret i forhold til forventningene i forkant:	**3.42**

Kommentarer og tilbakemeldinger

«Denne Tim talken anbefaler jeg 👆Trodde jeg kunne mye om dette feltet, men lært noe nytt også i dag. En ting er sikkert, ting endrer seg veldig raskt også på dette området.»

«Nysgjerrig på oppfølgingen av det som nevnes om Oslo kommune og personvernutfordringer. Kommer det ut info om tiltak noe sted? ...»

«Her var det veldig vanskelig å få tak på regelverk og hva vi som kommune må gjøre når vi bruker sosiale medier. ... Savnet konkrete råd og regler.»

Uke 43

#sikkerhetheleåret

Vurderinger

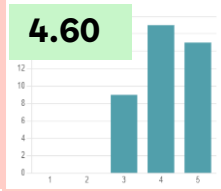
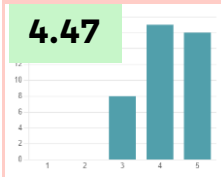
Kommentarer og tilbakemeldinger

Onsdag 26. oktober
Workshop: Øvelse, 4 t
I Rådhuset

#sikkerhetheleåret

35 deltakere

Koordinatorer

Seminaret som helhet:	**4.60** 
Faglig nivå i seminaret i forhold til forventningene i forkant:	**4.47** 

Gruppearbeidene fungerte bra - vi fikk til en god erfarings- og informasjonsutveksling. Opplevde seminaret som veldig nyttig - og midt i blinken for meg som holder på å oppdatere etatens beredskapsplaner

Torsdag 27. oktober
Foredrag: 30 min
På Gardermoen

Byrådets ledersamling
Økt cyber-risiko?
Og hva så...

130 deltakere

Toppledere

E-læringer – sendt på e-post og/eller tildelt i Kompetansemodulen

14 %

Uke 40:
Verdifull informasjon

13 %

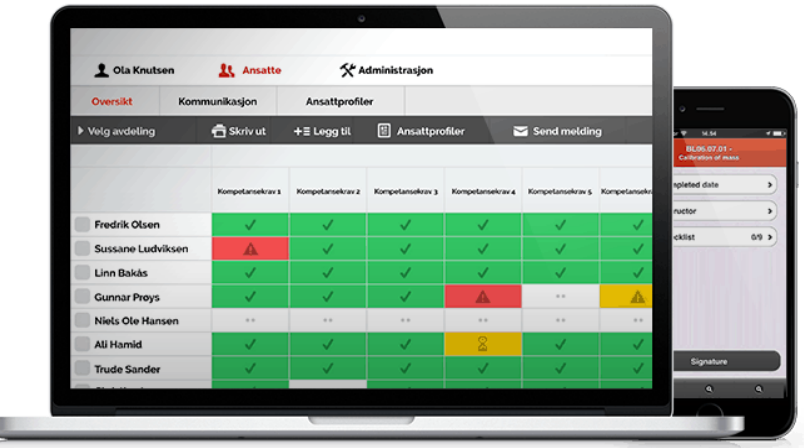
Uke 41:
Svindel på nett

12 %

Uke 42:
Mitt personvern

12 %

Uke 43:
Klarer du å slå hackeren?



- En virksomhet valgte kun Kompetansemodulen - PBE

	A	B	C
	Plan	**Antall tildelte**	**Antall fullført**
	Sikkerhetsmåneden 2022	1245	55,66%
	Sikkerhetsmåneden 2022 for ledere	205	44,29%

E-læringer: var det flere som gjennomførte enn året før?

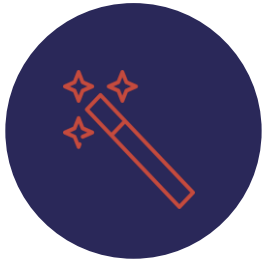
Gjennomføring av e-læring i Sikkerhetsmåneden 2021

	Oslo kommune	UKE	INE	BER
Mennesker og sikkerhet	11 %	53 %	81 %	94 %
Digital førstehjelp for å unngå kontokapring	10 %	55 %	78 %	94 %
Avvikskultur	10 %	51 %	76 %	94 %
En sikker digital fremtid for Tim	7 %	51 %	73 %	83 %
Knask eller knep	8 %	43 %	65 %	83 %

Gjennomføring av e-læringer i Sikkerhetsmåneden 2022

	Oslo kommune	UKE	INE	BER	PBE	BYR
Verdifull informasjon	14 %	67 %	90 %	87 %	53 %	51 %
Svindel på nett	13 %	62 %	91 %	87 %	48 %	50 %
Mitt personvern	12 %	66 %	91 %	73 %	48 %	44 %
Klarer du å slå hackeren?	12 %	57 %	85 %	73 %	50 %	44 %

- Mål
  - Flere gjennomfører e-læringene



9 %
av
27 500

13 %
av
38 000

70%

Oslo

Phishingøvelsen: dette skjedde…

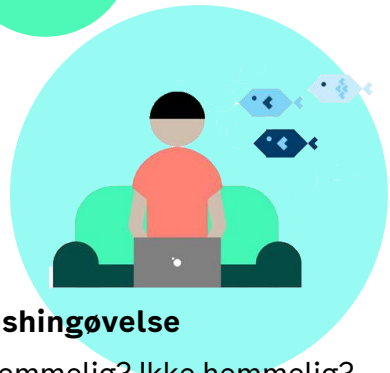
10. okt

E-læring

- Svindel på nett

13. okt

Målet:
Kjenne igjen svindel og melde fra



Phishingøvelse

- Hemmelig? Ikke hemmelig?
- E-post sendt til 36 317 medarbeidere torsdag 13.okt rundt kl 11 – gikk treigt…

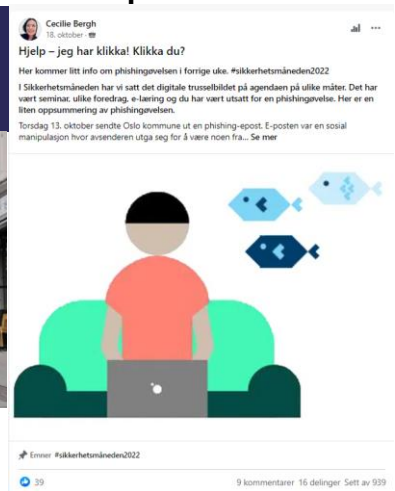
14. okt

Informasjon på intranett og Workplace

- Fra midnatt begynte ansatte å varsle på fellesgrupper på WP
- Vi bekreftet at det var en øvelse – ba om hemmeligholdelse en liten stund til…

18. okt

Informasjon på Workplace



Tim Talk om en ansatt i en kommune som ble svindlet

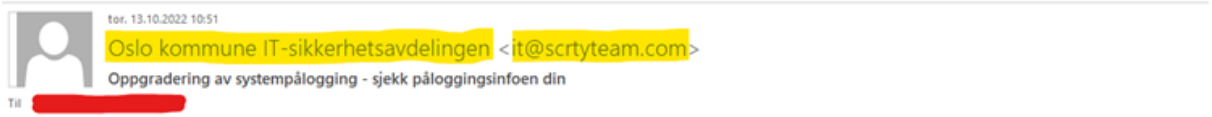
- Fokus på den ansattes opplevelse

Respons

Hei,

Takk for din rapport om phishing.
Godt jobbet med å identifisere at mailen var et phishing forsøk!
Dette har vært en phishing øvelse gjennomført av FIN som en del av sikkerhetsmåneden.
Vi setter stor pris på om du ikke forklarer dine medarbeidere om dette, for at resultatene av testen skal være mest mulig reelle.

Tegn på phishing
Hva syntes du var rart med mailen?



Hei,

Vi har oppgradert påloggingsprosedyrene for alle våre arbeidssystemer. Alle ansatte i Oslo kommune må logge på så snart som mulig for å sjekke at påloggingsinformasjonen deres fungerer.

Klikk her og skriv inn e-post og passord på innloggingsskjermen.

Takk skal du ha,

Hilsen oss på IT-sikkerhet
Oslo kommune

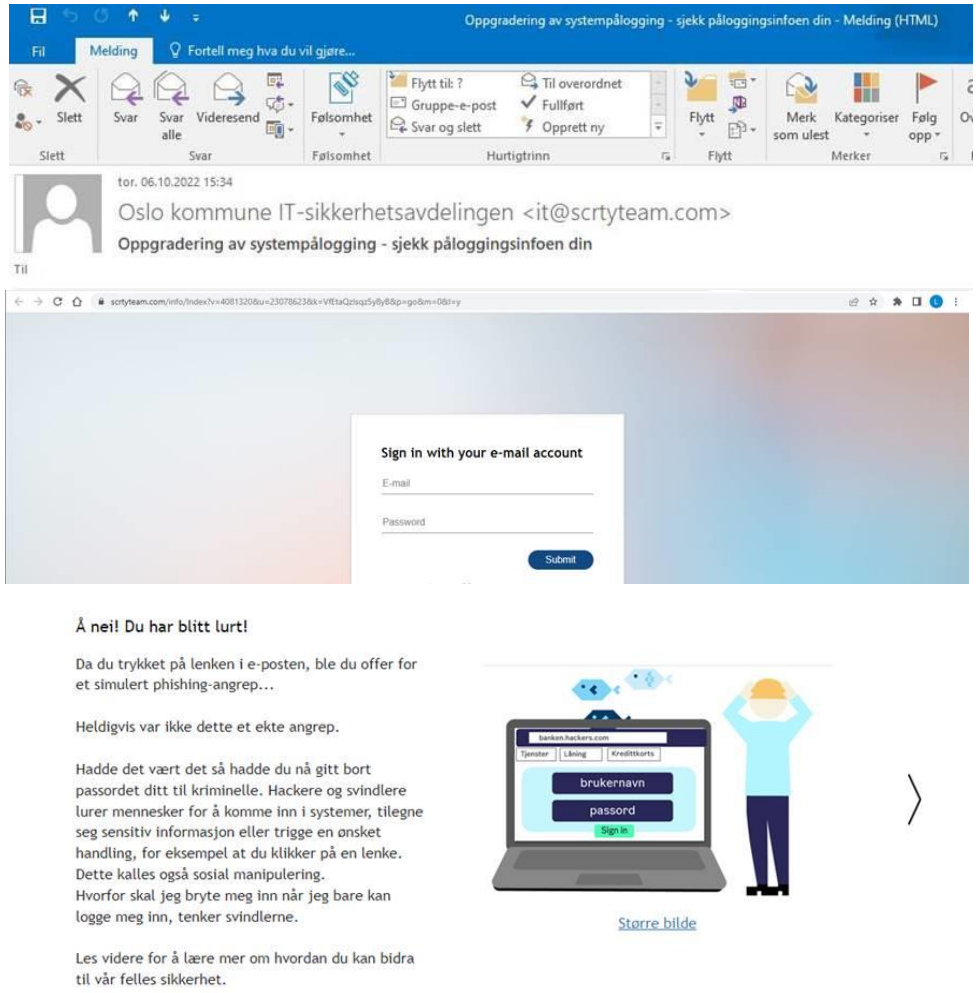
Mailen hadde mange phishing faretegn:

- Hvem er Oslo kommune IT-sikkerhetsavdelingen?
  - Jeg har jo ikke hørt om dem før?
- Den adressen så litt suspekt ut…
- Hvilken påloggingsprosedyre er det snakk om?
  - Hvorfor må jeg sjekke dette så snart som mulig?
  - Hvorfor skal ikke detaljene mine fungere?
- Skriv inn e-post og passord på en ukjent side?
  - Hva er den lenken for noe?

Phishing tester er en viktig måte for oss som driver med sikkerhet å teste hvor flinke ansatte er på å identifisere phishing e-poster.
Vi håper du også klarer å identifisere den neste phishing mailen du får!

Phishingøvelsen: hvor sårbare er vi ?

Phishingøvelse for alle på felles ikt-plattform



X % klikket på lenken

Over X ansatte ga fra seg passordet sitt

Av disse gjorde 42,5 % e-læringen

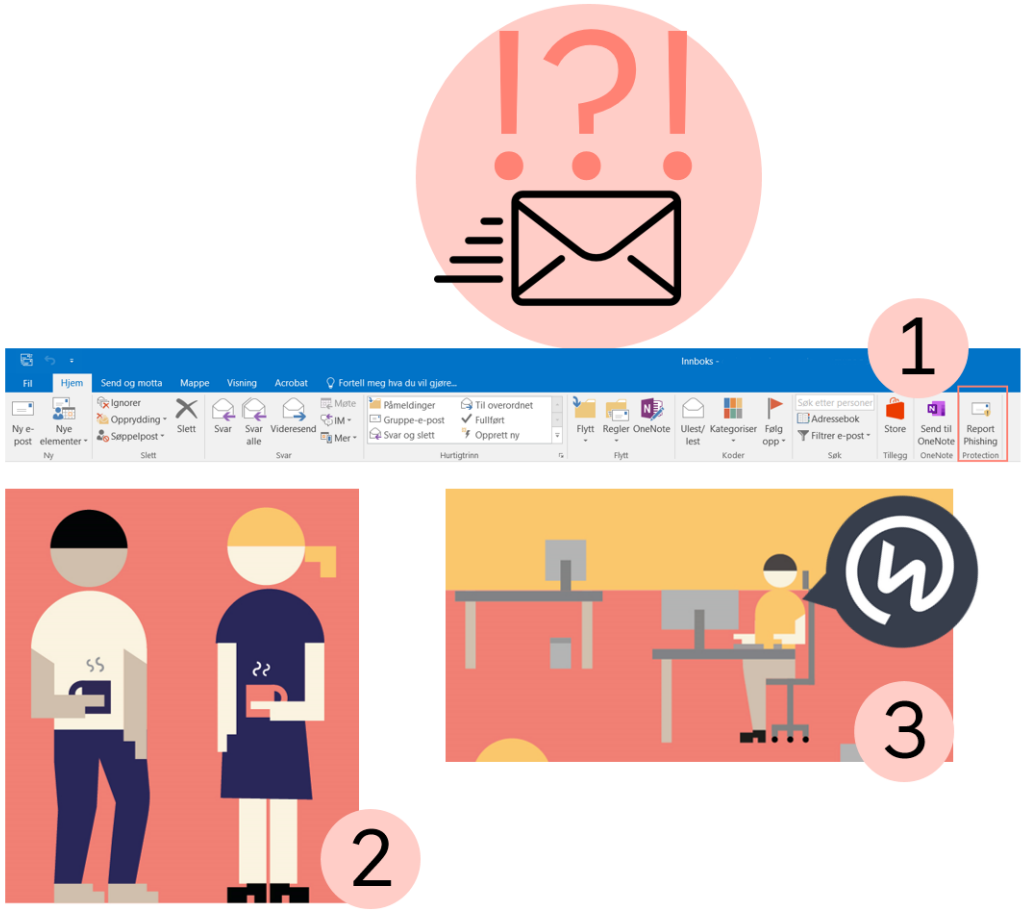
De siste spørsmålene i undersøkelsen

Spurte du noen om hjelp eller råd da du fikk phishingen?	Antall svar: 433
Ja	10.9 %
Nei	88.9 %

Vet du hvordan og til hvem du skal rapportere hvis du oppdager eller mistenker en trussel eller et nettangrep?	Antall svar: 433
Ja	59.8 %
Nei	40.2 %

Sånn ble resultatene delt…

- Koordinator i hver enkelt virksomhet har fått informasjon om resultater i egen virksomhet og om snittet i kommunen
  - Har også fått beskjed dersom egen virksomhet er på «topp 5» eller «bunn 5»

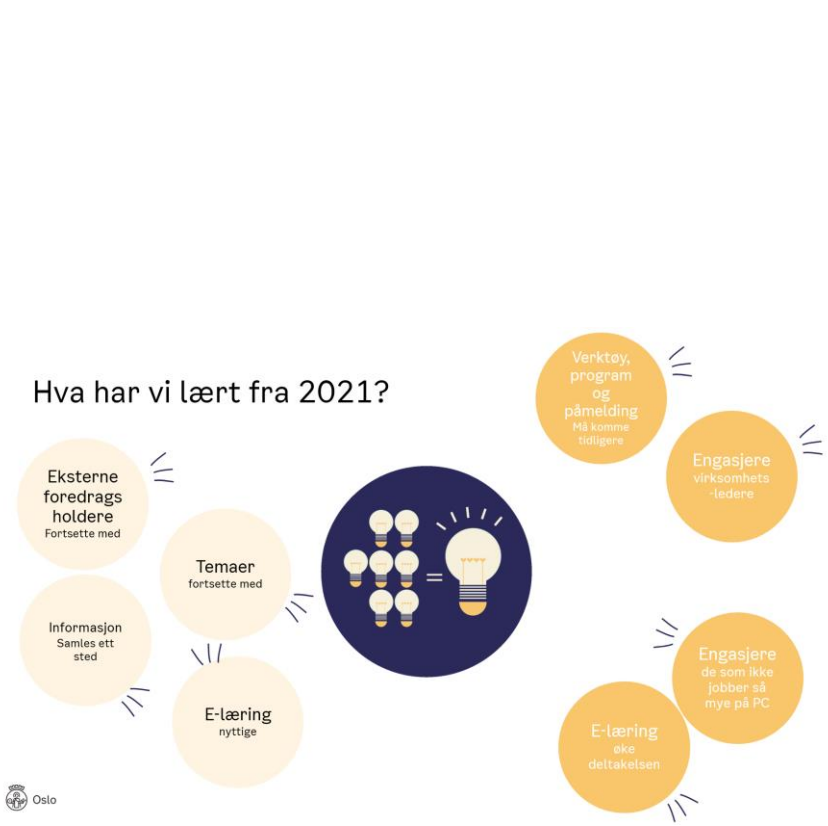


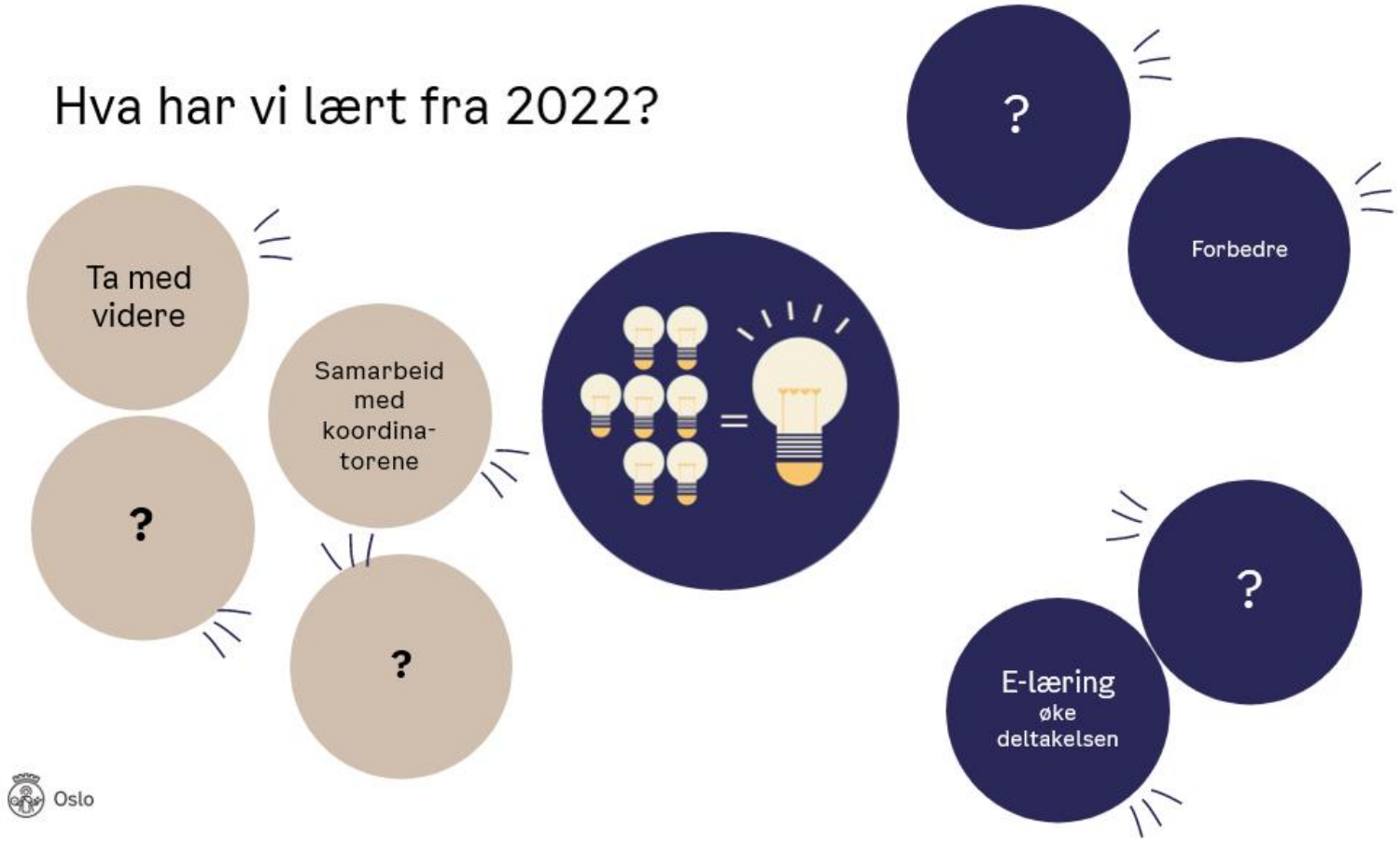
«Phishing-øvelsen var bra og avdekket behov for ytterligere kompetanseheving i grunnleggende sikkerhet og adferd på nett.»

«Jeg har lært enda mer om hva jeg gjør for å sjekke e-poster mot eventuell phishing og hvordan jeg skal rapportere videre.»

Oslo

Hva kan vi gjøre annerledes til neste år?



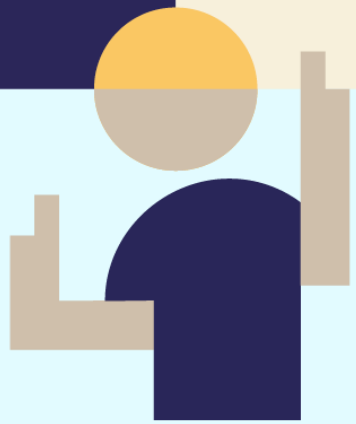


Avslutning

- Neste års forum – du kan melde deg på nå!
  - Se her: https://felles.intranett.oslo.kommune.no/informasjonssikkerhet-og-personvern/kompetanse/forum-for-informasjonssikkerhet-og-personvern/

Forum 2023

15. februar
19. april
7. juni
6. september
29. november



Avslutning

- Det blir sendt ut en evaluering etter dette forumet
- Kom gjerne med forslag til temaer for neste år!

God jul!