Masteroppgave

Masterstudium i atferdsvitenskap

Juni 2021

Informasjonssikkerhetskultur

En empirisk undersøkelse og teoretisk analyse av forsterkningsbetingelser for å melde dataangrep

Kandidatnavn: Ann Kristin Sjøflot
Emnekode: MALK5000
Antall studiepoeng: 30

Fakultet for helsevitenskap

OSLO METROPOLITAN UNIVERSITY
STORBYUNIVERSITETET

Forord

Arbeidet med masteroppgaven har vært både interessant, lærerikt og krevende. Interessant, fordi jeg har funnet et felt hvor atferdsvitenskapelig kunnskap kan komme til stor nytte. Lærerikt, fordi jeg har fått muligheten til å jobbe med hele gangen i et forskningsprosjekt. Fra idémyldring rundt problemstilling og tema, til å samle inn litteratur og lage en spørreundersøkelse, sende ut og rekruttere deltakere, analysere data, og ikke minst skriving og presentasjon av resultatene. Det har også vært krevende til tider, men jeg ser frem til å fortsette å jobbe med informasjonssikkerhet fra et atferdsvitenskapelig utgangspunkt.

Takk til Gunnar for god veiledning, inspirasjon og hyggelige samtaler. Takk til de som har bidratt med sin kunnskap og kompetanse fra IT-virksomheten. Takk til Lilja for hjelp med litteratursøk. Takk til venner, familie og lab-gruppa som var med på pilottesting av spørreundersøkelsen. Takk til alle som tok seg tid til å fortelle meg om informasjonssikkerhetsfeltet da jeg ringte og spurte, og takk til alle ved OsloMet som bidro i prosessen med å distribuere spørreundersøkelsen. Og ikke minst takk til alle som svarte på undersøkelsen.

Sammendrag

Dataangrep blir mer og mer vanlig. Dette vises både i statistikk, media, forskning og rapporter fra næringsliv og statlige virksomheter. Vi lever i informasjonens tidsalder, og informasjon er blitt en svært verdifull ressurs. Digitalisering av virksomheters verdier (informasjon) har skjedd raskt, og dette har økt behovet for sikkerhet og kompetanse for å bevare informasjonens integritet, tilgjengelighet og konfidensialitet. Dette er kjernen i informasjonssikkerhet. De tekniske verktøyene for sikkerhet har blitt veldig gode, men det er stor etterspørsel etter mer kunnskap om menneskers rolle i interaksjonen med teknologien.

Målet med dette masterprosjektet har vært å utforske hvilke betingelser som opprettholder, øker eller reduserer sannsynligheten for at ansatte i virksomheter melder ifra om dataangrep. Dette omfatter deltakernes kunnskap om dataangrep og informasjonssikkerhet, deres erfaringer med hendelser som har skjedd, og hvilke konsekvenser de har opplevd eller forventer å oppleve av å melde ifra om dataangrep. I samarbeid med et IT-konsulentfirma ble det utformet en spørreundersøkelse for å undersøke disse temaene.

Resultatene for hele utvalget presenteres i tabeller i resultatdelen. Det blir også trukket frem noen interessante funn av forskjeller mellom grupper. Resultatene diskuteres ut ifra teori som blir presentert innledningsvis. Mye av litteraturen om regelfølging (*compliance*) handler om kartlegging av faktorer som kan påvirke grad av regelfølging. Avslutningsvis argumenteres det for at en atferdsanalytisk tilnærming kan bidra med en praktisk anvendelse av atferdsprinsipper i kartlegging av årsaksforhold og tiltak for å endre atferd.

Stikkord: menneskelig atferd, informasjonssikkerhet, organisasjonskultur kultur, dataangrep, ledelse.

Abstract

Cyberattacks have become more and more common. This is evident from statistics, media, research and reports published by businesses and governmental institutions. We are living in the age of information, and information has become an extremely valuable resource. Digitalization of the assets of businesses has progressed quickly, and this has increased the need for security management and competence to keep the integrity, availability and confidentiality of information. This is the core of information security. The technical tools to increase security have high quality, but there is a great demand for more knowledge about human factors in interaction with this technology.

The goal of this project has been to explore what conditions that sustain, increase, or decrease the probability of employees reporting cyberattacks. This involves their knowledge about cyber security and attacks, their experiences from relevant events, and what consequences they have experienced or expect to experience, from reporting a cyber-attack. In collaboration with the participating IT-firm, a survey was developed to investigate these topics.

The average results for the entire selection are presented in tables in the result section of this paper. Some interesting differences between some groups, have been highlighted in the results. The results will be discussed based on theory presented in the theory-section. Much of the literature about compliance focus on factors that influence compliance. Finally, arguments for a behavior analytic approach to tackle the human aspect in information security will be discussed.

Key words: human behavior, information security, organizational culture, cyber-attack, management

Innholdsfortegnelse

Bakgrunn for Prosjektet

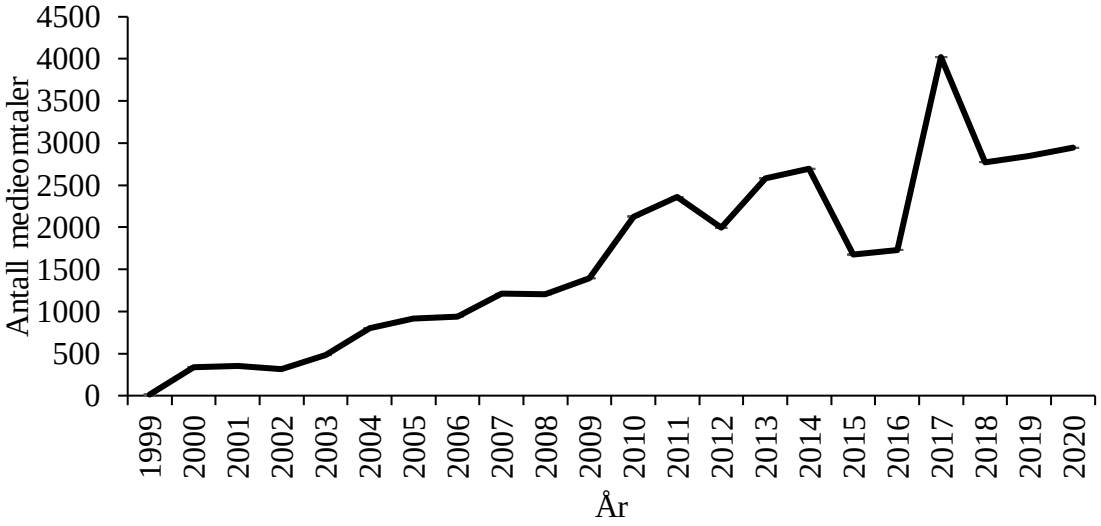
Økt grad av digitalisering og utvikling innen informasjons- og kommunikasjonsteknologi (IKT) har bidratt til effektivisering, men også økt risiko (Nasjonal Sikkerhetsmyndighet, 2020; NorSIS, 2021). IKT er en uunngåelig del av arbeidshverdagen til mange i Norge, og virksomheter er helt avhengige av det fungerer som det skal. Dette er en lønnsom mulighet for de som har kunnskap og ressurser til å angripe virksomhetene digitalt. Løsepengevirus, også kalt krypteringsangrep, er en av de vanligste typene dataangrep som rammer norske virksomheter (Næringslivets Sikkerhetsråd, 2020). Angriperne kommer seg inn i virksomhetens digitale infrastruktur, krypterer all informasjonen og krever løsepenger for å gi tilbake tilgangen. Tilgang til virksomhetenes digitale systemer kan oppnås gjennom å utnytte både tekniske og menneskelige svakheter. For eksempel ansattes passord og brukernavn stjeles, ved å sende ut phishing-epost med linker, eller vedlegg, som de ansatte blir bedt om å klikke på (NorSIS, 2021).

For å fanges opp et dataangrep så raskt som mulig, er det viktig at de som blir utsatt melder ifra. I dette masterprosjektet ble det utarbeidet og sendt ut en spørreundersøkelse til seks norske virksomheter. Undersøkelsen hadde som formål å få svar på hvilke betingelser som kunne påvirke melding av dataangrep i virksomhetene. Med betingelser så menes hvilke forkunnskaper ansatte har om dataangrep og melding av hendelser, deres erfaringer med melding av dataangrep, og faktiske eller forventede konsekvenser av å melde ifra om dataangrep.

Mediesaker. Nyhetsbildet dekker i økende grad dataangrep. Figur 1 viser resultatene av et søk i Atekst med søkeordene «Dataangrep, OR informasjonssikkerhet, OR hacking, OR datavirus, OR cybersikkerhet» for saker publisert i norsk media fra 1954 til 03.05.2021. Ett treff i 1990 ble fjernet da det var lagt inn med feil årstall. Her ser man en tydelig økende trend på antall publikasjoner.

Figur 1

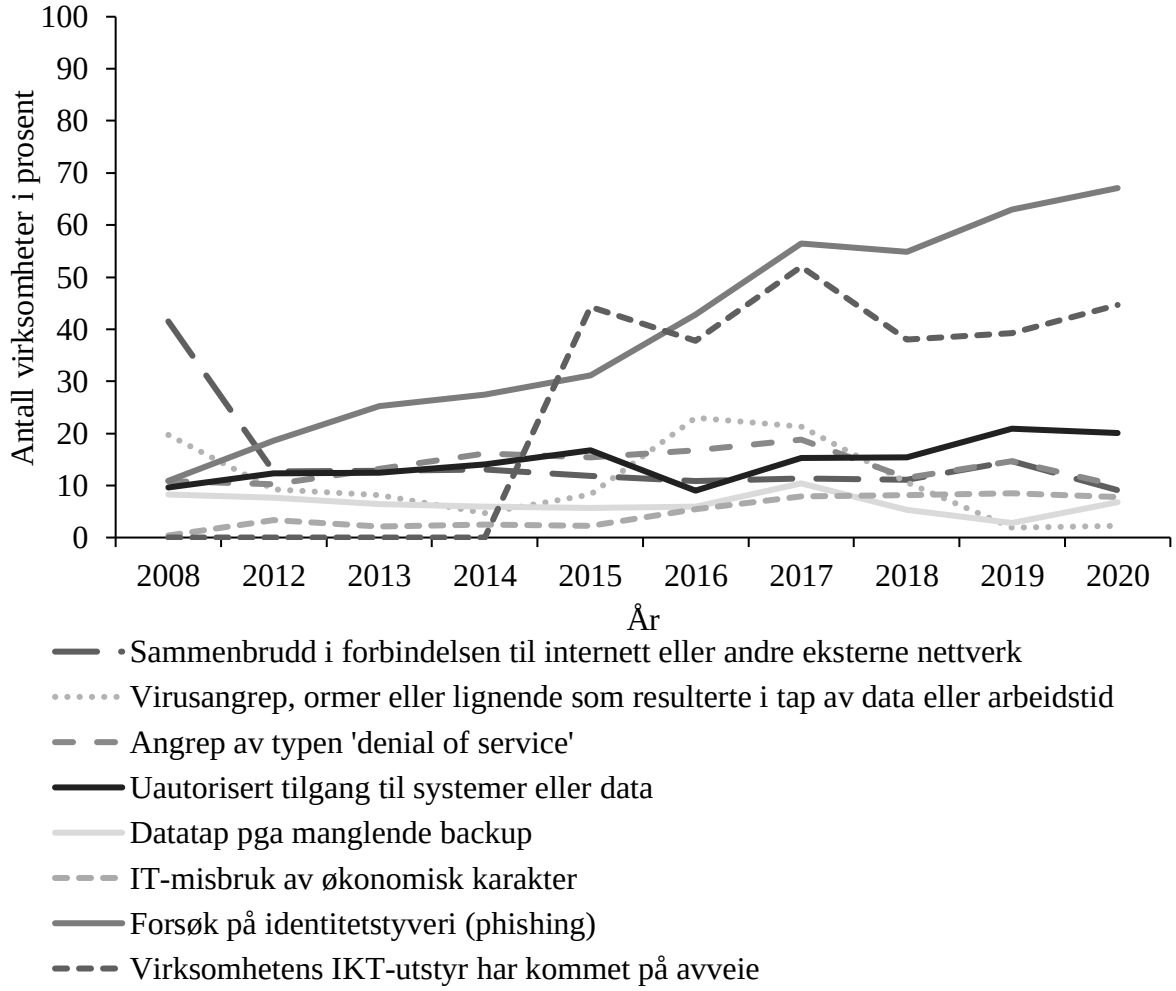
Antall medieomtaler i norsk media fra 1945-2020 hentet fra Atekst 03.05.21



Statistisk Sentralbyrå (SSB). Som vist i figur 2 er dataangrep og IKT-problemer i statlige virksomheter er svært vanlig (Statistisk sentralbyrå, 2021). En tydelig trend her er den økende forekomsten av phishing-angrep. Denne typen IKT-sikkerhetsproblem har økt fra 42.8% i 2016 til 67.1% i 2020, og er det mest vanlige. Samtidig som forekomsten av dataangrep øker, har også graden av digitalisering økt betraktelig i løpet av 2020. Dette blir sett på som en konsekvens av COVID-19-pandemien (Pay, 2021). Dette har hatt positive konsekvenser, slik som effektivisering. Mer informasjon blir gjort tilgjengelig, både for ansatte i virksomhetene og kriminelle (Nasjonal Sikkerhetsmyndighet, 2020).

Figur 2

Antall statlige virksomheter (i prosent) som har opplevd forskjellige typer IKT-problemer



Mørketallsundersøkelsen 2020. Næringslivets sikkerhetsråd (NSR) publiserer hvert andre år sin undersøkelse om IT-tilstanden i privat og offentlig næringsliv. Undersøkelsen er basert på 1601 telefonintervjuer hos norske virksomheter med 5 eller flere ansatte. Her har de undersøkt blant annet organisering av IT-driften, informasjonssikkerhetshendelser, årsaker, håndtering og følger av hendelsene og personvernregelverk og sikkerhetsbevissthet hos virksomhetene (Næringslivets Sikkerhetsråd, 2020).

Undersøkelsen viser at den vanligste årsaken til sikkerhetsbrudd er tilfeldigheter og uflaks. Menneskelige feil kommer på andreplass, og nummer tre er mangel på sikkerhetsbevissthet hos ansatte. I snitt ble like mange sikkerhetsbrudd oppdaget gjennom

rutinesjekk som ved en tilfeldighet. Dette påpekes som svært bekymringsverdig. Undersøkelsen viste også at virksomheter sjelden rapporterer hendelser til institusjoner slik som politiet og NorCERT eller sektor-CERT (Næringslivets Sikkerhetsråd, 2020).

Disse institusjonene jobber både forebyggende og har en beredskapsfunksjon. De kan kontaktes for bistand når informasjonssikkerhetshendelser oppstår, og de vil også varsle andre virksomheter i samme sektor om pågående dataangrep (NorSIS, 2015). Ved å ikke rapportere inn hendelser får ikke virksomheter nytte av disse ressursene. Flere rapporter påpeker derfor behovet for mer åpenhet om dataangrep mellom virksomheter for å bidra til økt sikkerhet for fellesskapet (NorSIS, 2021; Næringslivets Sikkerhetsråd, 2020).

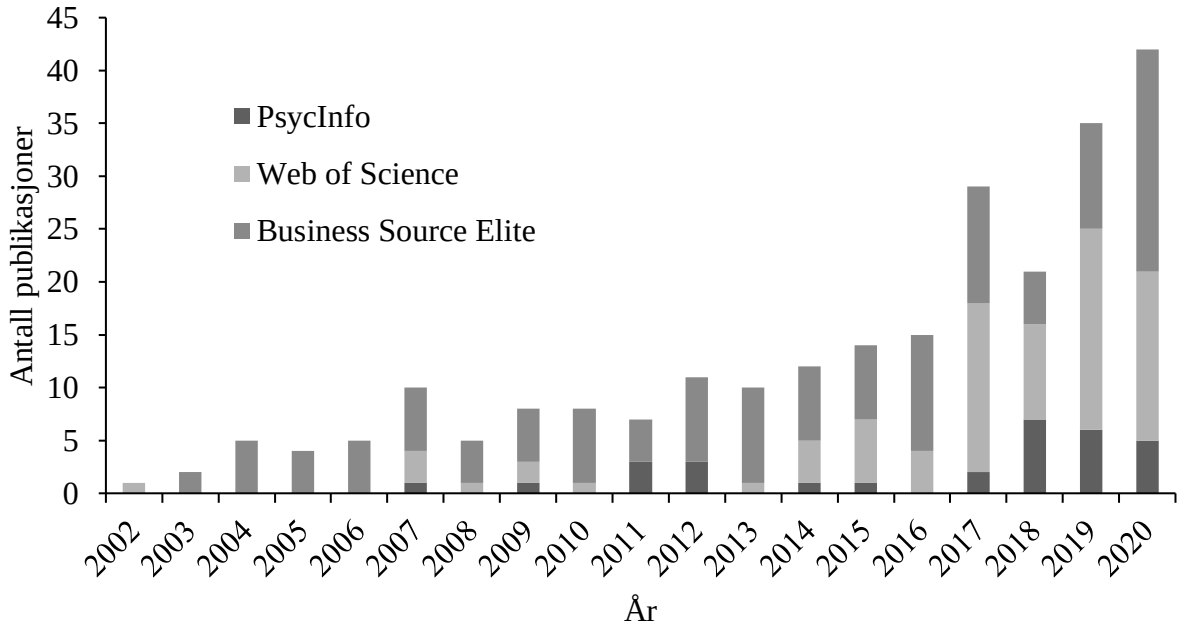
Risiko 2020. Nasjonal sikkerhetsmyndighet (NSM) publiserer hvert år en rapport om det nasjonale risikobildet. For året 2020 trekker de blant annet frem økende avhengighet av elektronisk kommunikasjon, satellittbaserte tjenester, digitale infrastrukturer som risikofaktorer (Nasjonal Sikkerhetsmyndighet, 2020).

Trusler og Trender 2021. Denne årlige rapporten publiseres av Norsk senter for informasjonssikring (NorSIS). Den beskriver trusselbildet for både enkeltpersoner, små og mellomstore virksomheter (NorSIS, 2021). I tillegg til å gi et overblikk av de vanligste truslene mot informasjonssikkerhet, peker NorSIS på at åpenhet mellom virksomheter er viktig. De poengterer at dataangrep er svært vanlig, og at på grunn av endringene som følge av COVID-19 pandemien, har risikoen for dataangrep økt. Avslutningsvis trekker de fram viktigheten av å øke ansattes kunnskap om informasjonssikkerhet.

Vitenskapelige Publikasjoner. Figur 3 er basert på antall treff med de samme søkeordene som ble brukt i litteratursøket til dette prosjektet (vedlegg A). Søket til denne figuren ble gjennomført 21.05.2021.

Figur 3

Antall publikasjoner per år i tre forskjellige databaser, se litteratursøk for søkeord



Lovverk og Standarder. I 2016 ble *General Data Privacy Regulation* (GDPR) innført for medlemsland i EU/EØS, og i 2018 fikk Norge sin egen personvernlov – personopplysningsloven. Dette innebærer at virksomheter er pliktige til å behandle personopplysninger i henhold til personvernprinsippene, blant annet ved å sørge for at håndtering av personopplysninger ivaretar integritet, konfidensialitet og tilgjengelighet (Personopplysningsloven, 2018). Disse tre aspektene er kjernen i det som kalles informasjonssikkerhet. Konfidensialitet vil si at kun personer som har autorisasjon (godkjent tilgang) har tilgang til bestemt informasjon, integritet vil si at informasjonen er korrekt, ikke endret eller kan slettes av uvedkommende, og tilgjengelighet vil si at informasjonen er tilgjengelig for de som trenger den når den trengs (Datatilsynet, 2021a).

Det finnes også bransjestandarder for informasjonssikkerhet, slik som ISO27000-serien. Store virksomheter sitter ofte på mye større mengder informasjon, og er avhengige av et rammeverk for å håndtere dette. I tillegg er slike standarder relativt kostbare å

implementere, og er derfor mest hensiktsmessige i større virksomheter (Næringslivets Sikkerhetsråd, 2020).

Retningslinjer og Prosedyrer. Basert på krav som stilles i lovverk og forskrifter, utarbeider virksomheter retningslinjer for å tydeliggjøre blant annet roller, ansvarsområder, rutiner for vedlikehold og mer. Dette er del av virksomhetens styringssystem, som både skal sikre at lovverk og forskrifter blir overholdt, og at informasjonssikkerheten ivaretas (Datatilsynet, 2021b). Prosedyrer er mer spesifikke, praktiske og mangfoldige enn retningslinjer. De kan beskrive hvordan og når man skal bytte passord, oppdatere programvare, logge ut av programmer, hvor man kan og ikke kan ta med jobb-PC, eller hva man gjør når man mottar en phishing-epost.

Å følge retningslinjer og prosedyrer knyttet til informasjonssikkerhet omtales ofte som *information security policy* (ISP) *compliance*. Hvordan man opprettholder regelfølging (*compliance*), i tillegg til en beskrivelse av prosedyrer som regelstyring, vil bli presentert senere i oppgaven.

Menneskelige Faktorer

Informasjonssikkerhet har endret seg fra å være et hovedsakelig teknisk felt, innenfor spesialiserte avdelinger, til å være del av arbeidshverdagen til de fleste ansatte i en virksomhet. Selv om kravene som stilles til de forskjellige ansatte varierer avhengig av deres rolle i virksomheten, handler informasjonssikkerhet i stor grad om menneskelige faktorer. I Mørketallsundersøkelsen 2020 svarte Norske virksomheter at menneskelige feil var den nest vanligste årsaken til sikkerhetsbrudd, etter tilfeldigheter og uflaks som den vanligste årsaken (Næringslivets Sikkerhetsråd, 2020). Mennesker er en stor del av de fleste funksjonene i en virksomhet. Derfor er det er naturlig å forvente at mennesker er en del av både forebygging av og årsak til sikkerhetshendelser (Reason, 1997). Dette innebærer ikke bare atferd hos

endebrukere, men hvilke prioriteringer ledere gjør, hvordan sikkerhetsledere jobber og kommuniserer til alle andre ansatte i virksomheten (Ashenden, 2008).

Hva som regnes som menneskelige feil og årsaker til sikkerhetshendelser, kan være svært variert (Reason, 1997). Å definere den menneskelige faktoren i informasjonssikkerhet som kun *compliance*, er overforenklet. Det hindrer identifisering av funksjonelle relasjoner for spesifikke atferder, og hvordan disse relasjonene kan variere på tvers av individer, avdelinger og virksomheter (Blythe, 2013).

Indre Årsaksforklaringer og Virkelighetsfordobling. da Veiga og Martins (2015) beskriver informasjonssikkerhetskultur som delte grunnleggende antakelser, kunnskap, holdninger og tro, som påvirker atferden til ansatte. Sommestad et al. (2014) har gjennomgått 29 studier om ISP regelfølging, og alle studiene brukte variabler som var psykologiske konstrukter. De fleste studiene baserte seg på teorier slik som *Theory of Planned Behavior* (TPB) (Ajzen, 1991) og *Protection-Motivation Theory* (PMT) (Rogers, 1975).

Sommestad et al. (2014) skriver at «*A dominant theory used in these studies is that attitude is an antecedent of intention and that intention is as an antecedent of actual behaviour*» (s.50). Atferd er ikke separat fra intensjon og holdninger, å skille mellom disse begrepene skaper en virkelighetsfordobling. *Intensjon* og *holdning* er oppsummerende merkelapper for spesifikke atferder, både observerbare og ikke-observerbare (Ree, 2013). Man kan ikke kontrollere eller endre atferd gjennom psykologiske konstrukter, fordi disse er utilgjengelige som den uavhengige variabelen, og kan ikke manipuleres (Hayes & Brownstein, 1986). Selv om tanker ikke kan observeres direkte av andre enn den som utfører tenkingen, regnes det fremdeles som atferd. Tanker er verbalatferd, og kan forklares gjennom atferdsprinsippene (Skinner, 1966). Gjennom verbalatferd, slik som egenregler, kan man forklare hvordan regelstyring av fremtidige kontingenser kan påvirke atferd i nåtid (Malott,

1989). Det er atferd som er betydningsfull for resultatene, og det som må være målet for tiltak, ikke konstruktene (Hayes & Brownstein, 1986).

Kultur

En mye brukt definisjon av organisasjonskultur er Schein (1990). Med organisasjon menes en gruppe mennesker som har hatt et stabilt forhold over tid, og dermed en felles historie. Han definerer kultur som et mønster av grunnleggende antakelser utviklet av gruppen, som tilpasses eksterne faktorer, og integrerer interne faktorer. Tilpasningene som fungerer godt, videreføres til nye medlemmer som den riktige måten å oppfatte, tenke og føle i bestemte situasjoner (Schein, 1990, s. 111). Atferdsvitenskapelig kan denne definisjonen av kultur beskrives som individenes felles læringshistorie, og læringshistorien til et individ påvirker deres atferd i alle fremtidige situasjoner (Cooper et al., 2014).

Et individ kan være del av flere kulturer, avhengig av hvem de har felles læringshistorie med (Schein, 1990). Organisasjoner kan ha en overordnet kultur, og flere underkulturer. Med bakgrunn i systemteori og kognitiv teori, sier Schein at individer vil tilstrebe likevekt. Individer oppnår dette ved å redusere kognitiv dissonans, gjennom overensstemmelse av de grunnleggende antakelsene i kulturen man er del av. Uoverensstemmelse mellom antakelsene i forskjellige kulturer kan gjøre det vanskelig å finne retningen for denne likevekten (Schein, 1990).

En informasjonssikkerhetskultur vil være basert ansattes læringshistorie relatert til informasjonssikkerhet. I tillegg til formell opplæring, innebærer dette erfaringer fra egen, og kollegers arbeidshverdag. Mange virksomheter har spesialiserte avdelinger, og ofte kan det være forskjell i informasjonssikkerhetskultur mellom avdelingene (Sarkar et al., 2020). Kulturen kan også variere avhengig av andre faktorer, slik som kjønn, alder, eller geografisk plassering av forskjellige avdelinger (da Veiga & Martins, 2017). Om man ønsker å endre

informasjonssikkerhetskultur, er det derfor viktig at man kartlegger disse forskjellene, slik at man kan tilpasse eventuelle tiltak til hver enkelt underkultur.

Sikkerhetskultur. Organisasjonskultur er svært viktig når man skal jobbe med sikkerhet, fordi kultur preger alle områder og nivåer av en organisasjon. Kultur har en global effekt som kan skape lineære svakheter gjennom flere lag med sikkerhet (Reason, 1998). Sikkerhetskultur kan bidra til høy grad av sikkerhet, eller lav grad av sikkerhet. Uavhengig av kvaliteten på sikkerheten, vil organisasjonen uansett ha en kultur for det.

Reason (1997) presenterer syv hovedelementer i en sikkerhetskultur. Det første er at målet må alltid være maksimum sikkerhet, og det andre er at man ikke må glemme å være på vakt. Ansatte i organisasjoner som opplever få negative hendelser, eller hvor de ikke vet at hendelsene skjer, kan risikere å undervurdere, eller glemme den faktiske risikoen. Den atferdsanalytiske beskrivelsen av dette er at kontingenser knyttet til sikkerhetshendelser er så sjeldne, eller fraværende, at deres stimuluskontroll over ansattes sikkerhetsatferd svekkes (Palmer, 1991).

Det tredje elementet er å opprettholde en informert kultur (Reason, 1997). Dette innebærer å ha oppdatert informasjon om ansatte, teknisk utstyr, organisatoriske faktorer, miljøfaktorer og mer. For Reason er dette punktet kjernen i en god sikkerhetskultur, og påvirkes av de andre elementene.

Nummer fire er å skape en god rapporteringskultur. Dette bidrar til at man kan oppdage hendelser, sårbarheter og andre relevante variabler som påvirker sikkerheten i en virksomhet. Ansatte i mer perifere roller er ofte i større grad i kontakt med sikkerhetshendelser når de oppstår, og har mulighet til å varsle på et tidlig stadium (Reason, 1997). For å oppmuntre til at ansatte skal rapportere sårbarheter og hendelser, er det viktig at man har en rettferdig kultur, som er det femte elementet. Frykt for urettferdige negative reaksjoner fra leder og kolleger kan minske sannsynligheten for at en ansatt velger å si ifra om

en hendelse. Her bør man være bevisst på å ikke begå den fundamentale attribusjonsfeilen, å attribuere årsaker til individers disposisjon, heller enn deres situasjon (Ross, 1977). Hvis man i en sikkerhetshendelse kunne holdt alle variablene konstant, erstattet den involverte ansatte med en annen, og det fremdeles er sannsynlig at hendelsen vil oppstå – så er årsaken mest sannsynlig organisatorisk (Reason, 1997).

Punkt seks er å ha nok fleksibilitet i de organisatoriske strukturene til å endre kontroll- og ansvarsfordeling i krisesituasjoner. Det siste punktet er å skape en læringskultur. Man må lære av informasjonen man blir presentert med, og være villig til å implementere endringer når det trengs (Reason, 1997).

Kontingenser for Atferd i Sikkerhetskultur. Hvis kultur består av felles tanker, praksis og antakelser knyttet til problemløsing, og disse er definert ut ifra individers atferd, så er det individers atferd som må være målet for endring. En gruppe har ikke atferd i seg selv, det er individer som har atferd (Daniels & Bailey, 2014). Selv om man kan gjøre tiltak på gruppenivå, skjer atferdsendringen hos individer. Å endre individers atferd er det samme som læring (Catania, 2013).

Foranledning, Atferd og Konsekvenser (FAK). Individers atferd er alltid i interaksjon med deres indre og ytre miljø, og tidligere læringshistorie (Pierce & Cheney, 2017). Denne interaksjonen kan beskrives som et komplekset dynamisk system, hvor en hendelser har flere årsaker og konsekvenser (Axelrod & Cohen, 2000). Atferd påvirkes sjelden av kun én foranledning eller konsekvens, men skjer som følge av en kjede av kontingenser, som en strøm av kausalitet (Daniels & Bailey, 2014). Konsekvensene individer opplever etter en bestemt atferd, påvirker sannsynligheten for at den forekommer igjen (Cooper et al., 2014). Man kan påvirke sannsynligheten gjennom motiverende operasjoner (MO), og manipulasjon av foranledigende stimuli og konsekvensene av atferden. En PIC/NIC Analyse® av konsekvensene for atferden kan bidra til en bedre forståelse av perspektivet til den som utførte

atferden på tidspunktet den forekom, og hvilke funksjonelle relasjoner som var gjeldende (Daniels & Bailey, 2014).

Regler er Verbal Atferd. Regler er kontingensspesifiserende stimuli (Skinner, 1966). Skinner beskrev fire varianter av regler; advarsler, trusler, løfte og råd. Advarsler kan formuleres som «hvis du gjør dette …, så kommer dette til å skje …». Et løfte kan formuleres som «hvis du gjør dette …, så vil jeg gi deg dette…». Disse reglene beskriver både atferden og konsekvensen, altså spesifiserer de kontingensene for en spesifikk atferd. En fullstendig regel beskriver både foranledning, atferd og konsekvens. Regler kan være ufullstendige, men likevel være effektive, hvis man har en læringshistorie som gjør at regelen likevel har stimuluskontroll (Skinner, 1966).

Prosedyrer for håndtering av dataangrep kan beskrive hva en ansatt skal gjøre hvis de mottar en phishing-epost. Beskrivelse av foranledningen vil være at den ansatte mottar en phishing-epost. Dermed bør prosedyren beskrive atferden som denne skal utløse, for eksempel å videresende e-posten til IT-support. For at prosedyren skal regnes som en fullstendig regel bør den også spesifisere konsekvensene av atferden, for eksempel å anerkjenne at personen har bidratt til økt sikkerhet. Med dette har regelen endret den atferdsmessige funksjonen til phishing-eposten (Schlinger & Blakely, 1987).

Ekstinksjon. Prosedyren som ble beskrevet over vil kun fungere om flere forutsetninger er på plass. Den ansatte må ha lært å diskriminere mellom en phishing-epost, og vanlig e-post. Uten at stimulusen (phishing-eposten) har oppnådd stimuluskontroll, vil ikke regelen ha noen effekt (Cooper et al., 2014; Schlinger & Blakely, 1987). En annen forutsetning er at korrekt atferd i korrekt situasjon, må etterfølges av konsekvenser som øker sannsynligheten for at den forekommer igjen. Dette er forsterkning (Catania, 2013). Hvorvidt atferden hos hvert enkelt individ forsterkes av det å følge regelen i seg selv, er avhengig av individets læringshistorie, og bør ikke overlates til tilfeldigheter (Daniels & Bailey, 2014). Ved fravær av målrettede

forsterkningsbetingelser risikerer man at regelbryting forsterkes, for eksempel ved at personen sparer tid ved å ikke si ifra om phishing-eposten. Om forsterker ikke formidles kontingent på korrekt atferd, er atferden i praksis på ekstinksjon (Malott, 1989).

Glemming. Stimuli som forekommer sjeldent, eller som ansatte ikke kommer i kontakt med, gir ansatte få muligheter til å lære seg kontingensene knyttet til stimulusen. Dette fører til at stimuluskontrollen svekkes, og sannsynligheten for at atferden forkommer i nærvær av stimulusen minsker (Palmer, 1991). Høy grad av automatikk i håndtering av hendelser kan bidra til at ansatte ikke lærer å håndtere hendelser selvstendig, i tillegg til at det er kostbart, og kan redusere fleksibilitet og tilpasningsevne (Workman et al., 2008).

Diskontering. Når det gjelder de negative konsekvensene et dataangrep kan få for virksomheter, kan disse være langt frem i tid og knyttet til høy grad av usikkerhet (Gundersen, 2020). Konsekvenser på organisasjonsnivå er heller ikke egnet for å endre atferd hos individer (Daniels & Bailey, 2014). Mennesker en tendens til å feilvurdere sannsynligheten for at konsekvenser som er usikre eller langt fram i tid har, vil forekomme (Green & Myerson, 2004; Malott, 1989; Zohar & Erev, 2007). Dette kan knyttes til det andre hovedelement i en god sikkerhetskultur, at man ikke må glemme å være på vakt (Reason, 1997).

Regelfølging

Sikkerhet måles ofte som fravær av sikkerhetsbrudd (Reason, 2000). En prosedyre eller retningslinje vil aldri kunne ta høyde for variasjonen i mulige hendelser som kan oppstå, likevel er de viktige for organisasjonens læring, og for å håndtere kjent risiko (Reason, 1997). Gjennom å undersøke i hvilken grad ansattes atferd er i tråd med retningslinjer og prosedyrer, får man et bilde av hvilke faktorer som bidrar til en god sikkerhetskultur (da Veiga & Martins, 2015).

Variasjon og Seleksjon. I et system av teknologiske løsninger med høy grad av kontroll og predikerbarhet, er menneskelig atferd er en kilde til variasjon (Reason, 1997). Prosedyrer,

retningslinjer og andre standardiseringsmetoder, er del av denne teknologien (Larsen & Røyrvik, 2017). Virksomheter må bestemme hvilket handlingsrom og grad av autonomi for ansatte teknologien skal tillate, og hvilken grad av kontroll og predikerbarhet som er nødvendig for å opprettholde sikkerheten (Post & Kagan, 2007). For høy grad av sikkerhet og kontroll er svært ressurskrevende, og kan i ytterste konsekvens føre til konkurs, samtidig som ingen kontroll kan få katastrofale utfall (Reason, 1997).

Prosedyrer og retningslinjer kan også oppleves som en hindring i utførelsen av arbeidsoppgavene til ansatte, som enten kan gå ut over regelfølgingen, eller kvaliteten i arbeidet deres (Ahmad et al., 2019; Kajtazi et al., 2018; Post & Kagan, 2007). Miljøvariabler slik som retningslinjer og prosedyrer kan øke risiko ved at de begrenser fleksibiliteten til ansatte til å tilpasse atferden sin i kritiske situasjoner (Reason, 2000). Derfor er det er særlig viktig at de med ansvar for informasjonssikkerhet er i stand til å kommunisere godt med både endebrukere og ledere. Hvis de som er ansvarlige for å utforme retningslinjer og prosedyrer ikke har god forståelse av eller kontakt med endebrukere, er det større sannsynlighet for at risikoen vil øke på grunn av lav brukervennlighet (Kraemer & Carayon, 2007).

Et system med høy grad av variasjon, har større sannsynlighet for å ha en variant som vil bli selektert for ved endrende miljøvariabler, altså er det mer robust (Axelrod & Cohen, 2000). Virksomheters sikkerhet jobber mot et miljø med høy grad av variasjon og innovasjon, og de kan ha nytte av økt kompleksitet og variasjon internt (Sandaker, 2009). Men for å øke kontroll og predikerbarhet, og dermed redusere risiko, ønsker man ofte å fjerne variabiliteten som menneskelig atferd utgjør (Reason, 2000). Dette trenger nødvendigvis ikke å redusere risiko, da det ofte er på grunn av variasjon i menneskers atferd og evne til å være fleksibel at man kan tilpasse seg plutselige endringer i miljøet. Dette forutsetter at ansatte har fått opplæring, noe som ofte krever mer ressurser enn å utforme prosedyrer, for å regelstyre utrente ansatte (Axelrod & Cohen, 2000; Reason, 1997). Uavhengig av opplæringen er den

mest sannsynlige atferden, altså den som selekteres, bestemt av forsterkningsbetingelsene (Daniels & Bailey, 2014).

Skinner beskriver tre nivåer av seleksjon; biologisk, atferd og kultur (Skinner, 1981). I kompleksitetsteori skiller man ikke like tydelig, men beskriver seleksjon som et samspill mellom alle tre nivåer (Axelrod & Cohen, 2000; Sandaker, 2009)**.** Atferd og tradisjoner som vedvarer over tid er ikke nødvendigvis de som øker sikkerheten i en organisasjon, men de som har høyest sannsynlighet for å forekomme basert på forsterkningsbetingelsene (Daniels & Bailey, 2014). Hvis prosedyrer og retningslinjer ikke håndheves ved at det også arrangeres forsterkningsbetingelser for atferden de er ment å påvirke, vil de ikke ha en atferdsendrende effekt. Da vil det oppstå en diskrepans mellom den deskriptive atferden, den vi faktisk gjør, og den normative, det reglene sier man skal gjøre (Angner, 2016). Fullstendige regler har ingen hensikt hvis forsterkningsbetingelsene i miljøet forsterker annen atferd enn den regelen beskriver. Da må man enten skrive om regelen, eller endre forsterkningsbetingelsene.

Håndheving av retningslinjer og prosedyrer. Hvis man ønsker å øke regelfølging må man først definere hvilke spesifikke atferder man skal forsøke å endre (Daniels & Bailey, 2014). Atferd knyttet til informasjonssikkerhet blir ofte redusert til bare «regelfølging», men består av mange forskjellige atferder, som hver har forskjellige foranledninger og konsekvenser (Blythe, 2013). Ofte møter virksomheter på utfordringer med å håndheve retningslinjer (Herath & Rao, 2009).

Straff Øker Ikke Atferd. En mye brukt fremgangsmåte for å få ansatte til å følge regler er avskrekkende tiltak og trusler om straff (D'Arcy & Herath, 2011; Herath & Rao, 2009; Padayachee, 2012). Straff defineres av Azrin og Holz (1966) som en prosedyre hvor konsekvensen av en respons fører til at responsen synker i frekvens, styrke eller varighet. Konsekvensen som følger etter responsen er da en straffer. Daniels og Bailey (2014) skiller mellom *punishment* (positiv straff) og *penalties* (negativ straff). Forskjellen er at ved positiv

straff formidles en straffende konsekvens, mens ved negativ straff fjernes en forsterker. Formålet med straff er å redusere forekomsten av en uønsket atferd (Cooper et al., 2014).

For at en straffeprosedyre skal være mest effektiv, bør konsekvensen formidles umiddelbart kontingent på hver respons, med høy nok intensitet. Samtidig bør man forhindre at målatferden samtidig forsterkes, forsterke alternative responser og minimalisere MO for målatferden. Straff er heller ikke noe som bør formidles over lengere tid. I tillegg til at den kan miste effekten, kan den ha negative bivirkninger, slik som aggresjon mot den som formidler straffen og andre, uønskede emosjonelle responser, undertrykkelse av større deler av atferdsrepertoaret og unngåelse (Cooper et al., 2014).

General Deterrence Theory (GDT) er en teori som har preget forskning på hvordan man skal håndheve retningslinjer og prosedyrer innenfor informasjonssikkerhet. Teorien baserer seg på trusler om sanksjoner for ulovlig atferd, og atferd som ikke er i tråd med retningslinjer. Forskning på bruk av straff for å øke regelfølging har ikke gitt et tydelig svar på effekten av slike tiltak (Aurigemma & Mattson, 2017; D'Arcy & Herath, 2011; Xue et al., 2011). Atferden til de som formidler straffen kan også forsterkes av at de umiddelbart oppnår ønsket reduksjon av den uønskede atferden hos andre. Her bør man i så fall benytte reduksjonen i uønsket atferd til å forsterke den atferden man faktisk ønsker (Daniels & Bailey, 2014).

Forsterkning Begge Veier. Reduksjon av uønsket atferd, betyr ikke øking av ønsket atferd. Ønsker man å øke regelfølging, må man bruke forsterkning (Daniels & Bailey, 2014). Om ansatte har en regel om at de skal si ifra til IT-ansvarlig om et dataangrep, må atferden forsterkes om den oppstår. Ved å utforme en regel for den IT-ansvarlige som sier «når en ansatt melder ifra om et dataangrep skal du si takk», bidrar man i å opprettholde ønsket atferd fra flere retninger. Atferd skjer alltid i en kjede av kontingenser, og en atferd kan være foranledning for en annen (Daniels & Bailey, 2014). Her er ansatte med ansvar for

informasjonssikkerhet avhengige av å ha kommunikasjonsferdigheter og kompetanse i å jobbe med mennesker (Ashenden, 2008).

Hjemmekontor. Flere rapporter har uttrykt bekymring for svekket sikkerhet med økende grad av hjemmekontor (Nasjonal Sikkerhetsmyndighet, 2020; NorSIS, 2021; Næringslivets Sikkerhetsråd, 2020). Mørketallsundersøkelsen 2020 viser ingen endringer i antall hendelser i snitt, men fordelt på sektor rapporteres det en økning innen industri, helse og sosial, varehandel og tjenesteytende næringer (Næringslivets Sikkerhetsråd, 2020, s. 42). Det har også blitt rapportert en reduksjon i sikkerhet innenfor offentlig administrasjon og undervisning. For de fleste innebærer også hjemmekontor skifte av miljø, og det er ikke usannsynlig at kontingensene for informasjonssikkerhetsatferd som gjaldt på ordinært kontor kan bli påvirket av dette miljøskiftet.

Problemstilling. Problemstillingen ble utformet basert på aktualiteten av tema, litteraturen om regelfølging innen informasjonssikkerhet, nytten av et atferdsvitenskapelig perspektiv på tema, og samtaler med personer som jobber innen dette feltet. Formålet med undersøkelsen var å utforske hvilke betingelser som påvirker atferd knyttet til informasjonssikkerhet, særlig varsling av dataangrep.

Undersøkelsen ble utformet for å få en bedre forståelse av foranledning, atferd og konsekvenser av atferden. Å reagere passende på foranledninger til atferd, innebærer at stimuluskontroll er etablert, og det kan knyttes til ansattes kunnskap om informasjonssikkerhet. Deltakerne ble også spurt om sine erfaringer med dataangrep, og hva de har valgt å gjøre i slike situasjoner. Deretter ble de spurt om konsekvensene av deres handlinger. Dette ble vurdert til å gi en god oversikt over hvilke atferdsmessige betingelser som er til stede for å si ifra om dataangrep.

På de fleste spørsmålene var det mulig å velge flere svaralternativ. Dette var for å gi et mest mulig realistisk bilde av kunnskap, hendelser og konsekvenser, fordi en person i virkeligheten kan velge å gjøre flere forskjellige ting i samme situasjon. Prosentene som er oppgitt i resultatdelen viser derfor hvor stor andel av de som har svart på spørsmålet som har valgt hvert enkelt alternativ. På påstandene var det kun mulig å krysse av for ett alternativ.

Metode

Rekruttering. Det ble gjort et bekvemmelighetsutvalg av deltakere på grunnlag av hvilke virksomheter som var tilgjengelige og antagelig ville delta. Den samarbeidende IT-bedriften bidro med rekruttering av alle virksomhetene bortsett fra Universitetet, som ble rekruttert av masterstudenten.

Etter det ble oppnådd tilgang til virksomhetene ble det sendt ut e-post med invitasjon til deltakelse til alle ansatte i virksomhetene. E-posten med lenke til undersøkelsen ble sendt ut 15.03.21 til alle ansatte i virksomhetene som skulle delta. En påminnelses-e-post ble sendt ut en uke etter. Linken til undersøkelsen var åpen frem til 13.04.21, slik at spørreundersøkelsen kunne besvares når som helst i dette tidsrommet.

Litteratursøk. Som del av innsamlingen av relevant informasjon til prosjektet ble det gjennomført et litteratursøk 08.03.2021. Det ble brukt tre databaser, Business Source Elite, PsycInfo og Web of Science. Inklusjonskriteriene var at treffene hadde blitt publisert i et fagfellevurdert tidsskrift og at de var på engelsk eller et skandinavisk språk. Det ble ikke satt noen kriterier utover disse. Søket ga totalt 246 treff. 132 i Business Source Elite, 28 i PsycInfo og 86 i Web of Science. Etter å ha fjernet duplikater var det 238 treff (131, 26, 81). Søkeord og søkehistorikk i vedlegg A.

Spørreundersøkelsens innhold. Alle som ble invitert til å delta ble informert om at deltakelsen var frivillig, og fikk informasjon om lagring og behandling av deres besvarelser i informasjonsskrivet de ble bedt om å lese (Vedlegg B). Etter at de ga samtykke til deltakelse,

ble de videresendt til selve undersøkelsen (Vedlegg D). Informasjonsskriv og selve undersøkelsen var kun på norsk. Undersøkelsen bestod av seks deler, med totalt 30 spørsmål og 26 påstander. Det ble estimert at det skulle ta 10-12 minutter å besvare undersøkelsen. Hvilke spørsmål hver deltaker fikk var til en viss grad avhengig av deres svar. Alle deltakerne svarte ikke nødvendigvis på alle 30 spørsmålene. For eksempel hvis du svarte «nei» på «har du hatt hjemmekontor i noen som helst utstrekning siden mars 2020?», så ville du ikke få spørsmål om du hadde opplevd dataangrep på hjemmekontor. Spørsmålene og påstandene i undersøkelsen ble delt inn i disse seks temaene:

Bakgrunnsinformasjon. Denne delen inneholdt spørsmål om deltakernes kjønn, alder, virksomhets- og avdelingstilhørighet og stillingsnivå.

Scenario. Denne delen inneholdt fire spørsmål knyttet til et scenario.

Kunnskap. Denne delen inneholdt seks spørsmål og syv påstander om deltakernes kjennskap til rutiner og regelverk knyttet til informasjonssikkerhet og dataangrep.

Hendelser. Denne delen inneholdt 11 spørsmål og åtte påstander om deltakerne hadde opplevd hendelser selv, hvorvidt de meldte ifra om hendelsene og eventuelt hvorfor ikke.

Konsekvenser. Denne delen inneholdt tre spørsmål og 7 påstander om hvilke konsekvenser deltakerne fikk, eller forventet å få som følge av å melde ifra om de ble utsatt for dataangrep.

Hjemmekontor. Denne delen inneholdt seks spørsmål og fire påstander for å undersøke om deltakerne opplevde forskjeller knyttet til informasjonssikkerhet på hjemmekontor i forhold til vanlig kontor.

Pilottesting. Før utsendelse av undersøkelsen til virksomhetene ble den testet av 15 personer. Dette inkluderte venner og bekjente, og også medlemmer av en lab-gruppe ved institutt for atferdsvitenskap ved OsloMet. Undersøkelsen ble bearbeidet basert på tilbakemeldingene fra pilottesten.

Tjenesteleverandør. Leverandøren av undersøkelsesverktøyet er Nettskjema, som er utviklet og eid av Universitetet i Oslo (UiO), hvor OsloMet har avtale om bruk av løsningen. Nettskjema er en løsning for utforming av spørreundersøkelser, innsamling og lagring av data. Data som samles inn, blir lagret kryptert. Nettskjema oppfyller krav til universell utforming, og undersøkelser kan besvare både på mobil, nettbrett og datamaskin.

Analyser. Dataene som ble samlet inn gjennom undersøkelsen blir fremstilt som prosenter i tabeller, eller presenteres visuelt i figurer. Prosentene for hele utvalget og fordelingen av besvarelser etter grupperingsvariablene ble regnet ut ved bruk av SPSS og Excel. Basert på resultatene av undersøkelsen og problemstillingen, blir noen forskjeller mellom grupperingsvariablene kjønn, virksomhet, felt og lederansvar trukket frem.

På noen av spørsmålene var det mulig å krysse av for svaralternativet «annet», og dermed beskrive nærmere i en tekstboks. De spørsmålene hvor en betydelig prosent valgte dette alternativet, vil kommenteres avslutningsvis i resultatdelen.

Resultater

Antall besvarelser. Invitasjon til å delta i undersøkelsen ble sendt ut til totalt 4101 personer (2995 OsloMet, 1000 kommuner, 28 IT konsulent, 20 revisjon, 8 rådgivning, 50 kraftverk). Det var totalt 723 personer som svarte på samtykkeskjema. Av disse var det 672 som svarte at de ønsket og delta, og 51 som svarte at de ikke ønsket å delta. Det var 6 personer som leverte besvarelse 2 ganger. Her ble den siste besvarelsen slettet. Det var også 6 personer som hadde krysset av for at de ikke ville gi samtykke, men likevel leverte en besvarelse på undersøkelsen. Disse ble også slettet. Resultatene som presenteres under er basert på de gjenværende 571 besvarelsene. Undersøkelsen hadde en svarprosent på 13,92%.

Tabell 1

Beskrivelse av utvalget med antall personer i hver gruppe

		n	%
Kjønn	Kvinne	348	60,90
	Mann	219	38,40
	Annet/ønsker ikke å oppgi	4	0,70
Virksomhet	Universitet	439	76,90
	Kommune	94	16,50
	IT-konsulentfirma	20	3,50
	Revisjonsfirma	12	2,10
	Rådgivningsvirksomhet	5	0,90
	Kraftverk	1	0,20
Felt	Forskning og undervisning	347	60,80
	Ledelse og administrasjon	89	15,60
	IT	36	6,30
	Økonomi	33	5,80
	Markedsføring/kommunikasjon, salg og tjenestelevering	22	3,90
	Kundeservice	15	2,60
	Drift og vedlikehold, produksjon	15	2,60
	HR og personal	14	2,50
Lederansvar	Nei	457	80
	Ja	114	20
Hvis ja, hvilket nivå	Mellomleder	64	56,1
	Leder	34	29,8
	Medarbeider	16	14

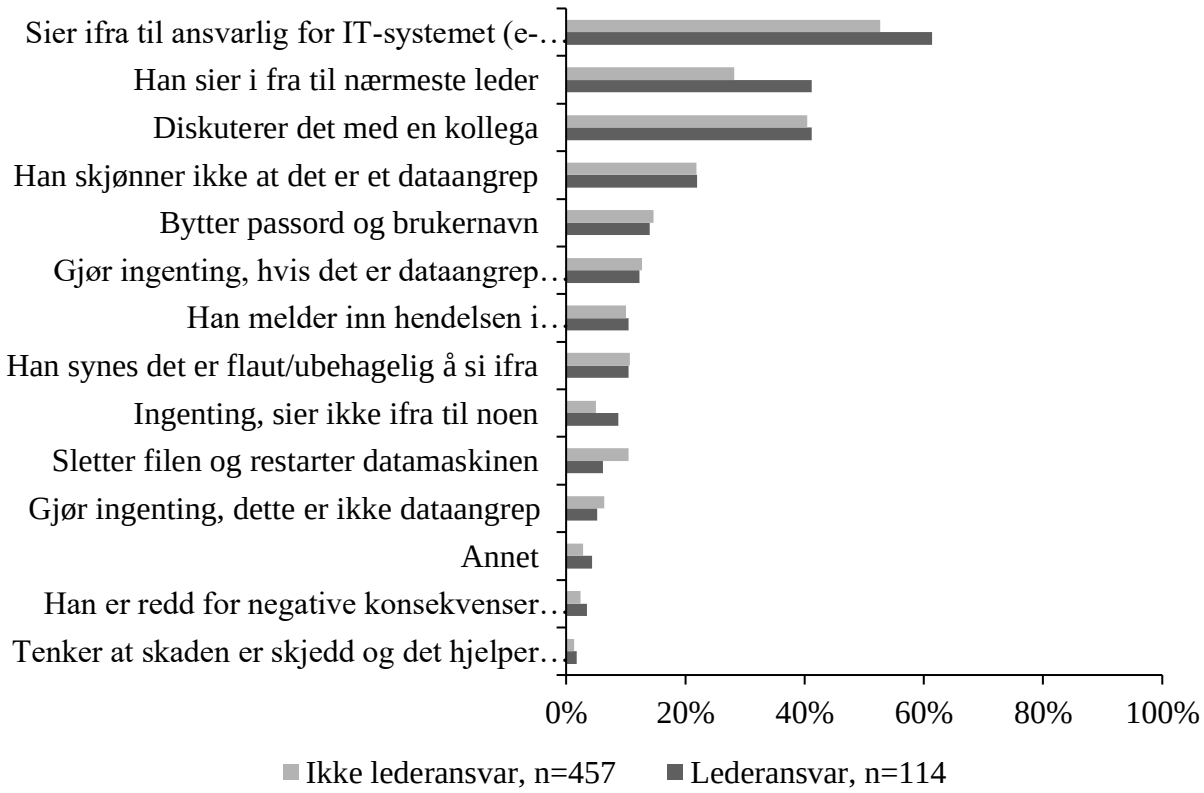
Note. N=571. Gjennomsnittlig alder 48.95 år (*SD*=11.46).

De gjennomsnittlige besvarelsene fra alle deltakerne fordelt på tema, spørsmål og påstander er presentert i tabell 2-13 etter referansene. I tillegg blir det presentert noen sammenligninger av forskjellige grupper i figur 4 til 10. Det er også viktig å huske at undersøkelsen har delt opp utvalget etter hva de svarer, flere av spørsmålene er bare besvart av deler av utvalget. Utregningen av prosentene er altså ikke nødvendigvis basert på hele utvalget, men antallet i gruppen som besvarte spørsmålet.

Scenario. På spørsmålet «Hva tror du er mest sannsynlig at din kollega vil tenke og/eller gjøre?» svarte hele utvalget at Ola Normann ville sagt ifra til ansvarlig for IT-systemet (54,47%), diskutert det med en kollega (40,63%), si ifra til nærmeste leder (30,82%) og/eller ikke skjønne at det er et dataangrep (21,89%), se tabell 2. Som vist i figur 4 er det noen forskjeller i svarene til de med lederansvar og de uten. De med lederansvar tror i større grad at Ola Normann kommer til å si ifra til ansvarlig for IT-systemet (61,4%), i forhold til de uten (52,74%). De med lederansvar tror også han i større grad kommer til å si ifra til nærmeste leder (41,23%), i forhold til de uten (28,23%).

Figur 4

Hva tror du er mest sannsynlig at din kollega vil tenke og/eller gjøre?

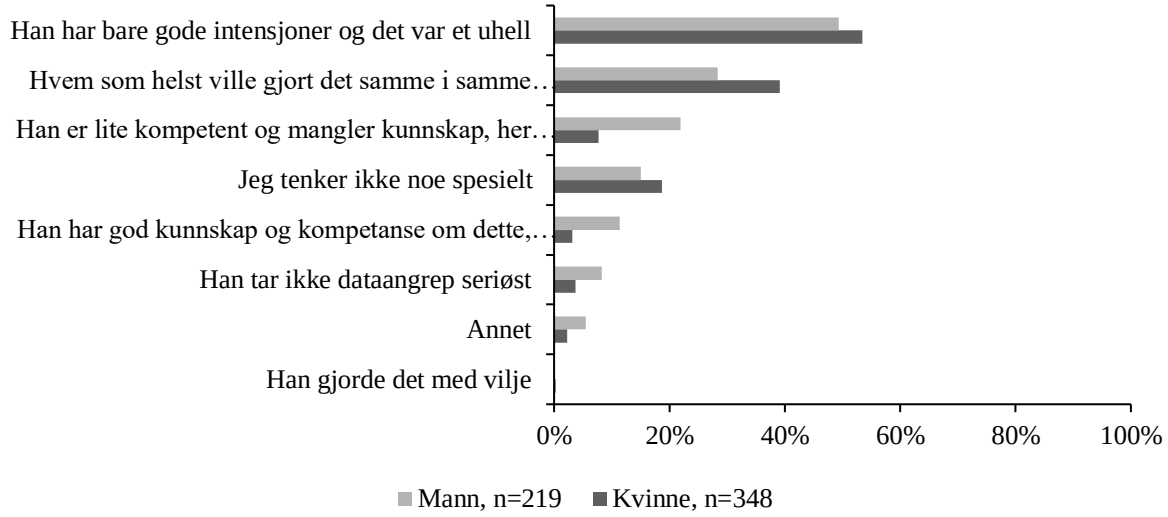


På spørsmålet om «Hva tenker du om din kollega som lastet ned dokumentet?», vist i tabell 3, svarte de fleste at «han hadde gode intensjoner og at det var et uhell» og at «hvem som helst ville gjort det samme i samme situasjon». Figur 5 viser at det var noe forskjeller mellom kvinner og menn på sistnevnte svaralternativ. 39,08% av kvinnene valgte dette alternativet,

mot 28,31% av mennene. 21,92% av menn svarte «Han er lite kompetent og mangler kunnskap, her burde han skjønt at det var et dataangrep», i motsetning til 7,76% av kvinner.

Figur 5

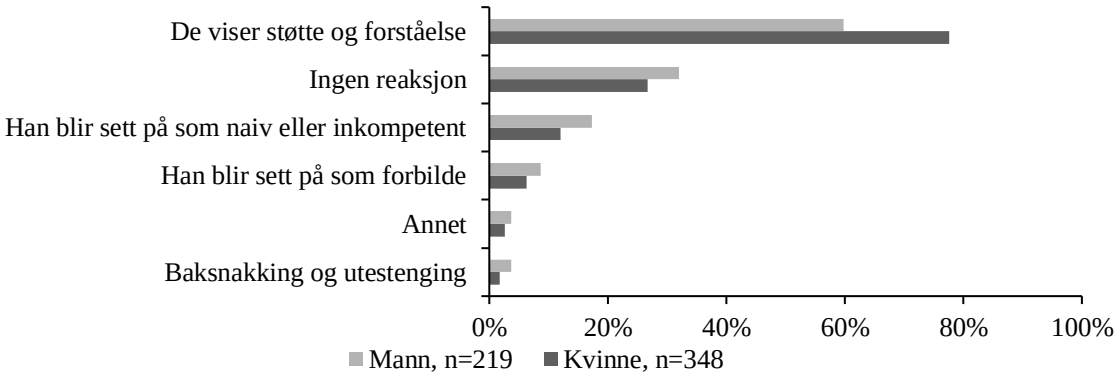
Hva tenker du om din kollega som lastet ned dokumentet?



Tabell 5 viser at de fleste svarte at Ola Normanns kolleger ville vise støtte og forståelse. Menn forventet dette i mindre grad (59,82%), enn kvinner (77,59%), se figur 6. Menn forventet alle de andre alternativene i noe større grad.

Figur 6

Hvilke reaksjoner får han fra andre kolleger?



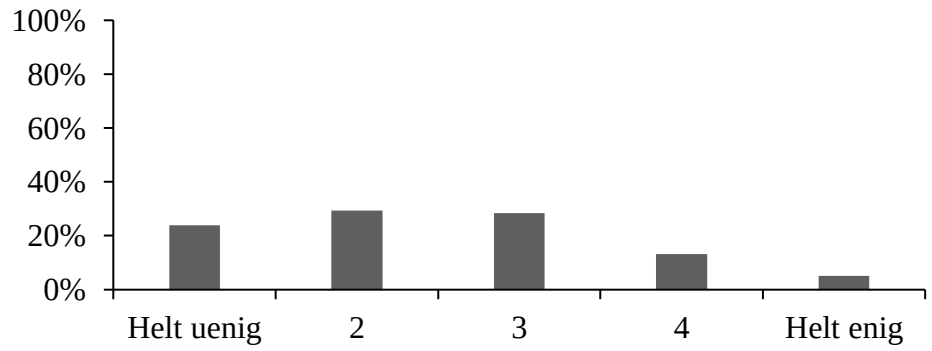
Kunnskap. De sammenlagte resultatene for denne delen av undersøkelsen er presentert i tabell 6. Flertallet (74,26%) sier at de vet hvordan de skal si ifra om de blir utsatt for et

dataangrep. Litt over halvparten (54,47%) svarer at deres arbeidsplass har et rapporteringssystem eller noen som er ansvarlig for å motta meldinger om dataangrep, og litt under halvparten (42,03%) svarer at de ikke vet dette.

Påstander. Deltakernes svar på påstandene om kunnskap er hovedsakelig konsentrert rundt den midterste verdien (se tabell 7), med unntak av påstandene presentert i figur 7 og 8.

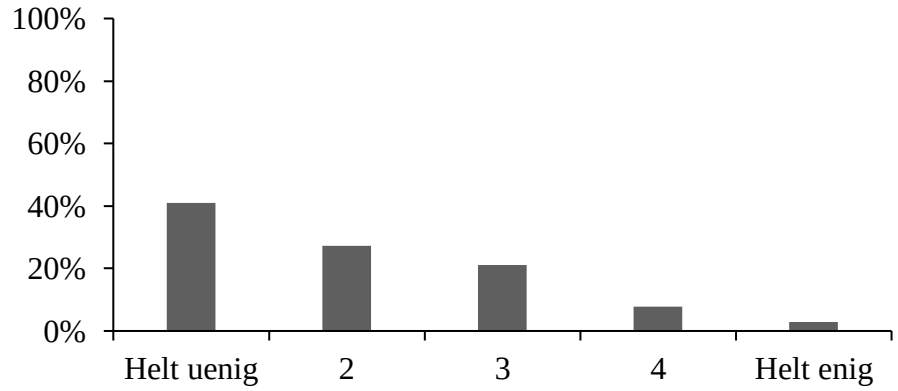
Figur 7

Vi mangler systemer og verktøy for å melde ifra om dataangrep



Figur 8

Det legges ikke vekt på datasikkerhet på min arbeidsplass



Hendelser. Resultatene for denne delen presenteres i tabell 8. Litt over halvparten svarte at de ikke visste om hendelsen ble rapportert til noen av alternativene som ble presentert, og halvparten svarte at hendelsen ble rapportert til administrator av det aktuelle tekniske systemet (se tabell 8). Som vist i Tabell 9 er det noen forskjeller på besvarelsene på dette spørsmålet. IT tror, i større grad enn alle andre gruppene, at dataangrep skjer daglig og

ukentlig, og svarer «vet ikke» mindre grad enn alle andre. Etter de som jobber innen IT-feltet, er det Kundeservice og HR som tror dataangrep skjer oftest.

Av alle deltakerne sier 34,85% at de selv har blitt utsatt for dataangrep, 47,64% at de ikke har det, og 17,51% vet ikke (tabell 8). Av de med lederansvar er det 44% som sier de har blitt utsatt for dataangrep, mot 33% av de som ikke har lederansvar.

For de forskjellige feltene er det kun IT og kundeservice hvor ingen svarte «vet ikke» på om de selv har blitt utsatt for dataangrep. Det var størst prosent som svarte «ja» på om de hadde blitt utsatt for dataangrep for de som jobber innen HR (50%), IT (44%), og ledelse/administrasjon og økonomi hvor begge hadde 39%. De fleste oppdaget selv at de var utsatt for dataangrep (84%), og/eller fikk melding fra IT-system (36%) og/eller at IT-avdelingen ga beskjed (31%).

Påstander. Resultatene fra påstandene er vist i tabell 10. Her ser man at svarene heller mot den ene siden på de fleste av påstandene. Deltakerne heller mot uenig i påstanden at det er umulig å vite hva man skal melde ifra om. De er også mer uenig enn enig i at de ikke kommer til å bli utsatt for dataangrep, de heller mot uenig i at rutiner for å melde ifra er tungvinte, og de er mer uenig enn enig i at deres kolleger ikke melder ifra om dataangrep. De fleste heller også mot at det å bli utsatt for dataangrep er uunngåelig, og det er en tydelig trend at de er uenige i at å melde ifra om dataangrep ikke kan påvirke utfallet av det.

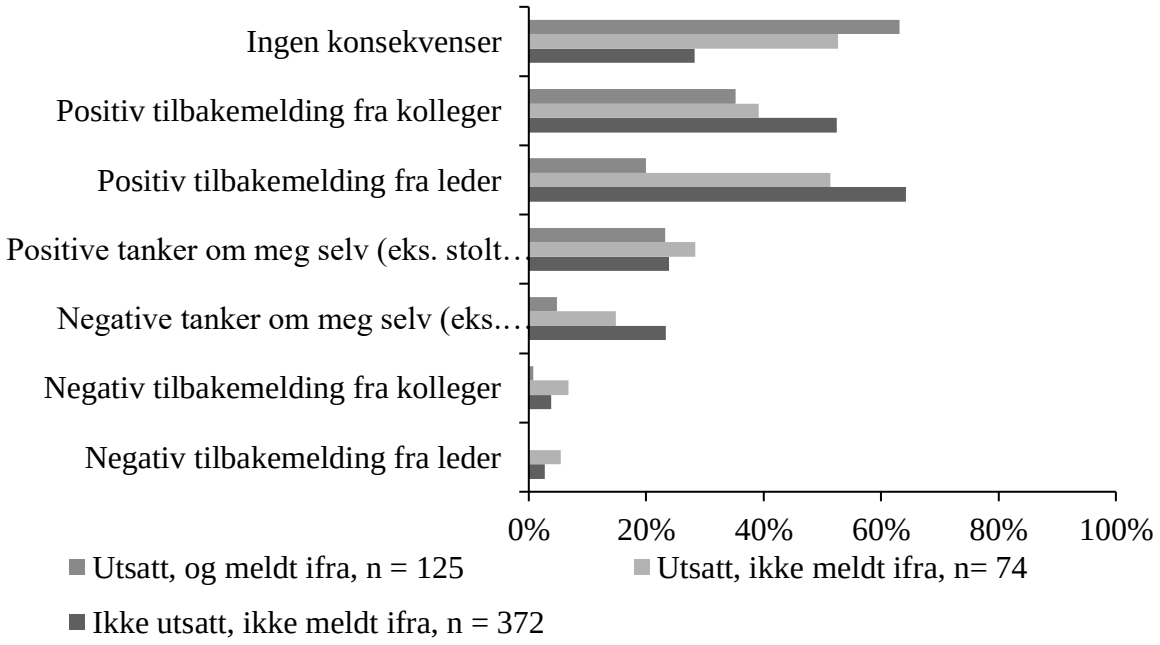
Konsekvenser. Tabell 11 viser resultatene for hele utvalget på spørsmålene om hvilke konsekvenser de opplevde eller forventet å oppleve etter å melde ifra om dataangrep. Av de som hadde opplevd dataangrep og meldt ifra svarte 63,20% at de ikke fikk noen konsekvenser, og hvis de fikk konsekvenser var det stort sett positive tilbakemeldinger fra kolleger, leder og positive tanker om seg selv.

De som hadde vært utsatt for dataangrep, men ikke meldt ifra svarte relativt likt. De forventet at de sannsynlige konsekvensene for å melde ifra om dataangrep ville være ingen konsekvenser, positiv tilbakemelding fra leder, kolleger og positive tanker om seg selv.

De som ikke hadde vært utsatt for dataangrep forventet i mindre grad ingen konsekvenser, og i mye større grad positive tilbakemeldinger fra leder og kolleger enn de som hadde blitt utsatt, og meldt ifra, faktisk opplevde. De forventet også i større grad negative tanker om seg selv, enn det de to andre gruppene forventet eller opplevde. Dette er illustrert i figur 9.

Figur 9

Opplevde og forventede konsekvenser av å melde ifra om dataangrep



Basert på forskjellene i besvarelsene på scenario mellom kjønn, ble det også undersøkt om menn og kvinner svarte forskjellig på spørsmål om opplevde eller forventede konsekvenser. Av de som har blitt utsatt og meldt ifra (menn *n*=54, kvinner *n*=70) opplevde 69% av mennene og 59% av kvinnene ingen konsekvenser. Kvinner opplevde i noe større grad positive tilbakemeldinger fra kolleger (37% vs. 33% av menn), og positive tilbakemeldinger fra leder (23% vs. 17%).

Av de som har blitt utsatt for dataangrep (menn *n*=28, kvinner *n*=45), men ikke meldt ifra, er cirka like stor andel av kvinnene (56%) som forventer ingen konsekvenser, som de som meldte ifra. Det er en mindre andel av mennene (46%) som forventer ingen konsekvenser, enn de som faktisk opplevde ingen konsekvenser (69%). Av de som ble utsatt, og ikke meldte ifra er det en større andel mennene som forventer å ha positive tanker om seg selv (39%), imot 22% av kvinnene.

For gruppen som ikke hadde blitt utsatt for dataangrep, og dermed ikke meldt ifra, var det ingen nevneverdige forskjeller mellom kjønnene. Denne gruppen er som helhet relativt forskjellig fra de to andre, som vist i figur 9.

En trend i hele utvalget er at forventninger om negative tanker om seg selv er høyest hos de som ikke har opplevd dataangrep, lavere hos de som har opplevd det, men ikke meldt ifra, og lavest hos de som har opplevd det og i tillegg meldt ifra.

Både de som har vært utsatt for dataangrep, men ikke meldt ifra, og de som ikke har blitt utsatt eller meldt ifra forventer i stor grad positiv tilbakemelding fra leder om de skulle melde ifra om dataangrep. Av de som faktisk har meldt ifra var det kun 20% som opplevde dette.

Påstander. Tabell 12 viser resultatene for hele utvalget på påstandene om konsekvenser. Her er det en tydelig overvekt av deltakere som sier at de er helt uenig i at det er flaut å bli utsatt for dataangrep, og at er uenige i at de vil få negative tilbakemeldinger for at dataangrepet skjedde om de melder ifra. Besvarelsene heller mot enig på påstandene om at man oppmuntres til å melde ifra om dataangrep, og at man blir godt ivaretatt av sine kolleger om det skulle skje.

Hjemmekontor. Av deltakerne i undersøkelsen har 523 personer hatt hjemmekontor i 2020, dette tilsvarer 91,59% av utvalget. I gjennomsnitt hadde disse 3,93 arbeidsdager på

hjemmekontor per uke. Tabell 13 viser svarene til hele utvalget på spørsmålene om hjemmekontor.

Påstander. Resultatene på påstandene er presentert i tabell 14. På påstanden om at hjemmekontor er like trygt som den ordinære arbeidsplassen heller flere mot enig. De fleste er uenig i at de ikke har det tekniske utstyret til å ivareta informasjonssikkerheten på hjemmekontor, og de fleste er uenig i at sannsynligheten for å bli utsatt for dataangrep er mindre på hjemmekontor enn ordinært kontor.

«Annet» kategorien. På de fleste spørsmålene ligger svarprosenten på dette alternativet på 3-6%. Det var særlig tre av spørsmålene hvor mange av deltakerne svarte «Annet». Svarene deres ble gått gjennom og sortert i tema som presenteres under.

Scenario. På spørsmålet «Hvilke konsekvenser tror du det fikk for ham å melde ifra til leder?» svarte 6,38% (*N*=571) «Annet». Svarene fordelte seg på tre tema: «vet ikke», «kommer an på hvem, situasjon, relasjoner, opplæring og mer» og «ikke alvorlige konsekvenser, litt irritasjon, medfølelse, sympati, noe å lære av».

Hendelser. På spørsmålet «Hvorfor var det ikke aktuelt å melde ifra?» svarte 37% (*n*=74) «Annet». Alle svarene handlet om phishing-epost, og fordelte seg på tre tema: de som skjønte at det var phishing-epost og slettet den, de som allerede hadde fått beskjed om dataangrepet eller at det allerede var meldt inn, og de som sier det skjer så ofte at de ikke tenker over det eller har tid til å melde inn alle e-postene.

Diskusjonsdel

Bakgrunn for valg av datainnsamlingsmetode. Det er flere argumenter for valg av spørreundersøkelse som datainnsamlingsmetode. Det første er at det ikke ville vært mulig å observere personer på jobb, både på grunn av pandemi og hjemmekontor, men også fordi det ville vært krevende og upraktisk å gjennomføre. Man vet ikke når en relevant hendelse vil oppstå, og kan ikke følge etter folk hele dagen. Det andre argumentet er at målet med

oppgaven er å utforske betingelser for melding av dataangrep. Et så stort og komplekst tema vil ikke kunne undersøkes eksperimentelt på organisasjonsnivå i et prosjekt som dette, men fortolking av dataene kan likevel gi et godt bilde på tilstanden i virksomhetene (Palmer, 1991). Et tredje argument, som også Guerin (2019) poengterer, er at man ikke kan observere hva andre tenker om sine kolleger, eller om de kjenner til regler og policy. Dette er informasjon man uansett ville vært nødt til å spørre dem om, og som er relevant for informasjonssikkerhetskultur. Spørreskjema ble vurdert som en effektiv og økonomisk måte å samle inn data på, innenfor tidsbegrensningene, og en datainnsamlingsmetode som ville gi et godt datagrunnlag for å besvare problemstillingen i oppgaven.

Utvalget. Det er store forskjeller størrelsen på virksomhetene, og derfor antall deltakere fra hver virksomhet. Det er også store forskjeller i antall deltakere fra hvert felt. De fleste jobber ved Universitet, og jobber innenfor forskning og undervisning. Det er en overvekt av kvinner i utvalget, og de fleste deltakerne har ikke lederansvar. Det er ikke mulig å generalisere funnene utover virksomhetene som har deltatt. Forskjeller mellom grupper av svært ulik størrelse bør tolkes forsiktig.

Kjønnsforskjeller. Det var noen forskjeller på hvordan menn og kvinner svarte på enkelte av spørsmålene. Dette har ikke blitt undersøkt med eksperimentelt design, og er derfor ikke mulig å si at forskjellene er på grunn av kjønn. Det kan være mange faktorer som påvirker resultatene, for eksempel hvilken virksomhet og hvilket felt deltakerne jobber innen.
Menn ser ut til å tenke litt mer negativt, og mindre positivt om Ola Normann etter han klikket på lenken i scenario. Menn svarer også at de i mindre grad opplever positive konsekvenser av å melde ifra om dataangrep enn kvinner, men de forventer i større grad enn kvinner å ha positive tanker om seg selv etter å si ifra.

Forskjeller knyttet til lederansvar. De med og uten lederansvar svarer forskjellig på hva de tror det er mest sannsynlig at Ola Normann kommer til å gjøre etter å ha klikket på linken i

phishing-eposten. De med lederansvar tror i større grad at han kommer til å si ifra til ansvarlig for IT-systemet eller nærmeste leder. Ledere oppgir i større grad at de har blitt utsatt for dataangrep enn de uten lederansvar. Om de faktisk er mer utsatt, eller har andre forutsetninger til å oppdage dette er uvisst.

Kunnskap, foranledning til atferd. Flertallet svarer at de vet hvordan de skal si ifra om dataangrep, men det er likevel stort forbedringspotensial på dette området. Mange har ikke deltatt på opplæring i informasjonssikkerhet, vet ikke om det gjennomføres, eller sier at det ikke gjennomføres på deres arbeidsplass. Faktorer som kan være med å påvirke dette er eventuelt nyansatte som enda ikke har kommet i gang med opplæring, hvis det for eksempel kun gjennomføres en gang i året. Ansatte som ikke har opplæring, ikke læringshistorie med S^D eller kunnskap til å improvisere korrekt atferd i nye situasjoner, vil velge det som er mest sannsynlig basert på forsterkningsbetingelsene (Daniels & Bailey, 2014; Reason, 1997). Samtidig er de fleste uenige i at informasjonssikkerhet ikke blir vektlagt på deres arbeidsplass.

Det kan diskuteres i hvilken grad man kan forvente at alle ansatte skal ha kjennskap til rutiner, hendelseshåndteringsplaner, standarder, forskrifter og lovverk, da dette mest sannsynlig ikke er hovedfokus for deres stilling. Desto viktigere er det at de som har informasjonssikkerhet som sin arbeidsoppgave kommuniserer og samarbeider godt med ansatte på alle nivåer i virksomheten, for å finne en måte for å integrere informasjonssikkerhet i deres arbeidshverdag (Ashenden, 2008; Kraemer & Carayon, 2007).

Hendelser, atferd. Litt over halvparten sier deres virksomhet har blitt utsatt for dataangrep, og av de som sier ja, er det litt over halvparten som ikke vet om det ble rapportert til noen av alternativene som ble oppgitt. Samtidig er dette kanskje ikke noe som kan forventes av ansatte som ikke jobber spesifikt med informasjonssikkerhet (Ahmad et al., 2019; Kajtazi et al., 2018; Post & Kagan, 2007).

Flertallet av de som ikke meldte ifra om at de hadde blitt utsatt for dataangrep, oppgir at dette var fordi hendelsen ble meldt inn automatisk, men mange svarte også at de bare slettet mailen fordi de skjønte at det var en phishing-epost. Her er går man glipp av muligheten til å bygge opp en informert kultur (Reason, 1997). Dette kan også ses i sammenheng med kunnskapen de ansatte har om dataangrep, da høy grad av automatikk kan føre til at de ikke kommer i kontakt med kontingensene, og stimuluskontrollen svekkes (Palmer, 1991).

Det er ikke alltid IT fanger opp phishing-eposter, og hvis en ansatt har mottatt den er det sannsynlig at flere har det. Om man melder den inn kan man håndtere hendelsen, og rekke å varsle andre som kanskje ikke skjønner at det er et dataangrep. Det samme gjelder på virksomhetsnivå, om varsling til Politiet og andre institusjoner (Næringslivets Sikkerhetsråd, 2020).

På spørsmålene om ofte dataangrep skjer, svarte svært mange vet ikke. Spørsmålene hadde forklaringsteksten «For eksempel phishing-epost, løsepengevirus og bedrageri. Både vellykkede og mislykkede angrep regnes med». Med tanke på hvor ofte dette omtales i media, i tillegg til at de oppgir at det vektlegges av arbeidsplassen deres, kunne man forventet at flere ga et estimat på hvor ofte dette skjedde.

Konsekvenser, forsterkningsbetingelser. Basert på litteraturen om regelfølging, kunne man forventet at deltakerne forventet negative reaksjoner fra leder eller kolleger av å ikke følge reglene (å ikke melde ifra) (D'Arcy & Herath, 2011; Herath & Rao, 2009; Padayachee, 2012). Svært få av deltakerne forventet eller opplevde negative konsekvenser ved å melde ifra om dataangrep. Likevel svarte nesten alle av de som ikke hadde blitt utsatt for dataangrep sier også at de ville meldt ifra om det var aktuelt. Det betyr ikke at de faktisk ville gjort det, men det gir en god indikator.

Det mest interessante funnet er forskjellene mellom opplevde og forventede konsekvenser (figur 9). For selv om man i stor grad har unngått negative reaksjoner, har

flertallet opplevd «ingen konsekvenser» av å melde ifra om dataangrep. De som ikke har meldt ifra, og særlig de som ikke har opplevd dataangrep, forventer i mye større grad positive tilbakemeldinger fra leder og kolleger. Sett i sammenheng med at de med lederansvar i større grad forventer at Ola Normann vil si ifra til nærmeste leder, er det interessant at mange færre opplever positive tilbakemeldinger fra leder enn de som forventer det. Fra et atferdsanalytisk perspektiv er denne atferden på et så tynt forsterkningsskjema at det vil bety ekstinksjon (Catania, 2013).

Hjemmekontor. Færre deltakere oppgir å ha blitt utsatt for dataangrep på hjemmekontor enn på ordinært kontor. Det kan være påvirket av at de fleste kun har hatt hjemmekontor det siste året. I motsetning til mørketallsrapporten, hvor ansatte innenfor utdanning rapporterte svekket sikkerhet, oppgir deltakerne at de ikke opplever noen forskjeller fra ordinært kontor. Selv om miljøet og kontingensene for å varsle kan være endret, oppgir deltakerne ingen endringer i vanskelighetsgraden av å si ifra om dataangrep.

Konklusjon fra spørreundersøkelsen

Resultatene viser at deltakerne stort sett har god kunnskap om hva et dataangrep er, de ønsker å melde ifra om de blir utsatt, de som har blitt utsatt melder ifra når det ikke varsles automatisk. De fleste vet det er viktig, de er enige i at det blir vektlagt på deres arbeidsplass, de forventer ingen negative konsekvenser av å varsle, tenker positivt om andre som blir utsatt og de tenker at det er veldig vanlig.

Når det gjelder konsekvenser av melding av dataangrep finnes et stort forbedringspotensiale. Om målet er å øke regelfølging, er det positivt at deltakerne ikke opplever eller forventer negative reaksjoner fra kolleger eller leder. De fleste sikkerhetshendelser skjer som følge av uhell og tilfeldigheter (Næringslivets Sikkerhetsråd, 2020). Tiltak som straffer ansatte for hendelser, kan bidra til en urettferdig kultur, som igjen påvirker rapporteringskulturen negativt (Reason, 1997). Men som figur 9 viser, forventer

ansatte i stor grad positive reaksjoner, som ikke blir formidlet i like stor grad. Med en atferdsanalytisk tilnærming, og systematisk formidling av forsterkning, er det mulig for virksomheter å skape en enda bedre sikkerhetskultur (Daniels & Bailey, 2014; Reason, 1997).

Tiltak. Det man ønsker er en endring i atferd, og i denne undersøkelsen har deltakerne blitt spurt om faktisk atferd, både tanker og handlinger. Dette gjør det mulig å danne et bilde av hvilke variabler man har å jobbe med, og hvilke områder som kan ha nytte av tiltak.

For å bidra til å opprettholde ønsket atferd kan man iverksette regelstyring i begge ender, både for de som melder ifra om dataangrep, og de som mottar meldingen. Atferd forekommer innenfor en kjede av kontingenser (Daniels & Bailey, 2014).

Hvis verken regelbryting straffes eller regelfølging forsterkes velger folk gjerne den letteste løsningen på problemet (Reason, 1997). Undersøkelsen viser tydelig at få opplever noen som helst konsekvenser av å melde ifra om dataangrep, og det er dermed å forvente at folk velger den letteste løsningen, som kan være å bare slette en phishing-epost.

Performance management.

***PIC/NIC Analyse*®.** Dette er en måte å undersøke foranledning og konsekvenser for en bestemt atferd (Daniels & Bailey, 2014). Foranledning, slik ordet brukes her, refererer til stimuli som fremkaller atferd på grunn av en spesifikk læringshistorie, ikke MO. Dette er en måte å organisere, og få oversikt over betingelsene for atferden, som bidrar til en bedre forståelse av atferden fra perspektivet til den som utførte atferden. Når man gjør en PIC/NIC Analyse® vurderer man om konsekvensene er positive (P), negative (N), umiddelbare (I), fremtidige (F), sikre (C) eller usikre (U). De konsekvensene som har størst atferdsendrende effekt kan være både positive eller negative, så lenge de er umiddelbare og sikre, derav PIC og NIC (Daniels & Bailey, 2014). En positiv konsekvens, slik som god helse, er relativt sikker og kommer lengere frem i tid, og har mindre effekt på en atferd enn de positive, umiddelbare og sikre konsekvensene av å spise en sjokolade.

Om man skal endre konsekvensene for en atferd, er det nødvendig å definere hvilken spesifikk atferd man vil undersøke kontingensene for (Daniels & Bailey, 2014). Her er det særlig viktig at man bruker et presist språk, og ikke slår sammen alle atferdene til kun regelfølging (Blythe, 2013).

Daniels og Bailey (2014) understreker at det folk gjør, gir mening for dem akkurat i det øyeblikket. Og det er betingelsene for atferd i dette øyeblikket, deres atferd må bedømmes ut ifra. For eksempel er det å melde ifra om en phishing-epost til IT-avdelingen, ved å videresende den til dem, en bestemt atferd. Som denne undersøkelsen har vist hender det at folk ofte gjør noe annet. Hvis forsterkningsbetingelsene for å følge prosedyren for en slik hendelse ikke er på plass, er det usannsynlig at personen vil utføre denne atferden (Daniels & Bailey, 2014).

En virksomhet som ønsker å forbedre informasjonssikkerhetskulturen sin, ser ofte på resultater over hvor mange phishing-eposter som mottas, hvor mange som oppdages, hvor ofte ansatte bytter passord eller oppdaterer programvare. Disse resultatene er direkte produkter av atferd (Daniels & Bailey, 2014). Å forsøke å forklare hvilke faktorer som påvirker intensjon om å følge regler blir unødvendig, og skaper også en virkelighetsfordobling (Ree, 2013).

Videre diskusjon

Menneskers rolle i informasjonssikkerhet. Hvilken atferd som forekommer, er avhengig av miljøet som selekterer (Ree, 2013; Skinner, 1981). Det som selekteres for, altså forsterkes, er det som blir videreført i fremtiden. Når forsterkningsbetingelsene ikke er i samsvar med reglene for informasjonssikkerhet, får man uoverensstemmelse mellom hva ansatte gjør og det reglene sier, selv om de er klar over hva reglene sier. Når man snakker om menneskelige svakheter og menneskelige feil, er dette definert ut i fra hva reglene sier er riktig, fordi ut i fra forsterkningsbetingelsene er det logisk (Daniels & Bailey, 2014).

I tillegg er det ofte få eller ingen personer som er ansatt i virksomhetene som har som hovedoppgave å jobbe med informasjonssikkerhet, og for andre kan det oppleves som en tilleggsoppgave de må gjøre (Ahmad et al., 2019; Kajtazi et al., 2018; Post & Kagan, 2007). Fra perspektivet til de som jobber med sikkerhet, er menneskelig variasjon en motkraft mot deres oppdrag (Daniels & Bailey, 2014). Fra andres perspektiv er sikker atferd noe nytt de må lære seg, som krever ressurser, og er på siden av deres oppdrag. Når det å utføre jobben sin går på bekostning av ISP regelfølging, bør man undersøke hvilke innvirkninger systemet har (Kajtazi et al., 2018). Dette kan også kobles til uoverensstemmelse mellom antakelsene i forskjellige subkulturer, for eksempel mellom ledelse, IT-avdeling og resten av virksomheten (Sarkar et al., 2020; Schein, 1990). Samtidig er det ofte IT som har ansvar for opplæring av andre ansatte, selv om de sjelden har kompetanse til å jobbe med mennesker på denne måten (Ashenden, 2008; Kraemer & Carayon, 2007).

Validitet og reliabilitet. Å besvare en undersøkelse som dette er atferd i seg selv, og hva deltakerne oppgir at de gjør eller vet på spørsmålene er valide data innenfor disse rammene. Det kan likevel ikke forveksles med hva de ville gjort i en reell situasjon, som er en annen (men ikke urelatert) atferd. På den andre siden kan man argumentere for at det vil være en viss grad av korrelasjon mellom det respondentene oppgir at de ville gjort, og det de faktisk hadde gjort i en lignende situasjon (Palmer, 1991).

Som nevnt kan ikke resultatene generaliseres utover utvalget, da det ikke ble gjort et randomisert utvalg. Resultatene har der for ikke ekstern validitet (Shadish et al., 2002). Fordi det ikke har blitt gjort noen slutninger om årsak-virkning i denne undersøkelsen, har den høy grad av intern validitet. Det er ikke forsøkt å undersøke noen funksjonelle relasjoner, men kun kartlegge betingelsene for melding av dataangrep i disse virksomhetene på tidspunktet de svarte. Undersøkelsen har også høy grad av overflatevaliditet, da spørsmålene har konkrete spørsmål om kunnskap, hendelser og konsekvenser, ikke konstrukter.

Svakheter ved undersøkelsen. Det ble forsøkt å avdekke de fleste svakhetene ved undersøkelsen før utsending, da det ikke var ønskelig å gjøre endringer i etterkant. En av tilbakemeldingene fra pilottestingen var at spørreundersøkelsen var for lang. Det ble gjort endringer for å forsøke å korte den ned, men noen av deltakerne kommenterte at den likevel var for lang. Dette kan også være grunnen til at det var en del flere som svarte på samtykkeskjema enn de som svarte på selve undersøkelsen.

Det var noen av påstandene som var logisk tvetydige, dette ble ikke fanget opp før undesøkelsen ble sendt ut. Noen deltakere sende også e-post til kontaktperson om at noen av spørsmålene ikke hadde svaralternativ som var dekkende nok. Med så mange respondenter vil det alltids være noen som ikke er tilfreds med spørsmålene som stilles eller tilgjengelige svaralternativ.

Ettersom det var en overvekt av kvinner i utvalget, ville et scenario med Kari Normann i stedet for Ola muligens ha gjort scenarioet mer gjenkjennelig. Det var ikke mulig å vite kjønnsfordelingen på forhånd, og det trenger ikke bety at alle som mottok invitasjon om deltakelse hadde samme kjønnsfordeling som de som svarte.

Etter utsendelsen fikk vi tilbakemelding fra Kraftverket om at spørreundersøkelsen ikke ville la seg gjennomføre der fordi språket ikke var tilpasset godt nok deres ansatte. Den ble derfor ikke distribuert i denne virksomheten, som er grunnen til at kun én person fra virksomheten har svart.

Etisk vurdering av prosjektet

Studien er gjennomført som en spørreundersøkelse der det er sikret anonymitet for deltakerne. Ingen av spørsmålene kan oppfattes som kontroversielle, støtende, inngripende eller sensitive. Det er ikke blitt gjennomført noe tiltak eller inngripen i deltakernes liv, eller andre ting som kan påvirke deres hverdag. Deltakelse i undersøkelsen er fullstendig frivillig, og deltakerne er

informert om at de har mulighet til å trekke samtykke til deltakelse og få slettet sin besvarelse om de ønsker det.

Risiko og sårbarhetsanalyse. Det ble gjennomført en risiko og sårbarhetsanalyse for prosjektet i samarbeid med veileder. Her ble det ikke funnet noen risiko som krevde tiltak. Det ble ikke samlet inn sensitive opplysninger. Deltakerne ble spurt om bakgrunnsinformasjon, som kan bli brukt til å identifisere individer. Ingen av de deltakende virksomhetene blir nevnt med navn. Deltakerne ble kun bedt om å oppgi e-postadresse, slik at deres besvarelse kunne slettes om ønskelig.

Prosjektet hadde behandlingsgrunnlag for data gjennom informert samtykke for alle deltakere. Deltakernes besvarelser ble lagret kryptert i lagringstjenestene til Nettskjema (UiO), og i OsloMet OneDrive, og ikke på noen private enheter. Nettskjemaløsningen har godkjennelse til å håndtere data fra og med grønn til svart kategori. Prosjektet ble meldt inn og godkjent av NSD (meldeskjema nr. 673307, vedlegg C).

Avslutning

Videre forskning. Det er mange muligheter for videre forskning innen dette feltet, særlig med utgangspunkt i atferdsanalyse. En mulighet er å undersøke kontingensene for ISP regelfølging i virksomheter gjennom eksperimentelle design. Her er det mulig å undersøke funksjonelle relasjoner, ved å manipulere uavhengige variabler i miljøet, gjerne også på tvers av avdelinger, for å se på hvilke tiltak som har best effekt.

Tverrfaglighet. Informasjonssikkerhetsfeltet har stort behov for mer kunnskap om menneskelig atferd, her kan man utnytte eksisterende ressurser innen atferdsvitenskap. Dette bidrar også til en mer helhetlig tilnærming til informasjonssikkerhet, fordi det er ikke bare et teknisk problem, men involverer alle aspekter ved en virksomhet.

Atferdsvitenskapens bidrag. Noe som blir svært vektlagt innenfor atferdsvitenskap er at vitenskapen skal være betydningsfull for de som er målet for tiltakene.

Ved å basere tiltak på atferdsvitenskapelige prinsipper, sikrer man et universelt utgangspunkt for atferdsendring, og man unngår å jobbe ut ifra utallige forskjellige modeller for intensjon om atferd.

Referanser

Ahmad, Z., Ong, T. S., Liew, T. H. & Norhashim, M. (2019). Security monitoring and information security assurance behaviour among employees An empirical analysis. *Information and Computer Security, 27*(2), 165-188. https://doi.org/10.1108/ics-10-2017-0073

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

American Psychological Association. (2020). *Publication manual of the American Psychological Association* (7. utg.). https://doi.org/10.1037/0000165-000

Angner, E. (2016). *A course in behavioral economics* (2. utg.). Palgrave Macmillan.

Ashenden, D. (2008). Information security management: A human challenge? *Information Security Technical Report, 13*(4), 195-201. https://doi.org/https://doi.org/10.1016/j.istr.2008.10.006

Aurigemma, S. & Mattson, T. (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information and Computer Security, 25*(4), 421-436. https://doi.org/10.1108/ics-11-2016-0089

Axelrod, R. & Cohen, M. D. (2000). *Harnessing complexity. Organizational implications of a scientific frontier*. Basic Books.

Azrin, N. H. & Holz, W. C. (1966). Punishment. *Operant behavior: Areas of research and application*, 380-447.

Blythe, J. M. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. *Proceedings of CHItaly 2013 Doctoral Consortium, 1065*, 92-101.

Catania, A. C. (2013). *Learning* (5. utg.). Sloan Publishing.

Cooper, J. O., Heron, T. E. & Heward, W. L. (2014). *Applied behavior analysis* (2. utg.). Pearson.

D'Arcy, J. & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20*, 643-658. https://doi.org/https://doi.org/10.1057/ejis.2011.23

da Veiga, A. & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*, 162-176. https://doi.org/10.1016/j.cose.2014.12.006

da Veiga, A. & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security, 70*, 72-94. https://doi.org/10.1016/j.cose.2017.05.002

Daniels, A. C. & Bailey, J. S. (2014). *Performance management: Changing behavior that drives organizational effectiveness* (5. utg.). Performance management publications.

Datatilsynet. (2021a). *Personvernprinsippene*. Datatilsynet. Hentet 13.06 fra https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/

Datatilsynet. (2021b). *Virksomhetens plikter*. Datatilsynet. Hentet 13.06 fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

Green, L. & Myerson, J. (2004). A discounting framework for choice with delayed and probabilistic rewards. *Psychological Bulletin, 130*(5). https://doi.org/10.1037/0033-2909.130.5.769

Guerin, B. (2019). The use of participatory and non-experimental research methods in behavior analysis. *Perspectivas em Análise do Comportamento, 9*(2), 248-264. https://doi.org/https://doi.org/10.18761/PAC.2018.n2.09

Gundersen, M. (2020, 20.10). Tar i snitt over 200 dager å oppdage et datainnbrudd. *NRKbeta*. https://nrkbeta.no/2020/09/10/tar-i-snitt-over-200-dager-a-oppdage-et-datainnbrudd/

Hayes, S. C. & Brownstein, A. J. (1986). Mentalisn, behavior-behavior relations, and a behavior analytic view of the purposes of science. *The Behavior Analyst, 9*(2). https://doi.org/10.1007/BF03391944

Herath, T. & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

Kajtazi, M., Cavusoglu, H., Benbasat, I. & Haftor, D. (2018). Escalation of commitment as an antecedent to noncompliance with information security policy. *Information and Computer Security, 26*(2), 171-193. https://doi.org/10.1108/ics-09-2017-0066

Kraemer, S. & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics, 38*(2), 143-154. https://doi.org/https://doi.org/10.1016/j.apergo.2006.03.010

Larsen, T. & Røyrvik, E. A. (Red.). (2017). *Trangen til å telle. Objektivering, måling og standardisering som samfunnspraksis*. Spartacus Forlag AS.

Malott, R. W. (1989). The achievement of evasive goals: Control by rules describing contingencies that are not direct acting. I S. C. Hayes (Red.), *Rule-governed behavior: Cognition, contingencies, and instructional control* (s. 269-322). Plenum.

Nasjonal Sikkerhetsmyndighet. (2020). *Risiko 2020*. Nasjonal Sikkerhetsmyndighet. https://nsm.no/aktuelt/risiko-2020

NorSIS. (2015). *Kommune CERT - utredning av behov og muligheter*. https://norsis.no/d18ba623c92d1ded748a61ae70/KommuneCSIRT_print.pdf

NorSIS. (2021). *Trusler og trender 2021*. https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf

Næringslivets Sikkerhetsråd. (2020). *Mørketallsundersøkelsen*. https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, *31*(5), 673-680. https://doi.org/https://doi.org/10.1016/j.cose.2012.04.004

Palmer, D. C. (1991). A behavioral interpretation of memory. I L. J. Hayes & P. N. Chase (Red.), *Dialogues on verbal behavior* (s. 261-279).

Pay, H. B. (2021). *Økt digitalisering i offentlig sektor som følge av koronapandemien* (Bruk av IKT i offentlig sektor). Statistisk Sentralbyrå. https://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/okt-digitalisering-i-offentlig-sektor-som-folge-av-koronapandemien

Personopplysningsloven. (2018). Lov om behandling av personopplysninger (LOV-2018-06-15-38) (5). https://lovdata.no/lov/2018-06-15-38/gdpr/a5

Pierce, W. D. & Cheney, C. D. (2017). *Behavior analysis and learning: A biobehavioral approach* (6. utg.). Routledge.

Post, G. V. & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, *26*(3). https://doi.org/https://doi.org/10.1016/j.cose.2006.10.004

Reason, J. (1997). *Managing the risks of organizational accidents*.

Reason, J. (1998). Achieving a safe culture: Theory and practice. *Work & Stress*, *12*(3), 293-306. https://doi.org/https://doi.org/10.1080/02678379808256868

Reason, J. (2000). Safety paradoxes and safety culture. *Injury Control & Safety Promotion*, *7*(1), 3-14. https://doi.org/https://doi.org/10.1076/1566-0974(200003)7:1;1-V;FT003

Ree, G. (2013). En enhetlig forklaringsmodell. Innledning til Donahoe (2003) Selectionism. *Norsk Tidsskrift for Atferdsanalyse*, *40*(1), 87-99.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

Ross, L. (1977). The intuitive psychologist and his shortcomings: Distortions in the attribution process. *Advances in Experimental Social Psychology*, *10*, 173-220. https://doi.org/https://doi.org/10.1016/S0065-2601(08)60357-3

Sandaker, I. (2009). A selectionist perspective on systemic and behavioral change in organizations. *Journal of organizational behavior management*, *29*(3-4), 276-293. https://doi.org/10.1080/01608060903092128

Sarkar, S., Vance, A., Ramesh, B., Demestihas, M. & Wu, D. T. (2020). The Influence of Professional Subculture on Information Security Policy Violations: A Field Study in a Healthcare Context. *Information Systems Research, 31*(4), 1240-1259. https://doi.org/10.1287/isre.2020.0941

Schein, E. H. (1990). Organizational Culture. *American Psychologist*(2), 109-119. https://doi.org/10.1037/0003-066X.45.2.109

Schlinger, H. & Blakely, E. (1987). Function-altering effects of contingency-specifying stimuli. *The Behavior Analyst, 10*, 41-45. https://doi.org/https://doi.org/10.1007/BF03392405

Shadish, W. R., Cook, T. D. & Campbell, D. T. (2002). *Experimental and quasi-experimental designs for generalized causal inference*. Houghton Mifflin.

Skinner, B. F. (1966). An operant analysis of problem solving. I B. Kleinmuntz (Red.), *Problem solving: research, method and theory*.

Skinner, B. F. (1981). Selection by consequences. *Science, 213*(4507), 501-504. https://doi.org/10.1126/science.7244649

Sommestad, T., Hallberg, J., Lundholm, K. & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*.

Statistisk sentralbyrå. (2021). *10859: IKT-sikkerhetsproblemer i statlige virksomheter (prosent), etter statistikkvariabel, status for sikkerhetsproblemet og år*. Statistisk sentralbyrå. Hentet 15.04 fra https://www.ssb.no/statbank/table/10859/

Workman, M., Bommer, W. H. & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816. https://doi.org/https://doi.org/10.1016/j.chb.2008.04.005

Xue, Y., Liang, H. & Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research, 22*(2), 400-414. https://doi.org/10.1287/isre.1090.0266

Zohar, D. & Erev, I. (2007). On the difficulty of promoting workers' safety behaviour: Overcoming the underweighting of routine risks. *International Journal of Risk Assessment and Management, 7*(2), 122–136. https://doi.org/https://doi.org/10.1504/IJRAM.2007.011726

Tabeller

Scenario

Tabell 2

Hva tror du er mest sannsynlig at din kollega vil tenke og/eller gjøre?

	n	%
Sier ifra til ansvarlig for IT-systemet (e-post/Office)	311	54,47 %
Diskuterer det med en kollega	232	40,63 %
Han sier ifra til nærmeste leder	176	30,82 %
Han skjønner ikke at det er et dataangrep	125	21,89 %
Bytter passord og brukernavn	83	14,54 %
Gjør ingenting, hvis det er dataangrep sier IT ifra	72	12,61 %
Han synes det er flaut/ubehagelig å si ifra	61	10,68 %
Han melder inn hendelsen i rapporteringssystem	58	10,16 %
Sletter filen og restarter datamaskinen	55	9,63 %
Gjør ingenting, dette er ikke dataangrep	35	6,13 %
Ingenting, sier ikke ifra til noen	33	5,78 %
Annet	18	3,15 %
Han er redd for negative konsekvenser fra andre ved å si ifra	15	2,63 %
Tenker at skaden er skjedd og det hjelper ikke å melde ifra	8	1,40 %

N = 571

Tabell 3

Hva tenker du om din kollega som lastet ned dokumentet?

	n	%
Han har bare gode intensjoner og det var et uhell	298	57,64 %
Hvem som helst ville gjort det samme i samme situasjon	198	38,30 %
Jeg tenker ikke noe spesielt	99	19,15 %
Han er lite kompetent og mangler kunnskap, her burde han skjønt at det var et dataangrep	76	14,70 %
Han har god kunnskap og kompetanse om dette, og det er mest sannsynlig ikke er et dataangrep	36	6,96 %
Han tar ikke dataangrep seriøst	32	6,19 %
Annet	20	3,87 %
Han gjorde det med vilje	1	0,19 %

N = 571

Tabell 4

Hvilke konsekvenser tror du det fikk for ham å melde ifra til leder?

	n	%
Ingen konsekvenser	335	64,80 %
Positive konsekvenser slik som ros, omtalt som forbilde	173	33,46 %
Han får økt tillit fra leder	150	29,01 %

Tap av tillit fra leder til kollega	41	7,93 %
Annet	33	6,38 %
Negative konsekvenser slik som kjeft og uthenging	12	2,32 %
Han får mer ansvar	7	1,35 %
Han mister jobben	1	0,19 %

N = 571

Tabell 5

Hvilke reaksjoner får han fra andre kolleger?

	n	%
De viser støtte og forståelse	403	77,95 %
Ingen reaksjon	164	31,72 %
Han blir sett på som naiv eller inkompetent	82	15,86 %
Han blir sett på som forbilde	41	7,93 %
Annet	18	3,48 %
Baksnakking og utestenging	14	2,71 %

N = 571

Kunnskap

Tabell 6

Vet du hvordan du skal si ifra om du blir utsatt for et dataangrep?	*n*	%
Ja	424	74,26 %
Nei	147	25,74 %
Har din arbeidsplass et rapporteringssystem eller noen som er ansvarlig for å motta meldinger om dataangrep?		
Ja	311	54,47 %
Nei	20	3,50 %
Vet ikke	240	42,03 %
Har din arbeidsplass rutiner for å sikre at ansatte følger lover, forskrifter eller standarder for informasjonssikkerhet?		
Ja	372	65,15 %
Nei	24	4,20 %
Vet ikke	175	30,65 %
Har din arbeidsplass rutiner for digital sikkerhet og hendelseshåndteringsplaner?		
Ja	468	81,96 %
Nei	9	1,58 %
Vet ikke	94	16,46 %
Gjennomføres det opplæring og kursing om informasjonssikkerhet på din arbeidsplass?		
Ja	351	61,47 %

Nei	82	14,36 %
Vet ikke	138	24,17 %
Har du deltatt på opplæring innenfor informasjonssikkerhet på din nåværende arbeidsplass?		
Ja	333	58,32 %
Nei	231	40,46 %
Ikke aktuelt	7	1,23 %

Tabell 7

Påstand	Helt uenig	2	3	4	Helt enig
Ansatte ved min arbeidsplass har god kjennskap til rutiner for informasjonssikkerhet	4,20 %	19,96 %	45,71 %	23,64 %	6,48 %
En gjennomsnittlig kollega ved min arbeidsplass ville ikke oppdaget et mulig dataangrep	7,18 %	33,63 %	39,23 %	17,69 %	2,28 %
Vi mangler systemer og verktøy for å melde ifra om dataangrep	23,82 %	29,42 %	28,37 %	13,31 %	5,08 %
Jeg kjenner igjen et forsøk på dataangrep når jeg ser det	3,85 %	7,88 %	33,27 %	45,18 %	9,81 %
En gjennomsnittlig ansatt ved min arbeidsplass vet hva som skal meldes i fra om	3,68 %	20,32 %	43,96 %	28,02 %	4,03 %
Det legges ikke vekt på datasikkerhet på min arbeidsplass	40,98 %	27,32 %	21,02 %	7,88 %	2,80 %
Mine medarbeidere følger alltid rutiner for informasjonssikkerhet	3,85 %	20,32 %	53,06 %	19,79 %	2,98 %

N = 571

Hendelser

Tabell 8

Har din virksomhet blitt utsatt for dataangrep?	**Antall**	**Prosent**
Ja	305	53,40 %
Nei	32	5,60 %
Vet ikke	234	41,00 %
N = 571		
Ble hendelsen rapportert til noen av de følgende?		
Vet ikke	163	53,44 %
Administrator av det aktuelle tekniske systemet	153	50,16 %
Politiet	24	7,87 %
Sektor CERT eller lignende	17	5,57 %
Andre myndighetsorganer	12	3,93 %
Ikke aktuelt	9	2,95 %
ISP (nett- og tjenesteleverandører)	8	2,62 %

NorCERT	8	2,62 %
Antivirusleverandør	6	1,97 %
Bank eller kredittkortselskap	4	1,31 %
n = 305		
Hvor ofte blir din arbeidsplass utsatt for dataangrep?		
Daglig	33	5,78 %
Ukentlig	38	6,65 %
Månedlig	42	7,36 %
Årlig	21	3,68 %
Aldri	5	0,88 %
Vet ikke	432	75,66 %
N = 571		
Har du vært utsatt for dataangrep i tilknytning til arbeidsplassen din?		
Ja	199	34,85 %
Nei	272	47,64 %
Vet ikke	100	17,51 %
N = 571		
Hvordan fikk du vite at du hadde blitt utsatt for dataangrep?		
Jeg oppdaget det selv	165	82,91 %
Melding fra IT-system	69	34,67 %
IT-avdeling sa ifra	67	33,67 %
Kollega sa ifra	16	8,04 %
Leder sa i fra	10	5,03 %
Annet	6	3,02 %
n = 199		
Hvilken type dataangrep ble du utsatt for?		
Phishing-epost	175	87,94 %
Bedrageri (direktørsvindel)	50	25,13 %
Annet	15	7,54 %
Krypteringsangrep (løsepengevirus)	12	6,03 %
Datainnbrudd/hacking	11	5,53 %
n = 199		
Meldte du ifra om at angrepet hadde skjedd?		
Ja	125	62,81 %
Nei	47	23,62 %
Ikke aktuelt	27	13,57 %
n = 199		
Hvorfor var det ikke aktuelt å melde ifra?		
Annet	28	37,84 %
IT-systemet meldte automatisk i fra	26	35,14 %
IT-avdelingen/den ansvarlige personen ble varslet automatisk	20	27,03 %
Jeg visste ikke hvordan jeg skulle melde i fra	11	14,86 %
Det hadde ingen hensikt, angrepet hadde allerede skjedd	9	12,16 %

Jeg visste ikke at jeg hadde blitt utsatt for dataangrep	1	1,35 %
Det fantes ingen å melde ifra til	1	1,35 %
Jeg var redd for negative reaksjoner fra leder	0	0,00 %
Jeg kunne ikke melde ifra anonymt	0	0,00 %
Jeg var redd for negative reaksjoner fra kolleger	0	0,00 %
n = 74		
Hvor lang tid gikk det fra du ble klar over at hendelsen hadde skjedd til du meldte i fra?		
Umiddelbart	104	83,20 %
Etter noen timer	8	6,40 %
Iløpet av en dag	10	8,00 %
Innen en uke	1	0,80 %
Innen en måned	2	1,60 %
n = 125		
Om du hadde blitt utsatt for et dataangrep og det var aktuelt, hadde du meldt i fra?		
Ja	356	95,70 %
Nei	3	0,81 %
Vet ikke	13	3,49 %
n = 372		
Hvorfor ville du ikke, eller vet du ikke om du ville, meldt i fra?		
Jeg vet ikke hvordan jeg melder i fra	6	37,50 %
Jeg ville ikke visst at jeg hadde blitt utsatt for et dataangrep	4	25,00 %
Annet	4	25,00 %
IT-avdelingen/den ansvarlige personen ble varslet automatisk	3	18,75 %
IT-systemet meldte automatisk i fra	1	6,25 %
Jeg har ikke mulighet til å melde ifra anonymt	1	6,25 %
Det har ingen hensikt, angrepet har allerede skjedd	1	6,25 %
Det finnes ingen å melde ifra til	0	0,00 %
Jeg er redd for negative reaksjoner fra leder	0	0,00 %
Jeg var redd for negative reaksjoner fra kolleger	0	0,00 %
n = 16		

Tabell 9

	Daglig	Ukentlig	Månedlig	Årlig	Aldri	Vet ikke
IT, *n = 36*	28 %	17 %	8 %	3 %	0 %	44 %
Kundeservice, n = 15	7 %	20 %	27 %	0 %	0 %	47 %
HR, *n = 14*	14 %	14 %	0 %	14 %	0 %	57 %
Markedsføring, *n* = 22	9 %	14 %	18 %	0 %	0 %	59 %
Økonomi, *n*= 33	6 %	6 %	6 %	18 %	0 %	64 %
Ledelse/admin, *n* = 89	4 %	10 %	3 %	2 %	3 %	76 %
Forskning/undervisning, *n* = 347	3 %	3 %	7 %	3 %	1 %	82 %
Drift/produksjon, *n* = 15	0 %	7 %	7 %	0 %	0 %	87 %

Tabell 10

Påstand	Helt uenig	2	3	4	Helt enig
Det er umulig å vite hva man skal melde ifra om	29,95 %	36,43 %	19,79 %	11,21 %	2,63 %
Jeg kommer ikke til å bli utsatt for dataangrep på min arbeidsplass	57,09 %	28,37 %	12,08 %	1,93 %	0,53 %
Våre rutiner for å melde ifra om dataangrep er tungvinte og kompliserte	22,24 %	28,55 %	40,46 %	7,01 %	1,75 %
Mine kolleger melder ikke ifra om dataangrep	20,67 %	28,20 %	46,58 %	3,50 %	1,05 %
Om min arbeidsplass utsettes for dataangrep vil vi ha full kontroll over situasjonen	7,71 %	21,54 %	52,54 %	15,41 %	2,80 %
Det er uunngåelig å bli utsatt for dataangrep	4,03 %	8,23 %	29,25 %	32,75 %	25,74 %
Å melde ifra om et dataangrep som allerede har skjedd påvirker ikke utfallet av det	54,64 %	24,34 %	16,11 %	3,50 %	1,40 %
Hvem som blir utsatt for dataangrep er helt tilfeldig	6,13 %	22,59 %	34,68 %	22,07 %	14,54 %

N = 571

Konsekvenser

Tabell 11

Da du meldte ifra om hendelsen(e), hvilke konsekvenser fikk det for deg?*	*n*	%
Positiv tilbakemelding fra kolleger	44	35,20 %
Negativ tilbakemelding fra kolleger	1	0,80 %
Positiv tilbakemelding fra leder	25	20,00 %
Negativ tilbakemelding fra leder	0	0,00 %
Positive tanker om meg selv (eks. stolt av å varsle ifra)	29	23,20 %
Negative tanker om meg selv (eks. flau, følte meg dum)	6	4,80 %
Ingen konsekvenser	79	63,20 %
n = 125		
* Kun mulig å besvare hvis man svarte «Ja» på «Meldte du ifra om at angrepet hadde skjedd?».		
Hvis du hadde meldt ifra da du ble utsatt for dataangrepet, hvilke konsekvenser er det sannsynlig at du ville fått?*		
Positiv tilbakemelding fra kolleger	29	39,19 %
Negativ tilbakemelding fra kolleger	5	6,76 %
Positiv tilbakemelding fra leder	38	51,35 %
Negativ tilbakemelding fra leder	4	5,41 %
Positive tanker om meg selv (eks. stolt av å varsle ifra)	21	28,38 %
Negative tanker om meg selv (eks. flau, følte meg dum)	11	14,86 %
Ingen konsekvenser	39	52,70 %

n = 74
* Kun mulig å besvare hvis man svarte «Nei» eller «Ikke aktuelt» på «Meldte du ifra om at angrepet hadde skjedd?».

Hvis du hadde blitt utsatt for et dataangrep og meldt ifra om hendelsen, hvilke konsekvenser er det sannsynlig at du ville fått?*		
Positiv tilbakemelding fra kolleger	195	52,42 %
Negativ tilbakemelding fra kolleger	14	3,76 %
Positiv tilbakemelding fra leder	239	64,25 %
Negativ tilbakemelding fra leder	10	2,69 %
Positive tanker om meg selv (eks. stolt av å varsle ifra)	89	23,92 %
Negative tanker om meg selv (eks. flau, følte meg dum)	87	23,39 %
Ingen konsekvenser	105	28,23 %

n = 372
* Kun mulig å besvare hvis man svarte «Nei» eller «Vet ikke» på «Har du vært utsatt for dataangrep i tilknytning til arbeidsplassen din?».

Tabell 12

Påstand	Helt uenig	2	3	4	Helt enig
Det er flaut å bli utsatt for dataangrep	50,26 %	18,21 %	15,94 %	11,03 %	4,55 %
Om jeg ikke melder ifra om et dataangrep får jeg negativ tilbakemelding fra kolleger eller leder	13,31 %	13,13 %	29,07 %	26,09 %	18,39 %
I min virksomhet oppmuntres man til å melde ifra om dataangrep	5,25 %	8,58 %	25,22 %	25,57 %	35,38 %
Jeg mister mestringsfølelse om jeg blir utsatt for dataangrep	40,81 %	22,07 %	23,64 %	10,86 %	2,63 %
Jeg får mestringsfølelse av å melde ifra om et (mulig) dataangrep	4,55 %	7,01 %	38,53 %	33,10 %	16,81 %
Om jeg melder ifra om et dataangrep får jeg negativ tilbakemelding for at angrepet skjedde i utgangspunktet	62,35 %	22,59 %	13,49 %	1,23 %	0,35 %
Om jeg blir utsatt for et dataangrep blir jeg godt ivaretatt av mine kolleger	1,93 %	2,63 %	32,05 %	35,20 %	28,20 %

N = 571

Hjemmekontor

Tabell 13

Har du hatt hjemmekontor (i noen som helst utstrekning) siden 12.mars 2020?	*n*	%
Ja	523	91,59 %
Nei	48	8,41 %
N = 571		
Har du fått informasjon om hvordan man kan ivareta informasjonssikkerhet på hjemmekontor?		
Ja	219	38,35 %
Nei	266	46,58 %
Vet ikke	86	15,06 %
N = 571		
Har du formidlet informasjon om hvordan man kan ivareta informasjonssikkerhet på hjemmekontor til ansatte i din virksomhet?		
Ja	64	11,21 %
Nei	507	88,79 %
Har du opplevd dataangrep etter du begynte med hjemmekontor det siste året?		
Ja	71	13,58 %
Nei	367	70,17 %
Vet ikke	85	16,25 %
n = 523 * Kun mulig å besvare hvis man svarte «Ja» på «Har du hatt hjemmekontor (i noen som helst utstrekning) siden 12.mars 2020?»		
Hvordan opplever du, eller ville du opplevd, å melde ifra om dataangrep fra hjemmekontor i motsetning til ordinært kontor?		
Vanskeligere, vet ikke hvordan jeg melder ifra på hjemmekontor	22	3,85 %
Lettere, trenger ikke si det ansikt til ansikt	9	1,58 %
Ingen forskjell fra vanlig kontor	523	91,59 %
Vanskeligere fordi jeg ikke oppdager dataangrep like lett	17	2,98 %
N = 571		

Tabell 14

Påstand	Helt uenig	2	3	4	Helt enig
Jeg opplever hjemmekontor like trygt som min ordinære arbeidsplass	3,68 %	13,31 %	18,74 %	28,02 %	27,85 %
Jeg har ikke det tekniske utstyret til å ivareta informasjonssikkerhet på hjemmekontor	32,75 %	24,34 %	25,04 %	7,18 %	2,28 %
På hjemmekontor er sannsynligheten for å bli utsatt for dataangrep mindre enn ordinært kontor	34,50 %	25,57 %	28,37 %	2,63 %	0,53 %
Mitt hjemmekontor er mer utsatt for dataangrep enn mitt ordinære kontor	17,86 %	18,74 %	37,65 %	12,43 %	4,90 %
N = 571					

Vedlegg A

Ebsco – Business Source Elite

Search ID#	Search Terms	Search Options	Last Run Via	Results
S11	S7 AND S10	Limiters - Scholarly (Peer Reviewed) Journals Search modes - Boolean/Phrase	Interface - EBSCOhost Research Databases Search Screen - Advanced Search Database - Business Source Elite	132
S10	S8 OR S9	Search modes - Boolean/Phrase	Interface - EBSCOhost Research Databases Search Screen - Advanced Search Database - Business Source Elite	Display
S9	adherence OR compliance OR reporting OR notif*	Search modes - Boolean/Phrase	Interface - EBSCOhost Research Databases Search Screen - Advanced Search Database - Business Source Elite	Display
S8	DE "COMPLIANCE auditing"	Search modes - Boolean/Phrase	Interface - EBSCOhost Research Databases Search Screen - Advanced Search Database - Business Source Elite	Display
S7	S3 AND S6	Limiters - Scholarly (Peer Reviewed) Journals; Published Date: -20210431	Interface - EBSCOhost Research Databases Search Screen - Advanced Search	Display

		Search modes - Boolean/Phrase	Database - Business Source Elite	
S6	S4 OR S5	Search modes - Boolean/Phrase	Interface - EBSCOhost Research Databases Search Screen - Advanced Search Database - Business Source Elite	Display
S5	organizational culture* OR organisational culture* OR corporate culture* OR institution* culture* OR safety culture* OR organization* behav* OR organisation* behav*	Search modes - Boolean/Phrase	Interface - EBSCOhost Research Databases Search Screen - Advanced Search Database - Business Source Elite	Display
S4	(DE "CORPORATE culture" OR DE "DECOUPLING (Organizational behavior)" OR DE "EMPLOYEE misconduct" OR DE "MISCONDUCT in office" OR DE "ORGANIZATIONAL citizenship behavior" OR DE "SILO mentality" OR DE "COMMUNICATION in industrial safety" OR DE "INDUSTRIAL safety education" OR DE "PROCESS safety management" OR DE "RISK management in business" OR DE "SAFETY incentive programs" OR DE "SAFETY managers" OR DE "SECURITY management")	Search modes - Boolean/Phrase	Interface - EBSCOhost Research Databases Search Screen - Advanced Search Database - Business Source Elite	Display
S3	S1 OR S2	Search modes - Boolean/Phrase	Interface - EBSCOhost Research Databases Search Screen - Advanced Search Database - Business Source Elite	Display

S2	information security OR cyber security OR computer security OR data security	Search modes - Boolean/Phrase	Interface - EBSCOhost Research Databases Search Screen - Advanced Search Database - Business Source Elite	Display
S1	(DE "INFORMATION technology security" OR DE "COMPUTER security" OR DE "ACCESS control" OR DE "COMPUTER passwords" OR DE "COMPUTER systems security vulnerabilities" OR DE "COMPUTER crimes" OR DE "COMPUTER hacking" OR DE "DATA security")	Search modes - Boolean/Phrase	Interface - EBSCOhost Research Databases Search Screen - Advanced Search Database - Business Source Elite	Display

Ovid – PsycInfo

1. exp Information Security/

2. exp Organizational Behavior/ or exp Employee Attitudes/ or exp Organizational Climate/ or exp Organizational Learning/ or exp Organizational Change/ or exp Leadership/ or organization* culture.mp.

3. 1 and 2

4. limit 3 to (peer reviewed journal and (danish or english or norwegian or swedish))

Web of Science

86 #8 AND #4
11 **Refined by: LANGUAGES:** (ENGLISH) AND **DOCUMENT TYPES:** (ARTICLE OR EARLY ACCESS OR REVIEW)
Indexes=SCI-EXPANDED, SSCI, A&HCI, ESCI Timespan=All years

86 #8 AND #4
10 **Refined by: LANGUAGES:** (ENGLISH)
Indexes=SCI-EXPANDED, SSCI, A&HCI, ESCI Timespan=All years

#9	87	#8 AND #4 *Indexes=SCI-EXPANDED, SSCI, A&HCI, ESCI Timespan=All years*
#8	3,463,802	TS=("reinforce" OR"consequence"OR "punish" OR "negative" OR "positive"OR"avoidance" OR"escape"OR"powerless"OR"attribute") *Indexes=SCI-EXPANDED, SSCI, A&HCI, ESCI Timespan=All years*
#7	551	#3 AND #2 AND #1 **Refined by: LANGUAGES:** (ENGLISH OR NORWEGIAN) AND **DOCUMENT TYPES:** (ARTICLE OR REVIEW) *Indexes=SCI-EXPANDED, SSCI, A&HCI, ESCI Timespan=All years*
#6	552	#3 AND #2 AND #1 **Refined by: LANGUAGES:** (ENGLISH OR NORWEGIAN) *Indexes=SCI-EXPANDED, SSCI, A&HCI, ESCI Timespan=All years*
#5	1	#3 AND #2 AND #1 **Refined by: LANGUAGES:** (NORWEGIAN) *Indexes=SCI-EXPANDED, SSCI, A&HCI, ESCI Timespan=All years*
#4	567	#3 AND #2 AND #1 *Indexes=SCI-EXPANDED, SSCI, A&HCI, ESCI Timespan=All years*
#3	854,890	TS=("reporting" OR "decoupling" OR "warning" OR "alert" OR "sanction"OR"Compliance"OR"awareness"OR"adherence"OR"notif*") *Indexes=SCI-EXPANDED, SSCI, A&HCI, ESCI Timespan=All years*
#2	231,606,044	TS=("organizational culture" OR "corporate culture" OR "organisational culture" OR "organizational behavior" OR "organizational climate" OR "organizational learning" OR "organizational change" OR "management" OR "leadership" OR "employee"OR"organizational behaviour"OR"human factors") *Indexes=SCI-EXPANDED, SSCI, A&HCI, ESCI Timespan=All years*
#1	11,994	**TOPIC:** ("information security" OR "computer security" OR "data security" OR "cyber security") *Indexes=SCI-EXPANDED, SSCI, A&HCI, ESCI Timespan=All years*

Vedlegg B

Informasjonsskriv og samtykke

Under finner du et informasjonsskriv som vi vil be deg lese gjennom før du krysser av for eventuelt samtykke. I dette skrivet får du informasjon om målene for prosjektet og om hva deltakelse vil innebære for deg. Har du spørsmål om undersøkelsen finner du kontaktinformasjon lenger ned.

Informasjonssikkerhetskultur
Formål

Denne spørreundersøkelsen er en del av et mastergradsprosjekt hvor formålet er å undersøke betingelser for atferd knyttet til informasjonssikkerhetskultur i virksomheter. Undersøkelsen inneholder spørsmål om informasjonssikkerhetshendelser ved din arbeidsplass, kjennskap til gjeldende regelverk og rutiner for varsling, håndtering av hendelser slik som phishing-epost, bedrageri og kryptering (løsepengevirus), konsekvenser av å melde ifra og spørsmål knyttet til hjemmekontor.

Undersøkelsen skal gi et overblikk over tilstanden i flere norske virksomheter, og oppgaven vil forsøke å forklare resultatene fra et atferdsanalytisk perspektiv.

Opplysningene som blir samlet inn gjennom spørreundersøkelsen skal brukes til masterprosjektet i første omgang. Det kan være aktuelt å publisere, og da vil alle data være fullstendig anonymisert.

Hvem er ansvarlig for forskningsprosjektet?
OsloMet er ansvarlig for prosjektet.
Hvorfor får du spørsmål om å delta?

Du har blitt bedt om å delta i denne spørreundersøkelsen gjennom et samarbeid med en IT-konsulentfirma, som har bidratt med rekruttering av flere relevante virksomheter og utforming av undersøkelsen.

Spørsmål om deltakelse har også blitt sendt ut til alle ansatte ved OsloMet, og vi har fått tilgang til din e-postadresse via innsynsbegjæring, og behandlingsgrunnlag for utsendelse med personvernforordningen berettigete interesser (art.6 nr. 1 bokstav f).

For alle deltakere er grunnlaget for selve innsamlingen av besvarelser informert samtykke (art. 6 nr. 1 bokstav a), som gis ved å krysse av for dette under.

Det vil bli sendt ut én påminnelse om undersøkelsen en uke etter første utsendelse.

Hva innebærer det for deg å delta?

For å delta gir du ditt samtykke nederst på denne siden. Her vil du bli bedt om å oppgi en e-postadresse, slik at din besvarelse kan gjenfinnes om du ønsker å trekke deg, slik at den da kan slettes. Etter samtykke blir du sendt videre til undersøkelsen i Nettskjema, og besvarelse vil ta 10-12 minutter. Dine svar blir registrert elektronisk.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

De som vil ha tilgang til data som samles inn i denne spørreundersøkelsen er dosent Gunnar Ree, og masterstudent Ann Kristin Sjøflot.

Opplysningene lagres kryptert i Nettskjema, som er godkjent for å samle inn og lagre denne typen data. Personinformasjon fra samtykket blir lagret kryptert, og kan kun kobles til din besvarelse med en koblingsnøkkel.

Leverandør av løsningen for spørreundersøkelsen er Nettskjema, https://www.uio.no/tjenester/it/adm-app/nettskjema/.

Individuelle besvarelser vil ikke bli delt direkte med din arbeidsplass eller andre enn prosjektansvarlig og masterstudenten. Den ferdigstilte oppgaven kan bli gjort tilgjengelig for virksomhetene som har deltatt, enkeltindivider som deltar i undersøkelsen vil ikke kunne gjenkjennes i den ferdigstilte masteroppgaven.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres ved at personidentifiserbare opplysninger fjernes, og koblingsnøkkel slettes når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 15.06.2021. Alle personopplysninger samlet inn gjennom rekrutteringen vil bli slettet ved prosjektets slutt.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke (art. 6 nr. 1 bokstav a). På oppdrag fra OsloMet - Institutt for atferdsvitenskap, har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene
- å få rettet personopplysninger om deg
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

NSD

Prosjektet har blitt meldt inn til NSD, og er godkjent for gjennomføring. Meldeskjema 673307.

Hvor kan jeg finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Gunnar Ree (dosent, Institutt for atferdsvitenskap, gree@oslomet.no) eller Ann Kristin Sjøflot (masterstudent, Institutt for atferdsvitenskap, s341266@oslomet.no, +47 98008401).
- Vårt personvernombud E-post: personvernombud@oslomet.no

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Gunnar Ree Ann Kristin Sjøflot

Vedlegg C

NSD NORSK SENTER FOR FORSKNINGSDATA

Meldeskjema 673307

Sist oppdatert

16.02.2021

Hvilke personopplysninger skal du behandle?

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator
- Bakgrunnsopplysninger som vil kunne identifisere en person

Type opplysninger

Du har svart ja til at du skal behandle bakgrunnsopplysninger, beskriv hvilke

Spørreundersøkelsen vil inneholde spørsmål om hvilket nivå personen jobber på i virksomheten (leder, mellomleder, ansatt), hvilken avdeling (HR, økonomi, markedsføring etc.) og alder/kjønn. I små virksomheter med få ansatte kan det være mulig å identifisere enkeltpersoner om data kommer på avveie. Men rådata fra undersøkelsen vil ikke bli delt direkte med virksomhetene som deltar, kun den ferdigstilte oppgaven.

Skal du behandle særlige kategorier personopplysninger eller personopplysninger om straffedommer eller lovovertredelser?

Nei

Prosjektinformasjon

Prosjekttittel

Masteroppgave

Prosjektbeskrivelse

Masteroppgave i atferdsvitenskap ved OsloMet. Skal undersøke informasjonssikkerhetskultur og praksis for varsling av avvik knyttet til informasjonssikkerhet i virksomheter, dette gjøres gjennom en spørreundersøkelse i Nettskjema.

Begrunn behovet for å behandle personopplysningene

Selve spørreundersøkelsen vil ikke spørre om noe sensitiv informasjon. De vil bli bedt om samtykke, som gis gjennom Nettskjema, og da blir de bedt om epostadresse/navn, men denne informasjonen vil lagres separat fra deres besvarelse på spørreundersøkelsen. Jeg har vært i kontakt med noen få personer i de virksomhetene hvor spørreskjema er tenkt å sendes ut til, og har dermed epost og navn til disse. Om de besvarer spørreundersøkelsen vil ikke det nødvendigvis si at jeg kan identifisere deres besvarelse. Jeg har navn og epost til noen få personer for å distribuere spørreundersøkelser i virksomheter, og kommer til å spørre om alder, kjønn, stillingstype og hvilket nivå de er på i virksomheten for å beskrive utvalget.

Ekstern finansiering

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Ann Kristin Sjøflot, s341266@oslomet.no, tlf: 98008401

Behandlingsansvar

Behandlingsansvarlig institusjon

OsloMet – storbyuniversitetet / Fakultet for helsevitenskap / Institutt for atferdsvitenskap

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Gunnar Ree, gree@oslomet.no, tlf: 91607580

Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?

Nei

Utvalg 1

Beskriv utvalget

Ansatte i de virksomhetene hvor spørreskjema sendes ut

Rekruttering eller trekking av utvalget

Jeg har samarbeidet med en konsulentvirksomhet som jobber med informasjonssikkerhet, og skal distribuere spørreundersøkelsen videre gjennom dem.

Alder

18 - 80

Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?

Nei

Personopplysninger for utvalg 1

- Navn (også ved signatur/samtykke)
-
- E-postadresse, IP-adresse eller annen nettidentifikator

Bakgrunnsopplysninger som vil kunne identifisere en person

Hvordan samler du inn data fra utvalg 1?

Elektronisk spørreskjema

Grunnlag for å behandle alminnelige kategorier av personopplysninger

Samtykke (art. 6 nr. 1 bokstav a)

Informasjon for utvalg 1

Informerer du utvalget om behandlingen av opplysningene?

Ja

Hvordan?

Skriftlig informasjon (papir eller elektronisk)

Utvalg 2

Beskriv utvalget

Alle ansatte ved OsloMet

Alder

18 - 80

Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?

Nei

Personopplysninger for utvalg 2

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator

Hvordan samler du inn data fra utvalg 2?

Annet

Beskriv

Får tilgang til ansattes e-postadresser for å rekruttere deltakere til selve spørreundersøkelsen

Grunnlag for å behandle alminnelige kategorier av personopplysninger

Berettigete interesser (art. 6 nr. 1 bokstav f)

Redegjør for valget av behandlingsgrunnlag

Trenger tilgang til ansattes e-postadresser for å sende ut forespørsel om deltakelse i undersøkelsen. Tematikken i prosjektet er nyttig for OsloMet som organisasjon.

Informasjon for utvalg 2

Informerer du utvalget om behandlingen av opplysningene? Ja

Hvordan?

Skriftlig informasjon (papir eller elektronisk)

Tredjepersoner

Skal du behandle personopplysninger om tredjepersoner?

Nei

Dokumentasjon

Hvordan dokumenteres samtykkene?

- Elektronisk (e-post, e-skjema, digital signatur)

Hvordan kan samtykket trekkes tilbake?

Deltakere vil kunne trekke tilbake samtykke gjennom samme link til spørreundersøkelse som de fikk utsendt først, og så endre avkrysning til at de ønsker å trekke seg.

Hvordan kan de registrerte få innsyn, rettet eller slettet opplysninger om seg selv?

Ved å kontakte personer som er oppgitt i informasjonsskrivet (masterstudent/prosjektansvarlig), som kan finne igjen deres besvarelse med en koblingsnøkkel.

Totalt antall registrerte i prosjektet

100-999

Tillatelser

Skal du innhente følgende godkjenninger eller tillatelser for prosjektet?

Behandling

Hvor behandles opplysningene?

- Maskinvare tilhørende behandlingsansvarlig institusjon
- Mobile enheter tilhørende behandlingsansvarlig institusjon
- Ekstern tjeneste eller nettverk

(databehandler) Private enheter

Hvem behandler/har tilgang til opplysningene?

- Prosjektansvarlig
- Student

(studentprosjekt)

Databehandler

Hvilken databehandler har tilgang til opplysningene?

Nettskjema. OsloMet har avtale med UiO om bruk av Nettskjema til innsamling og lagring av data.

Tilgjengeliggjøres opplysningene utenfor EU/EØS til en tredjestat eller internasjonal organisasjon?

Nei

Sikkerhet

Oppbevares personopplysningene atskilt fra øvrige data (koblingsnøkkel)?

Ja

Hvilke tekniske og fysiske tiltak sikrer personopplysningene?

- Opplysningene anonymiseres
- fortløpende opplysningene krypteres under lagring
- Adgangsbegrensning

Varighet

Prosjektperiode

01.01.2021 - 15.06.2021

Skal data med personopplysninger oppbevares utover prosjektperioden?

Nei, data vil bli oppbevart uten personopplysninger (anonymisering)

Hvilke anonymiseringstiltak vil bli foretatt?

- Koblingsnøkkelen slettes
- Personidentifiserbare opplysninger fjernes, omskrives eller grovkategoriseres

Vil de registrerte kunne identifiseres (direkte eller indirekte) i oppgave/avhandling/øvrige publikasjoner fra prosjektet?

Nei**Tilleggsopplysninger**

Vedlegg D

Spørreundersøkelse Informasjonssikkerhet

Side 1

Obligatoriske felter er merket med denne stjernen *

Denne undersøkelsen har 6 deler: bakgrunnsinformasjon, scenario, kunnskap, hendelser og konsekvenser, og hjemmekontor.

Det tar 10-12 minutter å svare.

Om ingen svaralternativ passer, velg det som blir mest riktig eller utdyp i tekstboks der det er mulig.

Alle spørsmål er obligatoriske. Det er ikke mulig å gå videre uten å svare.

Takk for at du tar deg tid til å svare på denne undersøkelsen!

Sideskift

Side 2

Obligatoriske felter er merket med denne stjernen *

Bakgrunnsinformasjon

Kjønn *

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Spørreundersøkelse Informasjonssikkerhet

Side 1

Obligatoriske felter er merket med denne stjernen *

Denne undersøkelsen har 6 deler: bakgrunnsinformasjon, scenario, kunnskap, hendelser og konsekvenser, og hjemmekontor.

Det tar 10-12 minutter å svare.

Om ingen svaralternativ passer, velg det som blir mest riktig eller utdyp i tekstboks der det er mulig.

Alle spørsmål er obligatoriske. Det er ikke mulig å gå videre uten å svare.

Takk for at du tar deg tid til å svare på denne undersøkelsen!

Sideskift

Side 2

Obligatoriske felter er merket med denne stjernen *

Bakgrunnsinformasjon

Kjønn *

https://nettskjema.no/user/form/preview.html?id=184450#/ 1/40

- ◯ Kvinne
- ◯ Mann
- ◯ Annet/ønsker ikke oppgi

Alder *

Hvilken virksomhet arbeider du i? *

- ◯ Universitet
- ◯ IT-konsulentfirma
- ◯ Rådgivningsvirksomhet
- ◯ Kraftverk
- ◯ Kommune
- ◯ Revisjonsfirma

Hvor mange ansatte arbeider i din virksomhet? *

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

- ◯ Kvinne
- ◯ Mann
- ◯ Annet/ønsker ikke oppgi

Alder *

Hvilken virksomhet arbeider du i? *

- ◯ Universitet
- ◯ IT-konsulentfirma
- ◯ Rådgivningsvirksomhet
- ◯ Kraftverk
- ◯ Kommune
- ◯ Revisjonsfirma

Hvor mange ansatte arbeider i din virksomhet? *

https://nettskjema.no/user/form/preview.html?id=184450#/ 2/40

- 5-19
- 20-49
- 50-99
- 100 eller mer

Har du lederansvar på din arbeidsplass? *

- Ja
- Nei

På hvilket nivå er stillingen din? *

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du lederansvar på din arbeidsplass?»

- Medarbeider
- Mellomleder
- Leder

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

- 5-19
- 20-49
- 50-99
- 100 eller mer

Har du lederansvar på din arbeidsplass? *

- Ja
- Nei

På hvilket nivå er stillingen din? *

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du lederansvar på din arbeidsplass?»

- Medarbeider
- Mellomleder
- Leder

https://nettskjema.no/user/form/preview.html?id=184450#/ 3/40

Hvilket felt jobber du innenfor? *

Velg det som passer best

- ○ IT
- ○ HR og personal
- ○ Markedsføring/kommunikasjon, salg og tjenestelevering
- ○ Ledelse og administrasjon
- ○ Økonomi
- ○ Kundeservice
- ○ Forskning og undervisning
- ○ Drift og vedlikehold, produksjon

Sideskift

Obligatoriske felter er merket med denne stjernen *

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Hvilket felt jobber du innenfor? *

Velg det som passer best

- ○ IT
- ○ HR og personal
- ○ Markedsføring/kommunikasjon, salg og tjenestelevering
- ○ Ledelse og administrasjon
- ○ Økonomi
- ○ Kundeservice
- ○ Forskning og undervisning
- ○ Drift og vedlikehold, produksjon

Sideskift

Side 3

Obligatoriske felter er merket med denne stjernen *

https://nettskjema.no/user/form/preview.html?id=184450#/ 4/40

Scenario

Nå får du presentert et tenkt scenario som er veldig vanlig i norske virksomheter i dag. Svar hvordan du tror en kollega i din virksomhet mest sannsynlig ville håndtert denne saken.

En kollega av deg får tilsendt en mail fra Ola Normann med deling av et dokument fra Microsoft Sharepoint (se bilde). Ola Normann er en kjent person fra en samarbeidende virksomhet. Din kollega klikker på dokumentet, og får opp en innloggingside fra Microsoft som ber ham logge inn med sitt brukernavn og passord. Han logger på, og laster ned dokumentet. Dokumentet inneholder lite relevant informasjon, og din kollega begynner å lure på om han akkurat har blitt utsatt for et phising-angrep.

Dette elementet vises kun dersom alternativet «HR og personal» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

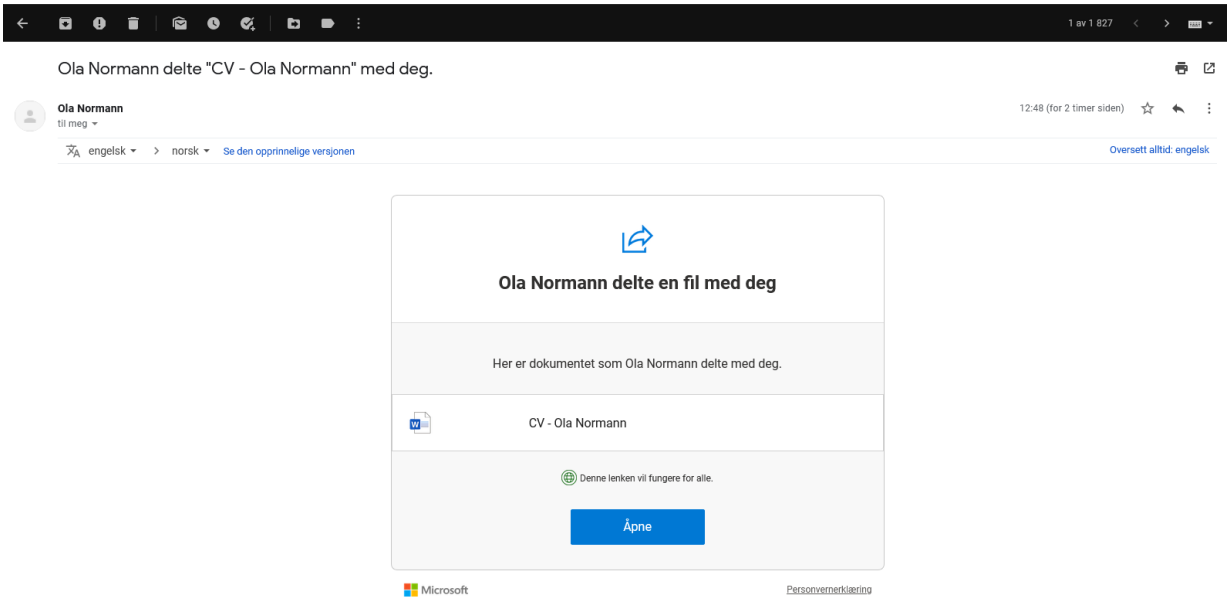
Scenario

Nå får du presentert et tenkt scenario som er veldig vanlig i norske virksomheter i dag. Svar hvordan du tror en kollega i din virksomhet mest sannsynlig ville håndtert denne saken.

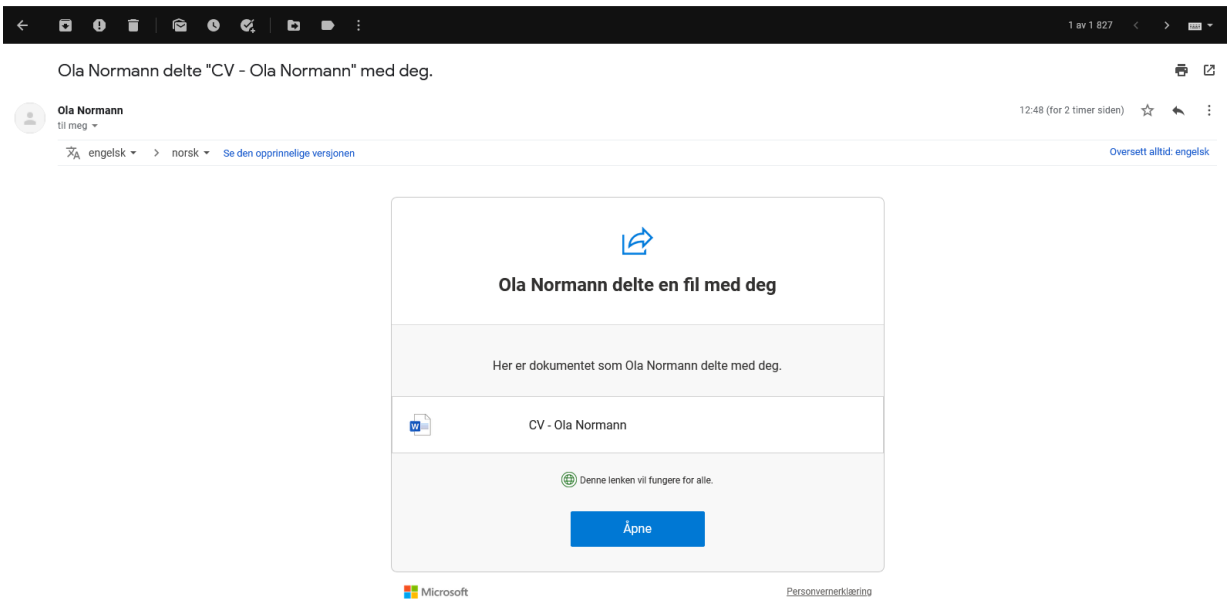
En kollega av deg får tilsendt en mail fra Ola Normann med deling av et dokument fra Microsoft Sharepoint (se bilde). Ola Normann er en kjent person fra en samarbeidende virksomhet. Din kollega klikker på dokumentet, og får opp en innloggingside fra Microsoft som ber ham logge inn med sitt brukernavn og passord. Han logger på, og laster ned dokumentet. Dokumentet inneholder lite relevant informasjon, og din kollega begynner å lure på om han akkurat har blitt utsatt for et phising-angrep.

Dette elementet vises kun dersom alternativet «HR og personal» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»

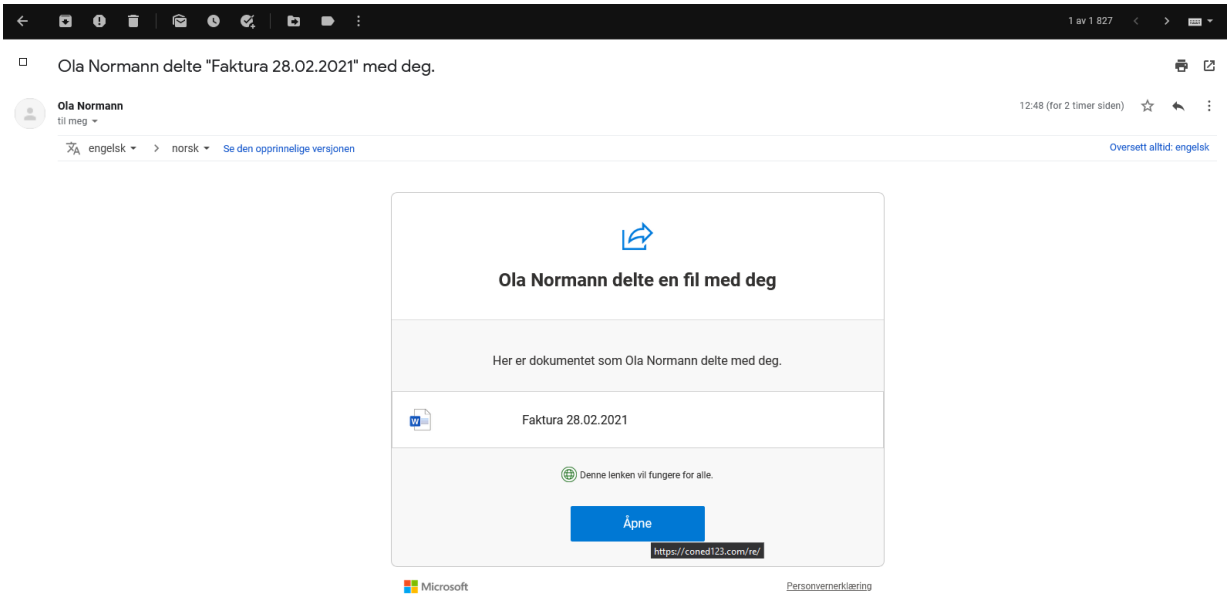
https://nettskjema.no/user/form/preview.html?id=184450#/ 5/40



Dette elementet vises kun dersom alternativet «Økonomi» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»

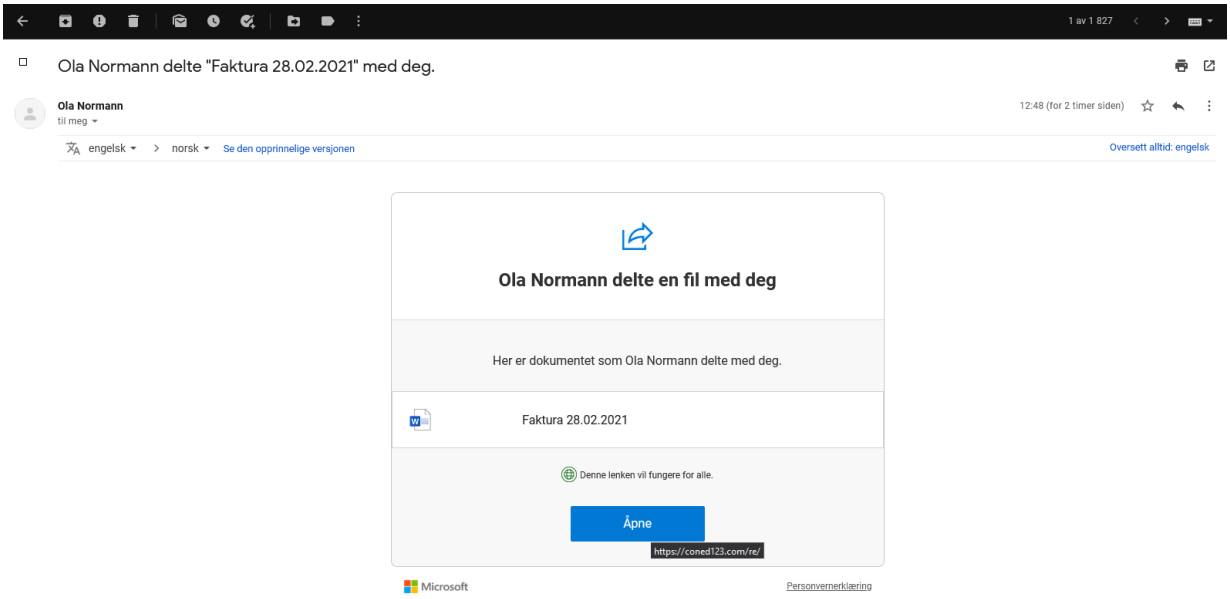


Dette elementet vises kun dersom alternativet «Økonomi» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»

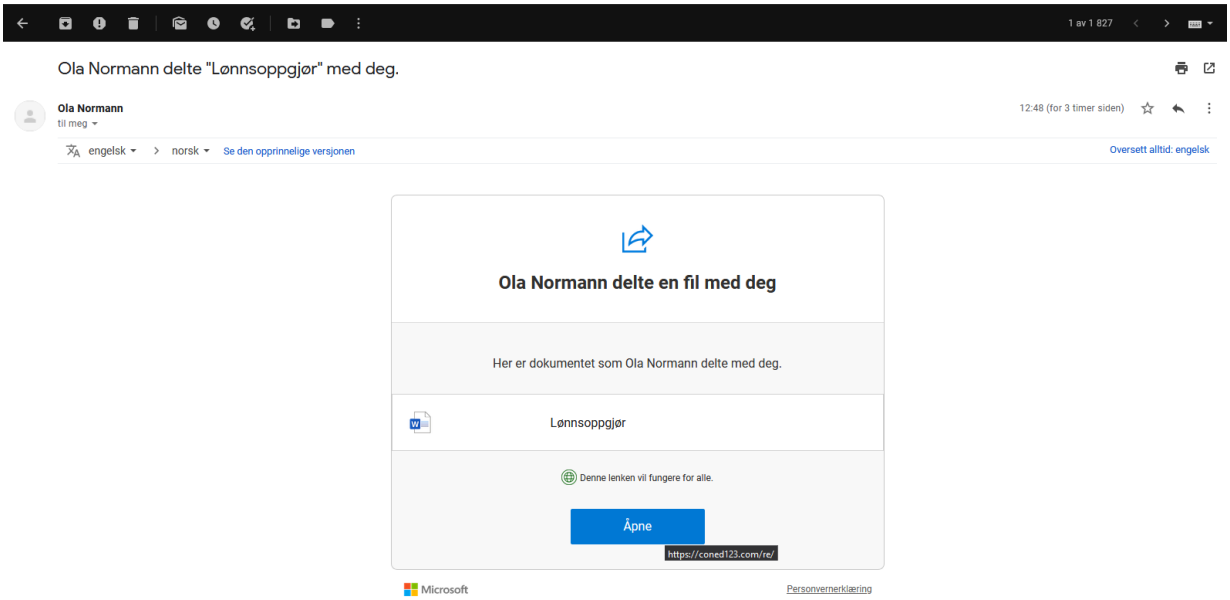


Dette elementet vises kun dersom alternativet «Ledelse og administrasjon» eller «Forskning og undervisning» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

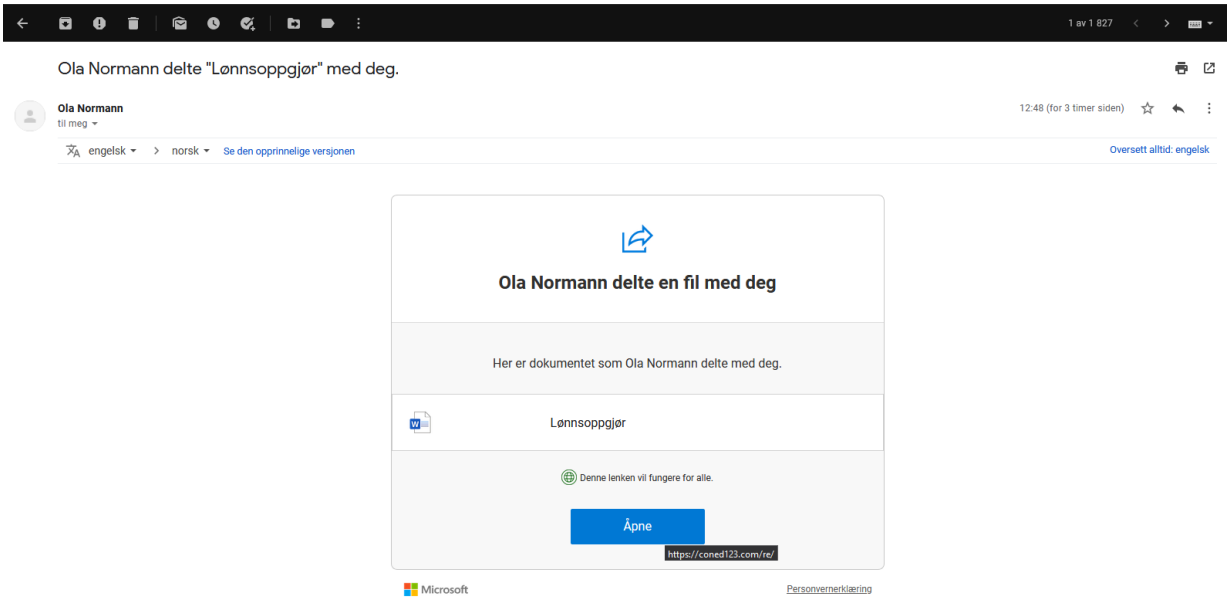


Dette elementet vises kun dersom alternativet «Ledelse og administrasjon» eller «Forskning og undervisning» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»

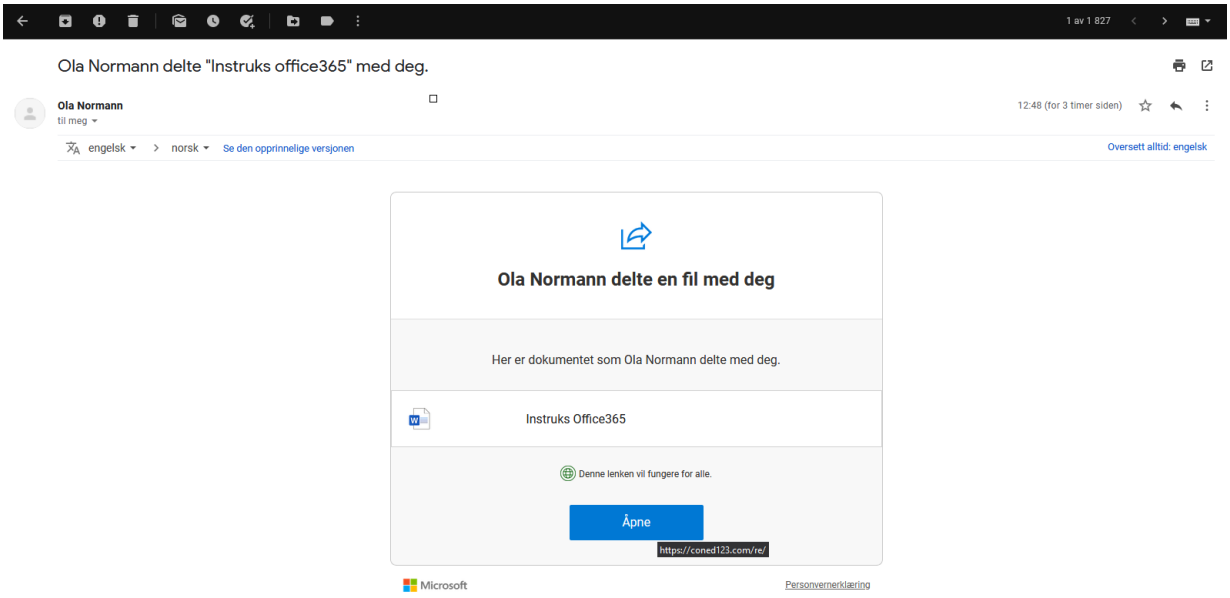


Dette elementet vises kun dersom alternativet «IT» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»

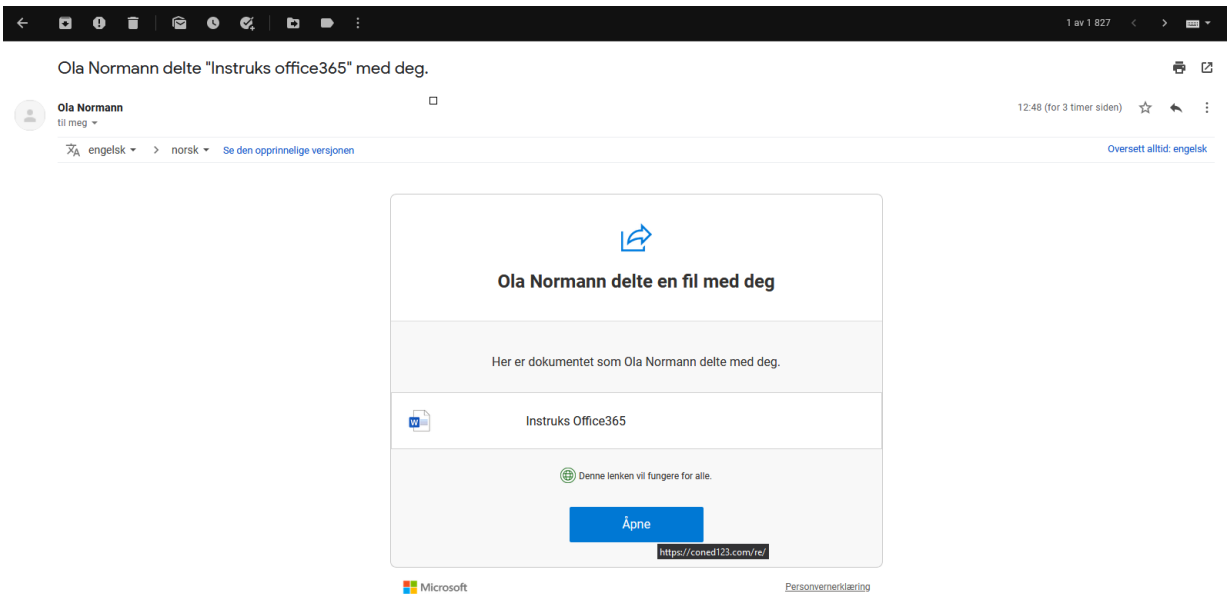
14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema



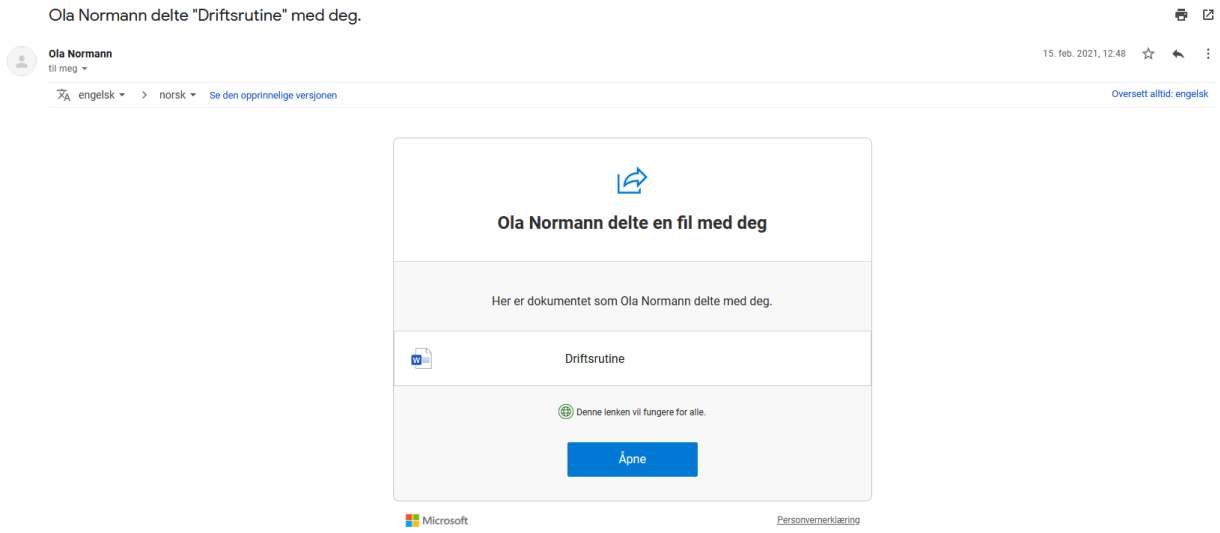
Dette elementet vises kun dersom alternativet «IT» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»



Dette elementet vises kun dersom alternativet «Drift og vedlikehold, produksjon» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»

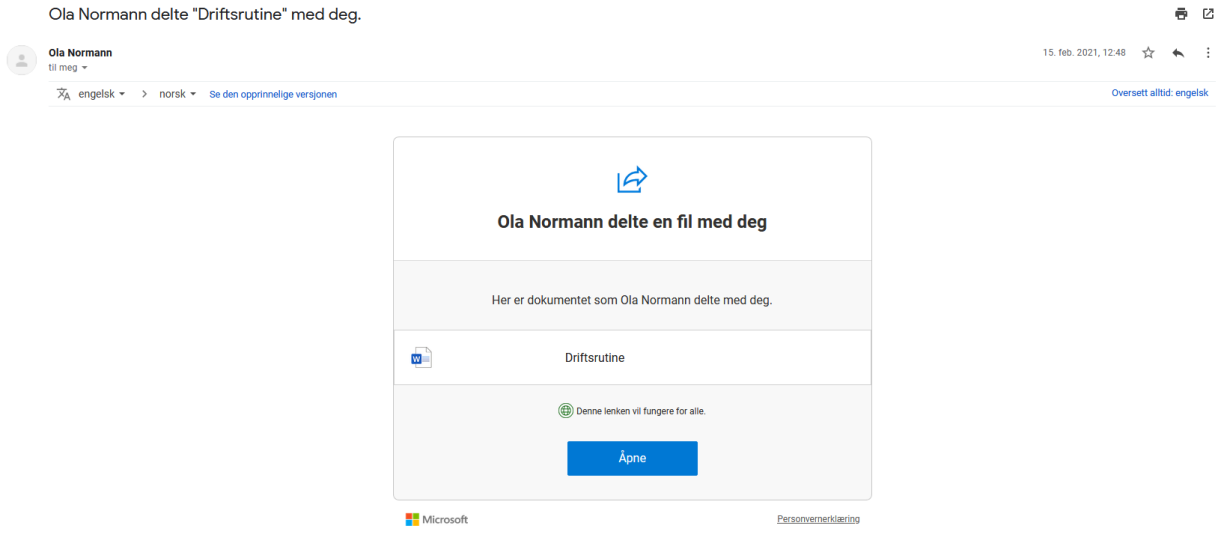


Dette elementet vises kun dersom alternativet «Drift og vedlikehold, produksjon» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»

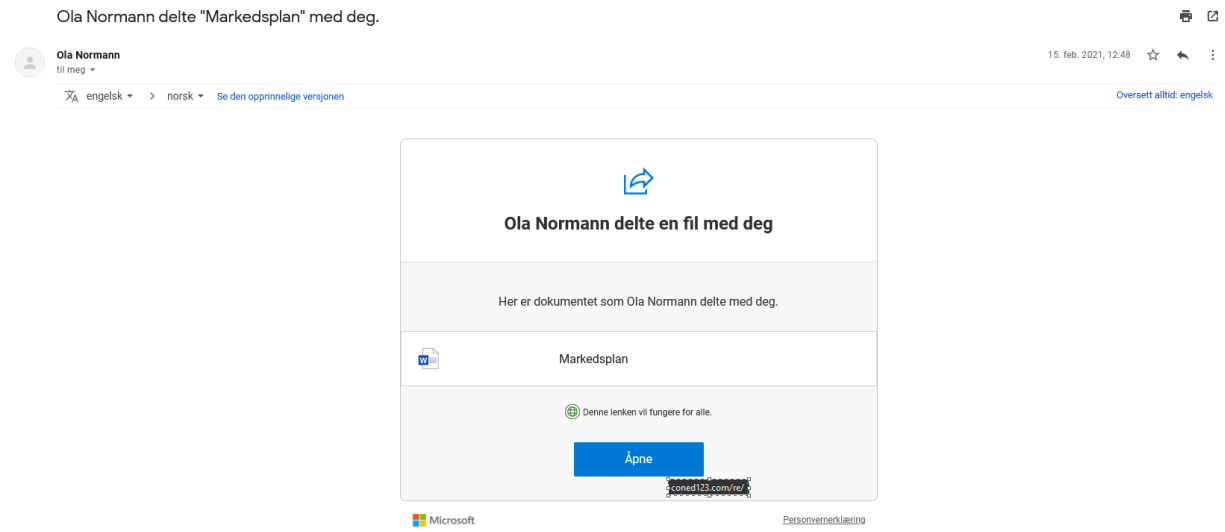


Dette elementet vises kun dersom alternativet «Markedsføring/kommunikasjon, salg og tjenestelevering» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»

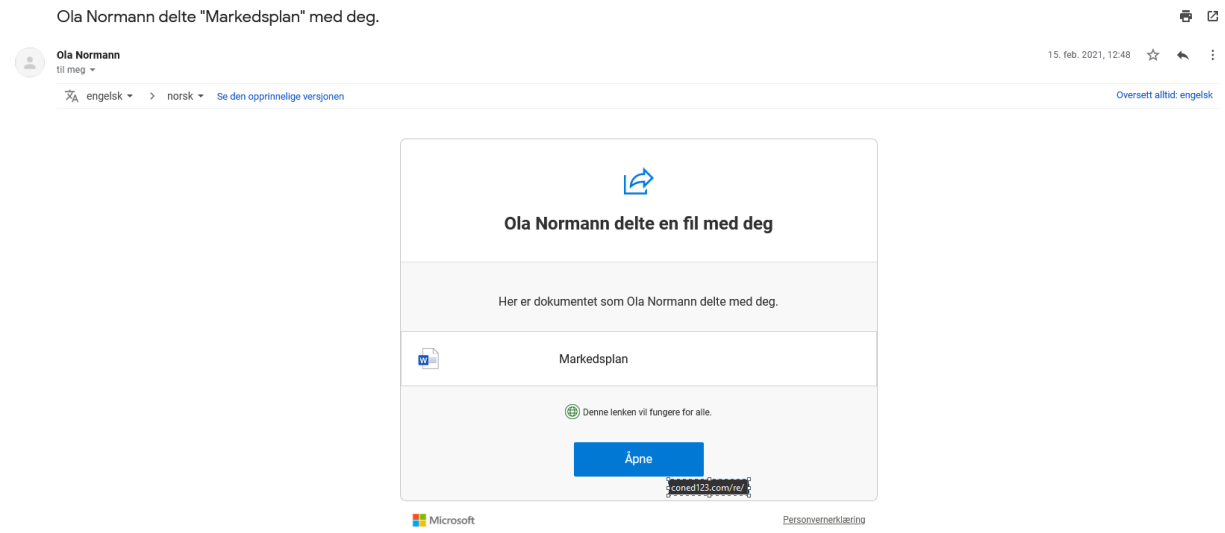
14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema



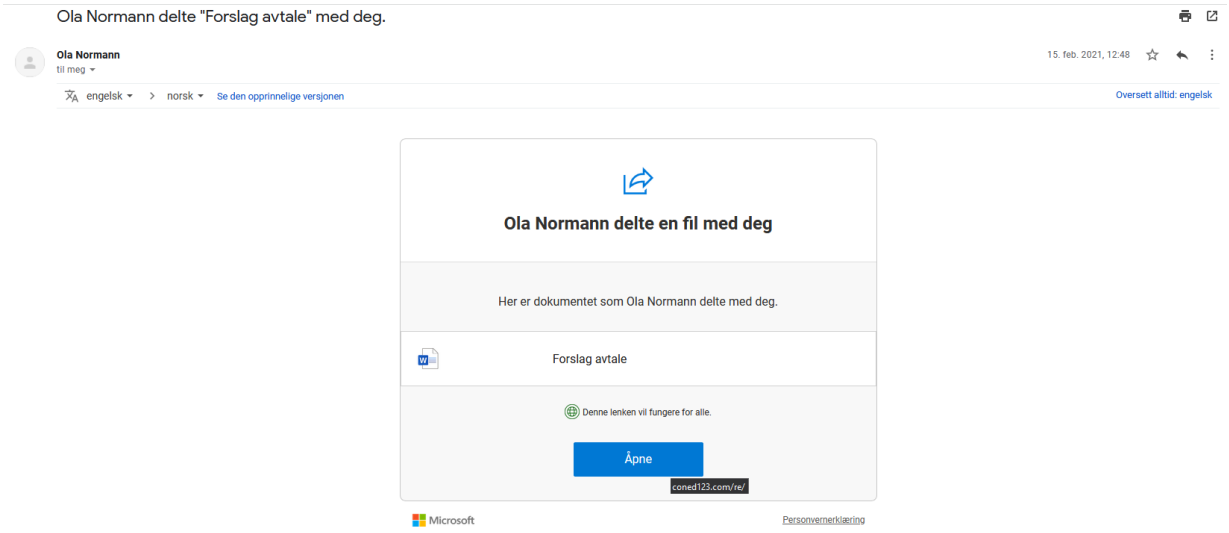
Dette elementet vises kun dersom alternativet «Markedsføring/kommunikasjon, salg og tjenestelevering» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»



Dette elementet vises kun dersom alternativet «Kundeservice» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»



Dette elementet vises kun dersom alternativet «Kundeservice» er valgt i spørsmålet «Hvilket felt jobber du innenfor?»

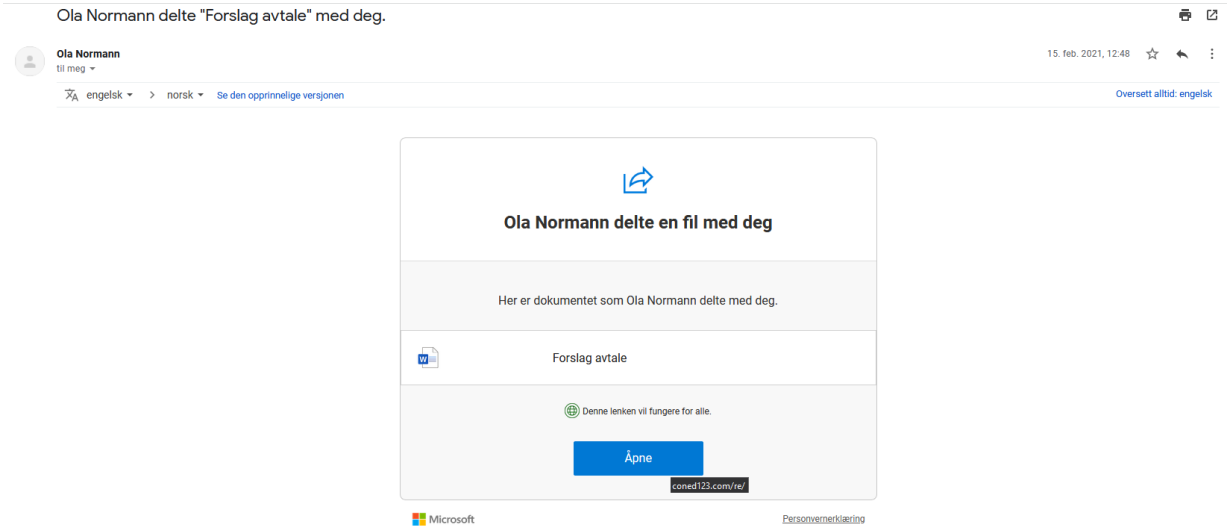


Hva tror du er mest sannsynlig at din kollega vil tenke og/eller gjøre? *

Her kan du krysse av flere alternativ

- [ ] Han er redd for negative konsekvenser fra andre ved å si i fra
- [ ] Han synes det er flaut/ubehagelig å si i fra

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema



Hva tror du er mest sannsynlig at din kollega vil tenke og/eller gjøre? *

Her kan du krysse av flere alternativ

- [ ] Han er redd for negative konsekvenser fra andre ved å si i fra
- [ ] Han synes det er flaut/ubehagelig å si i fra

- [ ] Gjør ingenting, dette er ikke dataangrep
- [ ] Gjør ingenting, hvis det er dataangrep sier IT ifra
- [ ] Tenker at skaden er skjedd og det hjelper ikke å melde i fra
- [ ] Han skjønner ikke at det er et dataangrep
- [ ] Ingenting, sier ikke ifra til noen
- [ ] Bytter passord og brukernavn
- [ ] Sletter filen og restarter datamaskinen
- [ ] Diskuterer det med en kollega
- [ ] Han sier i fra til nærmeste leder
- [ ] Han melder inn hendelsen i rapporteringssystem
- [ ] Sier ifra til ansvarlig for IT-systemet (e-post/Office)
- [ ] Annet

Hvis annet, beskriv *

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hva tror du er mest sannsynlig at din kollega vil tenke og/eller gjøre?»

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

- [ ] Gjør ingenting, dette er ikke dataangrep
- [ ] Gjør ingenting, hvis det er dataangrep sier IT ifra
- [ ] Tenker at skaden er skjedd og det hjelper ikke å melde i fra
- [ ] Han skjønner ikke at det er et dataangrep
- [ ] Ingenting, sier ikke ifra til noen
- [ ] Bytter passord og brukernavn
- [ ] Sletter filen og restarter datamaskinen
- [ ] Diskuterer det med en kollega
- [ ] Han sier i fra til nærmeste leder
- [ ] Han melder inn hendelsen i rapporteringssystem
- [ ] Sier ifra til ansvarlig for IT-systemet (e-post/Office)
- [ ] Annet

Hvis annet, beskriv *

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hva tror du er mest sannsynlig at din kollega vil tenke og/eller gjøre?»

https://nettskjema.no/user/form/preview.html?id=184450#/ 13/40

Hva tenker du om din kollega som lastet ned dokumentet? *

Her kan du krysse av flere alternativ

- [ ] Han er lite kompetent og mangler kunnskap, her burde han skjønt at det var et dataangrep
- [ ] Han har god kunnskap og kompetanse om dette, og det er mest sannsynlig ikke er et dataangrep
- [ ] Hvem som helst ville gjort det samme i samme situasjon
- [ ] Han gjorde det med vilje
- [ ] Han har bare gode intensjoner og det var et uhell
- [ ] Han tar ikke dataangrep seriøst
- [ ] Jeg tenker ikke noe spesielt
- [ ] Annet

Hvis annet, beskriv *

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Hva tenker du om din kollega som lastet ned dokumentet? *

Her kan du krysse av flere alternativ

- [ ] Han er lite kompetent og mangler kunnskap, her burde han skjønt at det var et dataangrep
- [ ] Han har god kunnskap og kompetanse om dette, og det er mest sannsynlig ikke er et dataangrep
- [ ] Hvem som helst ville gjort det samme i samme situasjon
- [ ] Han gjorde det med vilje
- [ ] Han har bare gode intensjoner og det var et uhell
- [ ] Han tar ikke dataangrep seriøst
- [ ] Jeg tenker ikke noe spesielt
- [ ] Annet

Hvis annet, beskriv *

https://nettskjema.no/user/form/preview.html?id=184450#/ 14/40

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hva tenker du om din kollega som lastet ned dokumentet?»

Sideskift

Side 4

Obligatoriske felter er merket med denne stjernen *

Fortsettelse av scenario

Din kollega valgte å melde i fra til sin nærmeste leder, og det viste seg at dette faktisk var et dataangrep. Hendelsen fikk negative konsekvenser for deres virksomhet i form av informasjon på avveie, at selskapet sitt navn ble benyttet for nye angrep og tap av arbeidstid.

Hvilke konsekvenser tror du det fikk for ham å melde i fra til leder? *

Konsekvensene kan være både umiddelbare og mer langsiktige. Her kan du krysse av flere alternativ

- [ ] Negative konsekvenser slik som kjeft og uthenging
- [ ] Tap av tillit fra leder til kollega

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hva tenker du om din kollega som lastet ned dokumentet?»

Sideskift

Side 4

Obligatoriske felter er merket med denne stjernen *

Fortsettelse av scenario

Din kollega valgte å melde i fra til sin nærmeste leder, og det viste seg at dette faktisk var et dataangrep. Hendelsen fikk negative konsekvenser for deres virksomhet i form av informasjon på avveie, at selskapet sitt navn ble benyttet for nye angrep og tap av arbeidstid.

Hvilke konsekvenser tror du det fikk for ham å melde i fra til leder? *

Konsekvensene kan være både umiddelbare og mer langsiktige. Her kan du krysse av flere alternativ

- [ ] Negative konsekvenser slik som kjeft og uthenging
- [ ] Tap av tillit fra leder til kollega

https://nettskjema.no/user/form/preview.html?id=184450#/ 15/40

- [ ] Han mister jobben
- [ ] Ingen konsekvenser
- [ ] Positive konsekvenser slik som ros, omtalt som forbilde
- [ ] Han får økt tillit fra leder
- [ ] Han får mer ansvar
- [ ] Annet

Hvis annet, beskriv *

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvilke konsekvenser tror du det fikk for ham å melde i fra til leder?»

Hvilke reaksjoner får han fra andre kolleger? *

Her kan du krysse av flere alternativ

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

- [ ] Han mister jobben
- [ ] Ingen konsekvenser
- [ ] Positive konsekvenser slik som ros, omtalt som forbilde
- [ ] Han får økt tillit fra leder
- [ ] Han får mer ansvar
- [ ] Annet

Hvis annet, beskriv *

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvilke konsekvenser tror du det fikk for ham å melde i fra til leder?»

Hvilke reaksjoner får han fra andre kolleger? *

Her kan du krysse av flere alternativ

https://nettskjema.no/user/form/preview.html?id=184450#/ 16/40

- [ ] De viser støtte og forståelse
- [ ] Baksnakking og utestenging
- [ ] Han blir sett på som forbilde
- [ ] Han blir sett på som naiv eller inkompetent
- [ ] Ingen reaksjon
- [ ] Annet

Hvis annet, beskriv *

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvilke reaksjoner får han fra andre kolleger?»

Sideskift

Obligatoriske felter er merket med denne stjernen *

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

- [ ] De viser støtte og forståelse
- [ ] Baksnakking og utestenging
- [ ] Han blir sett på som forbilde
- [ ] Han blir sett på som naiv eller inkompetent
- [ ] Ingen reaksjon
- [ ] Annet

Hvis annet, beskriv *

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvilke reaksjoner får han fra andre kolleger?»

Sideskift

Side 5

Obligatoriske felter er merket med denne stjernen *

https://nettskjema.no/user/form/preview.html?id=184450#/ 17/40

Kunnskap

Denne delen vil kartlegge om du kjenner til sikkerhetsrutiner, og om du vet hvordan man melder i fra om potensielle dataangrep. Det finnes mange typer dataangrep, men de vanligste er phishing-epost, krypteringsangrep og bedrageri. Under finner du en forklaring på hva disse er.

Phishing-epost

I scenariodelen av denne undersøkelsen så du et eksempel på en spear phishing-epost. Her var det en kjent avsender og relevant innhold. I phishing-eposter blir man ofte bedt om å klikke på en link og deretter oppgi personopplysninger, eller om å laste ned filer.

Krypteringsangrep

Ved et krypteringsangrep blir informasjon i virksomhetens databaser eller IKT systemer gjort utilgjengelig gjennom kryptering, og bedriften må betale for å få dem frigjort. Dette kalles også løsepengevirus.

Bedrageri

Bedrageri refererer til det som kalles direktørsvindel (CEO-fraud). Begrepet brukes om angrep hvor noen utgir seg for å være direktør eller en annen høytstående stilling i virksomheten, og kontakter for eksempel en økonomimedarbeider og ber dem overføre større beløp til deres konto. Ofte uttrykker de også at det haster å få overført pengene.

Sideskift

Obligatoriske felter er merket med denne stjernen *

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Kunnskap

Denne delen vil kartlegge om du kjenner til sikkerhetsrutiner, og om du vet hvordan man melder i fra om potensielle dataangrep. Det finnes mange typer dataangrep, men de vanligste er phishing-epost, krypteringsangrep og bedrageri. Under finner du en forklaring på hva disse er.

Phishing-epost

I scenariodelen av denne undersøkelsen så du et eksempel på en spear phishing-epost. Her var det en kjent avsender og relevant innhold. I phishing-eposter blir man ofte bedt om å klikke på en link og deretter oppgi personopplysninger, eller om å laste ned filer.

Krypteringsangrep

Ved et krypteringsangrep blir informasjon i virksomhetens databaser eller IKT systemer gjort utilgjengelig gjennom kryptering, og bedriften må betale for å få dem frigjort. Dette kalles også løsepengevirus.

Bedrageri

Bedrageri refererer til det som kalles direktørsvindel (CEO-fraud). Begrepet brukes om angrep hvor noen utgir seg for å være direktør eller en annen høytstående stilling i virksomheten, og kontakter for eksempel en økonomimedarbeider og ber dem overføre større beløp til deres konto. Ofte uttrykker de også at det haster å få overført pengene.

Sideskift

Side 6

Obligatoriske felter er merket med denne stjernen *

https://nettskjema.no/user/form/preview.html?id=184450#/ 18/40

Vet du hvordan du skal si ifra om du blir utsatt for et dataangrep? *

- ◯ Ja
- ◯ Nei

Har din arbeidsplass et rapporteringssystem eller noen som er ansvarlig for å motta meldinger om dataangrep? *

- ◯ Ja
- ◯ Nei
- ◯ Vet ikke

Har din arbeidsplass rutiner for å sikre at ansatte følger lover, forskrifter eller standarder for informasjonssikkerhet? *

For eksempel eForvaltningsforskriften § 15, beredskapsforskriften, offentlighetsloven, GDPR eller ISO27000-serien.

- ◯ Ja
- ◯ Nei
- ◯ Vet ikke

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Vet du hvordan du skal si ifra om du blir utsatt for et dataangrep? *

- ◯ Ja
- ◯ Nei

Har din arbeidsplass et rapporteringssystem eller noen som er ansvarlig for å motta meldinger om dataangrep? *

- ◯ Ja
- ◯ Nei
- ◯ Vet ikke

Har din arbeidsplass rutiner for å sikre at ansatte følger lover, forskrifter eller standarder for informasjonssikkerhet? *

For eksempel eForvaltningsforskriften § 15, beredskapsforskriften, offentlighetsloven, GDPR eller ISO27000-serien.

- ◯ Ja
- ◯ Nei
- ◯ Vet ikke

https://nettskjema.no/user/form/preview.html?id=184450#/ 19/40

Har din arbeidsplass rutiner for digital sikkerhet og hendelseshåndteringsplaner? *

For eksempel rutiner for bytting av passord, oppdatering av programvare, oppbevaring av utstyr og lagring av data.

- ◯ Ja
- ◯ Nei
- ◯ Vet ikke

Gjennomføres det opplæring og kursing om informasjonssikkerhet på din arbeidsplass? *

- ◯ Ja
- ◯ Nei
- ◯ Vet ikke

Har du deltatt på opplæring innenfor informasjonssikkerhet på din nåværende arbeidsplass? *

- ◯ Ja
- ◯ Nei
- ◯ Ikke aktuelt

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Har din arbeidsplass rutiner for digital sikkerhet og hendelseshåndteringsplaner? *

For eksempel rutiner for bytting av passord, oppdatering av programvare, oppbevaring av utstyr og lagring av data.

- ◯ Ja
- ◯ Nei
- ◯ Vet ikke

Gjennomføres det opplæring og kursing om informasjonssikkerhet på din arbeidsplass? *

- ◯ Ja
- ◯ Nei
- ◯ Vet ikke

Har du deltatt på opplæring innenfor informasjonssikkerhet på din nåværende arbeidsplass? *

- ◯ Ja
- ◯ Nei
- ◯ Ikke aktuelt

https://nettskjema.no/user/form/preview.html?id=184450#/ 20/40

Påstander kunnskap

Her kommer en rekke påstander knyttet til kunnskap om informasjonssikkerhet ved din arbeidsplass. Kryss av for hvor enig eller uenig du er i hver enkelt påstand.

	1 Helt uenig	2	3	4	5 Helt enig
Ansatte ved min arbeidsplass har god kjennskap til rutiner for informasjonssikkerhet *	○	○	○	○	○
En gjennomsnittlig kollega ved min arbeidsplass ville ikke oppdaget et mulig dataangrep *	○	○	○	○	○
Vi mangler systemer og verktøy for å melde i fra om dataangrep *	○	○	○	○	○
Jeg kjenner igjen et forsøk på dataangrep når jeg ser det *	○	○	○	○	○
En gjennomsnittlig ansatt ved min arbeidsplass vet hva som skal meldes i fra om *	○	○	○	○	○
Det legges ikke vekt på datasikkerhet på min arbeidsplass *	○	○	○	○	○

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Påstander kunnskap

Her kommer en rekke påstander knyttet til kunnskap om informasjonssikkerhet ved din arbeidsplass. Kryss av for hvor enig eller uenig du er i hver enkelt påstand.

	1 Helt uenig	2	3	4	5 Helt enig
Ansatte ved min arbeidsplass har god kjennskap til rutiner for informasjonssikkerhet *	○	○	○	○	○
En gjennomsnittlig kollega ved min arbeidsplass ville ikke oppdaget et mulig dataangrep *	○	○	○	○	○
Vi mangler systemer og verktøy for å melde i fra om dataangrep *	○	○	○	○	○
Jeg kjenner igjen et forsøk på dataangrep når jeg ser det *	○	○	○	○	○
En gjennomsnittlig ansatt ved min arbeidsplass vet hva som skal meldes i fra om *	○	○	○	○	○
Det legges ikke vekt på datasikkerhet på min arbeidsplass *	○	○	○	○	○

https://nettskjema.no/user/form/preview.html?id=184450#/ 21/40

Mine medarbeidere følger alltid rutiner for informasjonssikkerhet *

Sideskift

Side 7

Obligatoriske felter er merket med denne stjernen *

Hendelser

Denne delen handler om informasjonssikkerhetshendelser og fokuserer på dataangrep.

Både forsøk på dataangrep som ble avverget og «vellykkede» dataangrep med store konsekvenser telles som dataangrep.

Baser svarene dine på tiden du har tilbrakt på din nåværerende arbeidsplass, med mindre noe annet blir spesifisert.

Har din virksomhet blitt utsatt for dataangrep? *

For eksempel phishing-epost, løsepengevirus, bedrageri. Både vellykkede og mislykkede angrep regnes med

- Ja
- Nei

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Mine medarbeidere følger alltid rutiner for informasjonssikkerhet *

Sideskift

Side 7

Obligatoriske felter er merket med denne stjernen *

Hendelser

Denne delen handler om informasjonssikkerhetshendelser og fokuserer på dataangrep.

Både forsøk på dataangrep som ble avverget og «vellykkede» dataangrep med store konsekvenser telles som dataangrep.

Baser svarene dine på tiden du har tilbrakt på din nåværerende arbeidsplass, med mindre noe annet blir spesifisert.

Har din virksomhet blitt utsatt for dataangrep? *

For eksempel phishing-epost, løsepengevirus, bedrageri. Både vellykkede og mislykkede angrep regnes med

- Ja
- Nei

https://nettskjema.no/user/form/preview.html?id=184450#/ 22/40

- ○ Vet ikke

Ble hendelsen(e) rapportert til noen av de følgende? *

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har din virksomhet blitt utsatt for dataangrep?»

Her kan du krysse av for flere alternativ

- ☐ Administrator av det aktuelle tekniske systemet
- ☐ Antivirusleverandør
- ☐ Politiet
- ☐ Andre myndighetsorganer
- ☐ Bank eller kredittkortselskap
- ☐ ISP (nett- og tjenesteleverandører)
- ☐ Sektor CERT eller lignende
- ☐ NorCERT

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

- ○ Vet ikke

Ble hendelsen(e) rapportert til noen av de følgende? *

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har din virksomhet blitt utsatt for dataangrep?»

Her kan du krysse av for flere alternativ

- ☐ Administrator av det aktuelle tekniske systemet
- ☐ Antivirusleverandør
- ☐ Politiet
- ☐ Andre myndighetsorganer
- ☐ Bank eller kredittkortselskap
- ☐ ISP (nett- og tjenesteleverandører)
- ☐ Sektor CERT eller lignende
- ☐ NorCERT

https://nettskjema.no/user/form/preview.html?id=184450#/ 23/40

- [ ] Vet ikke
- [ ] Ikke aktuelt

Hvor ofte blir din arbeidsplass utsatt for dataangrep? *

For eksempel phishing-epost, løsepengevirus, bedrageri. Både vellykkede og mislykkede angrep regnes med.

- ◯ Daglig
- ◯ Ukentlig
- ◯ Månedlig
- ◯ Årlig
- ◯ Aldri
- ◯ Vet ikke

Har du vært utsatt for dataangrep i tilknytning til arbeidsplassen din? *

Kryss av selv om angrepet ble avverget

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

- [ ] Vet ikke
- [ ] Ikke aktuelt

Hvor ofte blir din arbeidsplass utsatt for dataangrep? *

For eksempel phishing-epost, løsepengevirus, bedrageri. Både vellykkede og mislykkede angrep regnes med.

- ◯ Daglig
- ◯ Ukentlig
- ◯ Månedlig
- ◯ Årlig
- ◯ Aldri
- ◯ Vet ikke

Har du vært utsatt for dataangrep i tilknytning til arbeidsplassen din? *

Kryss av selv om angrepet ble avverget

https://nettskjema.no/user/form/preview.html?id=184450#/ 24/40

- ○ Ja
- ○ Nei
- ○ Vet ikke

Hvordan fikk du vite at du hadde blitt utsatt for dataangrep? *

ⓘ Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du vært utsatt for dataangrep i tilknytning til arbeidsplassen din?»

Har det skjedd flere ganger, kan du krysse av flere alternativ

- ☐ Melding fra IT-system
- ☐ Kollega sa i fra
- ☐ Jeg oppdaget det selv
- ☐ Leder sa i fra
- ☐ IT-avdeling sa i fra
- ☐ Annet

Hvis annet, beskriv *

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

- ○ Ja
- ○ Nei
- ○ Vet ikke

Hvordan fikk du vite at du hadde blitt utsatt for dataangrep? *

ⓘ Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du vært utsatt for dataangrep i tilknytning til arbeidsplassen din?»

Har det skjedd flere ganger, kan du krysse av flere alternativ

- ☐ Melding fra IT-system
- ☐ Kollega sa i fra
- ☐ Jeg oppdaget det selv
- ☐ Leder sa i fra
- ☐ IT-avdeling sa i fra
- ☐ Annet

Hvis annet, beskriv *

https://nettskjema.no/user/form/preview.html?id=184450#/ 25/40

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvordan fikk du vite at du hadde blitt utsatt for dataangrep?»

Hvilken type dataangrep ble du utsatt for? *

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du vært utsatt for dataangrep i tilknytning til arbeidsplassen din?»

Om det har skjedd flere ganger kan du krysse av flere alternativ

- [ ] Phishing-epost
- [ ] Krypteringsangrep (løsepengevirus)
- [ ] Bedrageri (direktørsvindel)
- [ ] Datainnbrudd/hacking
- [ ] Annet

Meldte du i fra om at angrepet hadde skjedd? *

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvordan fikk du vite at du hadde blitt utsatt for dataangrep?»

Hvilken type dataangrep ble du utsatt for? *

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du vært utsatt for dataangrep i tilknytning til arbeidsplassen din?»

Om det har skjedd flere ganger kan du krysse av flere alternativ

- [ ] Phishing-epost
- [ ] Krypteringsangrep (løsepengevirus)
- [ ] Bedrageri (direktørsvindel)
- [ ] Datainnbrudd/hacking
- [ ] Annet

Meldte du i fra om at angrepet hadde skjedd? *

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du

https://nettskjema.no/user/form/preview.html?id=184450#/ 26/40

vært utsatt for dataangrep i tilknytning til arbeidsplassen din?»

Om det har skjedd flere ganger, svar for siste hendelse

- ○ Nei
- ○ Ja
- ○ Ikke aktuelt

Hvorfor var det ikke aktuelt å melde i fra? *

ⓘ Dette elementet vises kun dersom alternativet «Nei» eller «Ikke aktuelt» er valgt i spørsmålet «Meldte du i fra om at angrepet hadde skjedd?»

Her kan du krysse av flere alternativ

- ☐ IT-system meldte automatisk i fra
- ☐ IT-avdeling/den ansvarlige person ble varslet automatisk
- ☐ Det hadde ingen hensikt, angrepet hadde allerede skjedd
- ☐ Jeg visste ikke at jeg hadde blitt utsatt for dataangrep
- ☐ Det fantes ingen å melde i fra til

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

vært utsatt for dataangrep i tilknytning til arbeidsplassen din?»

Om det har skjedd flere ganger, svar for siste hendelse

- ○ Nei
- ○ Ja
- ○ Ikke aktuelt

Hvorfor var det ikke aktuelt å melde i fra? *

ⓘ Dette elementet vises kun dersom alternativet «Nei» eller «Ikke aktuelt» er valgt i spørsmålet «Meldte du i fra om at angrepet hadde skjedd?»

Her kan du krysse av flere alternativ

- ☐ IT-system meldte automatisk i fra
- ☐ IT-avdeling/den ansvarlige person ble varslet automatisk
- ☐ Det hadde ingen hensikt, angrepet hadde allerede skjedd
- ☐ Jeg visste ikke at jeg hadde blitt utsatt for dataangrep
- ☐ Det fantes ingen å melde i fra til

https://nettskjema.no/user/form/preview.html?id=184450#/ 27/40

- [ ] Jeg visste ikke hvordan jeg skulle melde i fra
- [ ] Jeg var redd for negative reaksjoner fra leder
- [ ] Jeg kunne ikke melde i fra anonymt
- [ ] Jeg var redd for negative reaksjoner fra kolleger
- [ ] Annet

Hvis annet, beskriv *

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvorfor var det ikke aktuelt å melde i fra?»

Hvor lang tid gikk det fra du ble klar over at hendelsen hadde skjedd til du meldte i fra? *

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Meldte du i fra om at angrepet hadde skjedd?»

Om det har skjedd flere ganger, svar for siste hendelse

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

- [ ] Jeg visste ikke hvordan jeg skulle melde i fra
- [ ] Jeg var redd for negative reaksjoner fra leder
- [ ] Jeg kunne ikke melde i fra anonymt
- [ ] Jeg var redd for negative reaksjoner fra kolleger
- [ ] Annet

Hvis annet, beskriv *

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvorfor var det ikke aktuelt å melde i fra?»

Hvor lang tid gikk det fra du ble klar over at hendelsen hadde skjedd til du meldte i fra? *

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Meldte du i fra om at angrepet hadde skjedd?»

Om det har skjedd flere ganger, svar for siste hendelse

https://nettskjema.no/user/form/preview.html?id=184450#/ 28/40

- ◯ Umiddelbart
- ◯ Etter noen timer
- ◯ I løpet av en dag
- ◯ Innen en uke
- ◯ Innen en måned
- ◯ Innen 100 dager
- ◯ Lenger enn 100 dager

Om du hadde blitt utsatt for et dataangrep og det var aktuelt, hadde du meldt i fra? *

Dette elementet vises kun dersom alternativet «Nei» eller «Vet ikke» er valgt i spørsmålet «Har du vært utsatt for dataangrep i tilknytning til arbeidsplassen din?»

- ◯ Nei
- ◯ Ja
- ◯ Vet ikke

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

- ◯ Umiddelbart
- ◯ Etter noen timer
- ◯ I løpet av en dag
- ◯ Innen en uke
- ◯ Innen en måned
- ◯ Innen 100 dager
- ◯ Lenger enn 100 dager

Om du hadde blitt utsatt for et dataangrep og det var aktuelt, hadde du meldt i fra? *

Dette elementet vises kun dersom alternativet «Nei» eller «Vet ikke» er valgt i spørsmålet «Har du vært utsatt for dataangrep i tilknytning til arbeidsplassen din?»

- ◯ Nei
- ◯ Ja
- ◯ Vet ikke

https://nettskjema.no/user/form/preview.html?id=184450#/ 29/40

Hvorfor ville du ikke, eller vet du ikke om du ville, meldt i fra? *

Dette elementet vises kun dersom alternativet «Nei» eller «Vet ikke» er valgt i spørsmålet «Om du hadde blitt utsatt for et dataangrep og det var aktuelt, hadde du meldt i fra?»

Her kan du krysse av flere alternativ

- [ ] IT-systemet melder i fra automatisk
- [ ] IT-avdeling/den ansvarlige personen blir varslet automatisk
- [ ] Det finnes ingen å melde i fra til
- [ ] Jeg ville ikke visst at jeg hadde blitt utsatt for et dataangrep
- [ ] Jeg vet ikke hvordan jeg melder i fra
- [ ] Jeg har ikke mulighet til å melde i fra anonymt
- [ ] Det har ingen hensikt, angrepet har allerede skjedd
- [ ] Jeg er redd for negative reaksjoner fra leder
- [ ] Jeg er redd for negative reaksjoner fra kolleger
- [ ] Annet

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Hvorfor ville du ikke, eller vet du ikke om du ville, meldt i fra? *

Dette elementet vises kun dersom alternativet «Nei» eller «Vet ikke» er valgt i spørsmålet «Om du hadde blitt utsatt for et dataangrep og det var aktuelt, hadde du meldt i fra?»

Her kan du krysse av flere alternativ

- [ ] IT-systemet melder i fra automatisk
- [ ] IT-avdeling/den ansvarlige personen blir varslet automatisk
- [ ] Det finnes ingen å melde i fra til
- [ ] Jeg ville ikke visst at jeg hadde blitt utsatt for et dataangrep
- [ ] Jeg vet ikke hvordan jeg melder i fra
- [ ] Jeg har ikke mulighet til å melde i fra anonymt
- [ ] Det har ingen hensikt, angrepet har allerede skjedd
- [ ] Jeg er redd for negative reaksjoner fra leder
- [ ] Jeg er redd for negative reaksjoner fra kolleger
- [ ] Annet

https://nettskjema.no/user/form/preview.html?id=184450#/ 30/40

Hvis annet, beskriv *

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvorfor ville du ikke, eller vet du ikke om du ville, meldt i fra?»

Påstander hendelser

Her er noen påstander knyttet til informasjonssikkerhet og det å melde i fra om hendelser ved din arbeidsplass. Kryss av for hvor enig eller uenig du er i hver enkelt påstand.

	1 Helt uenig	2	3	4	5 Helt enig
Det er umulig å vite hva man skal melde i fra om *	○	○	○	○	○
Jeg kommer ikke til å bli utsatt for dataangrep på min arbeidsplass *	○	○	○	○	○
Våre rutiner for å melde i fra om dataangrep er tungvinte og kompliserte *	○	○	○	○	○
Mine kolleger melder ikke ifra om dataangrep *	○	○	○	○	○

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Hvis annet, beskriv *

Dette elementet vises kun dersom alternativet «Annet» er valgt i spørsmålet «Hvorfor ville du ikke, eller vet du ikke om du ville, meldt i fra?»

Påstander hendelser

Her er noen påstander knyttet til informasjonssikkerhet og det å melde i fra om hendelser ved din arbeidsplass. Kryss av for hvor enig eller uenig du er i hver enkelt påstand.

	1 Helt uenig	2	3	4	5 Helt enig
Det er umulig å vite hva man skal melde i fra om *	○	○	○	○	○
Jeg kommer ikke til å bli utsatt for dataangrep på min arbeidsplass *	○	○	○	○	○
Våre rutiner for å melde i fra om dataangrep er tungvinte og kompliserte *	○	○	○	○	○
Mine kolleger melder ikke ifra om dataangrep *	○	○	○	○	○

https://nettskjema.no/user/form/preview.html?id=184450#/ 31/40

Om min arbeidsplass utsettes for dataangrep vil vi ha full kontroll over situasjonen *	○	○	○	○	○
Det er uunngåelig å bli utsatt for dataangrep *	○	○	○	○	○
Å melde i fra om et dataangrep som allerede har skjedd påvirker ikke utfallet av det *	○	○	○	○	○
Hvem som blir utsatt for dataangrep er helt tilfeldig *	○	○	○	○	○

Sideskift

Side 8

Obligatoriske felter er merket med denne stjernen *

Konsekvenser

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Om min arbeidsplass utsettes for dataangrep vil vi ha full kontroll over situasjonen *
Det er uunngåelig å bli utsatt for dataangrep *
Å melde i fra om et dataangrep som allerede har skjedd påvirker ikke utfallet av det *
Hvem som blir utsatt for dataangrep er helt tilfeldig *

Sideskift

Side 8

Obligatoriske felter er merket med denne stjernen *

Konsekvenser

https://nettskjema.no/user/form/preview.html?id=184450#/ 32/40

Denne delen inneholder spørsmål og påstander knyttet til dataangrep og hvilke konsekvenser det har å melde i fra for enkeltindivider, altså ikke virksomheten som helhet.
Konsekvensene kan være både positive og negative.

Du skal nå svare på spørsmål og påstander om hvilke konsekvenser du har opplevd, eller hvilke du tror er sannsynlig å oppleve, for deg og dine kolleger i virksomheten.

Da du meldte i fra om hendelsen(e), hvilke konsekvenser fikk det for deg? *

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Meldte du i fra om at angrepet hadde skjedd?»

Her kan du krysse av flere alternativ

- [ ] Positiv tilbakemelding fra kolleger
- [ ] Negativ tilbakemelding fra kolleger
- [ ] Positiv tilbakemelding fra leder
- [ ] Negativ tilbakemelding fra leder
- [ ] Positive tanker om meg selv (eks. stolt av å varsle ifra)
- [ ] Negative tanker om meg selv (eks. flau, følte meg dum)
- [ ] Ingen konsekvenser

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Denne delen inneholder spørsmål og påstander knyttet til dataangrep og hvilke konsekvenser det har å melde i fra for enkeltindivider, altså ikke virksomheten som helhet.
Konsekvensene kan være både positive og negative.

Du skal nå svare på spørsmål og påstander om hvilke konsekvenser du har opplevd, eller hvilke du tror er sannsynlig å oppleve, for deg og dine kolleger i virksomheten.

Da du meldte i fra om hendelsen(e), hvilke konsekvenser fikk det for deg? *

Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Meldte du i fra om at angrepet hadde skjedd?»

Her kan du krysse av flere alternativ

- [ ] Positiv tilbakemelding fra kolleger
- [ ] Negativ tilbakemelding fra kolleger
- [ ] Positiv tilbakemelding fra leder
- [ ] Negativ tilbakemelding fra leder
- [ ] Positive tanker om meg selv (eks. stolt av å varsle ifra)
- [ ] Negative tanker om meg selv (eks. flau, følte meg dum)
- [ ] Ingen konsekvenser

https://nettskjema.no/user/form/preview.html?id=184450#/ 33/40

Hvis du hadde meldt i fra da du ble utsatt for dataangrepet, hvilke konsekvenser er det sannsynlig at du ville fått? *

Dette elementet vises kun dersom alternativet «Nei» eller «Ikke aktuelt» er valgt i spørsmålet «Meldte du i fra om at angrepet hadde skjedd?»

Her kan du krysse av for flere alternativ

- [ ] Positiv tilbakemelding fra kolleger
- [ ] Negativ tilbakemelding fra kolleger
- [ ] Positiv tilbakemelding fra leder
- [ ] Negativ tilbakemelding fra leder
- [ ] Positive tanker om meg selv (eks. stolt av å melde i fra)
- [ ] Negative tanker om meg selv (eks. flau, føler meg dum)
- [ ] Ingen konsekvenser

Hvis du hadde blitt utsatt for et dataangrep og meldt i fra om hendelsen, hvilke konsekvenser er det sannsynlig at du ville fått? *

Dette elementet vises kun dersom alternativet «Nei» eller «Vet ikke» er valgt i

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Hvis du hadde meldt i fra da du ble utsatt for dataangrepet, hvilke konsekvenser er det sannsynlig at du ville fått? *

Dette elementet vises kun dersom alternativet «Nei» eller «Ikke aktuelt» er valgt i spørsmålet «Meldte du i fra om at angrepet hadde skjedd?»

Her kan du krysse av for flere alternativ

- [ ] Positiv tilbakemelding fra kolleger
- [ ] Negativ tilbakemelding fra kolleger
- [ ] Positiv tilbakemelding fra leder
- [ ] Negativ tilbakemelding fra leder
- [ ] Positive tanker om meg selv (eks. stolt av å melde i fra)
- [ ] Negative tanker om meg selv (eks. flau, føler meg dum)
- [ ] Ingen konsekvenser

Hvis du hadde blitt utsatt for et dataangrep og meldt i fra om hendelsen, hvilke konsekvenser er det sannsynlig at du ville fått? *

Dette elementet vises kun dersom alternativet «Nei» eller «Vet ikke» er valgt i

https://nettskjema.no/user/form/preview.html?id=184450#/ 34/40

spørsmålet «Har du vært utsatt for dataangrep i tilknytning til arbeidsplassen din?»

Her kan du krysse av for flere alternativ

- [ ] Positiv tilbakemelding fra kolleger
- [ ] Negativ tilbakemelding fra kolleger
- [ ] Positiv tilbakemelding fra leder
- [ ] Negativ tilbakemelding fra leder
- [ ] Positive tanker om meg selv (eks. stolt av å melde i fra)
- [ ] Negative tanker om meg selv (eks. flau, føler meg dum)
- [ ] Ingen konsekvenser

Påstander konsekvenser

Under kommer en rekke påstander om mulige konsekvenser. Kryss av for i hvilken grad du er enig eller uenig.

	1 Helt uenig	2	3	4	5 Helt enig
Det er flaut å bli utsatt for dataan-	○	○	○	○	○

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

spørsmålet «Har du vært utsatt for dataangrep i tilknytning til arbeidsplassen din?»

Her kan du krysse av for flere alternativ

- [ ] Positiv tilbakemelding fra kolleger
- [ ] Negativ tilbakemelding fra kolleger
- [ ] Positiv tilbakemelding fra leder
- [ ] Negativ tilbakemelding fra leder
- [ ] Positive tanker om meg selv (eks. stolt av å melde i fra)
- [ ] Negative tanker om meg selv (eks. flau, føler meg dum)
- [ ] Ingen konsekvenser

Påstander konsekvenser

Under kommer en rekke påstander om mulige konsekvenser. Kryss av for i hvilken grad du er enig eller uenig.

	1 Helt uenig	2	3	4	5 Helt enig
Det er flaut å bli utsatt for dataan-	○	○	○	○	○

https://nettskjema.no/user/form/preview.html?id=184450#/ 35/40

grep ˆ

Om jeg ikke melder i fra om et dataangrep får jeg negativ tilbakemelding fra kolleger eller leder *	○	○	○	○	○
I min virksomhet oppmuntres man til å melde i fra om dataangrep *	○	○	○	○	○
Jeg mister mestringsfølelse om jeg blir utsatt for dataangrep *	○	○	○	○	○
Jeg får mestringsfølelse av å melde i fra om et (mulig) dataangrep *	○	○	○	○	○
Om jeg melder i fra om et dataangrep får jeg negativ tilbakemelding for at angrepet skjedde i utgangspunktet *	○	○	○	○	○
Om jeg blir utsatt for et dataangrep blir jeg godt ivaretatt av mine kolleger *	○	○	○	○	○

Sideskift

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

grep ˆ

Om jeg ikke melder i fra om et dataangrep får jeg negativ tilbakemelding fra kolleger eller leder *	○	○	○	○	○
I min virksomhet oppmuntres man til å melde i fra om dataangrep *	○	○	○	○	○
Jeg mister mestringsfølelse om jeg blir utsatt for dataangrep *	○	○	○	○	○
Jeg får mestringsfølelse av å melde i fra om et (mulig) dataangrep *	○	○	○	○	○
Om jeg melder i fra om et dataangrep får jeg negativ tilbakemelding for at angrepet skjedde i utgangspunktet *	○	○	○	○	○
Om jeg blir utsatt for et dataangrep blir jeg godt ivaretatt av mine kolleger *	○	○	○	○	○

Sideskift

https://nettskjema.no/user/form/preview.html?id=184450#/ 36/40

Side 9

Obligatoriske felter er merket med denne stjernen *

Hjemmekontor

COVID-19 har preget samfunnet og arbeidshverdagen til alle, og mange har måttet flytte fra arbeidsplassen til hjemmekontor. Du vil nå få spørsmål knyttet til hjemmekontor og informasjonssikkerhet.

Har du hatt hjemmekontor (i noen som helst utstrekning) siden 12.mars 2020? *

Hyttekontor regnes som hjemmekontor.

- ○ Ja
- ○ Nei

Hvor mange dager i snitt i løpet av en uke har du hatt hjemmekontor det siste året? *

ⓘ Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du hatt hjemmekontor (i noen som helst utstrekning) siden 12.mars 2020?»

Her kan du bruke desimaltall om det er nødvendig

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Side 9

Obligatoriske felter er merket med denne stjernen *

Hjemmekontor

COVID-19 har preget samfunnet og arbeidshverdagen til alle, og mange har måttet flytte fra arbeidsplassen til hjemmekontor. Du vil nå få spørsmål knyttet til hjemmekontor og informasjonssikkerhet.

Har du hatt hjemmekontor (i noen som helst utstrekning) siden 12.mars 2020? *

Hyttekontor regnes som hjemmekontor.

- ○ Ja
- ○ Nei

Hvor mange dager i snitt i løpet av en uke har du hatt hjemmekontor det siste året? *

ⓘ Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du hatt hjemmekontor (i noen som helst utstrekning) siden 12.mars 2020?»

Her kan du bruke desimaltall om det er nødvendig

https://nettskjema.no/user/form/preview.html?id=184450#/ 37/40

Har du fått informasjon om hvordan man kan ivareta informasjonssikkerhet på hjemmekontor? *

- ◯ Ja
- ◯ Nei
- ◯ Vet ikke

Har du formidlet informasjon om hvordan man kan ivareta informasjonssikkerhet på hjemmekontor til ansatte i din virksomhet? *

- ◯ Ja
- ◯ Nei

Har du opplevd dataangrep etter du begynte med hjemmekontor det siste året? *

ⓘ Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du hatt hjemmekontor (i noen som helst utstrekning) siden 12.mars 2020?»

- ◯ Ja
- ◯ Nei

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

Har du fått informasjon om hvordan man kan ivareta informasjonssikkerhet på hjemmekontor? *

- ◯ Ja
- ◯ Nei
- ◯ Vet ikke

Har du formidlet informasjon om hvordan man kan ivareta informasjonssikkerhet på hjemmekontor til ansatte i din virksomhet? *

- ◯ Ja
- ◯ Nei

Har du opplevd dataangrep etter du begynte med hjemmekontor det siste året? *

ⓘ Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du hatt hjemmekontor (i noen som helst utstrekning) siden 12.mars 2020?»

- ◯ Ja
- ◯ Nei

https://nettskjema.no/user/form/preview.html?id=184450#/ 38/40

- ○ Vet ikke

Hvordan opplever du, eller ville du opplevd, å melde i fra om dataangrep fra hjemmekontor i motsetning til ordinært kontor? *

- ○ Vanskeligere, vet ikke hvordan jeg melder i fra på hjemmekontor
- ○ Lettere, trenger ikke si det ansikt til ansikt
- ○ Ingen forskjell fra vanlig kontor
- ○ Lettere, oppdager dataangrep lettere
- ○ Vanskeligere, fordi jeg ikke oppdager dataangrep like lett

ⓘ Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du hatt hjemmekontor (i noen som helst utstrekning) siden 12.mars 2020?»

Påstander hjemmekontor

	1 Helt uenig	2	3	4	5 Helt enig
Jeg opplever hjemmekontor like trygt som min ordinære arbeids-	○	○	○	○	○

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

- ○ Vet ikke

Hvordan opplever du, eller ville du opplevd, å melde i fra om dataangrep fra hjemmekontor i motsetning til ordinært kontor? *

- ○ Vanskeligere, vet ikke hvordan jeg melder i fra på hjemmekontor
- ○ Lettere, trenger ikke si det ansikt til ansikt
- ○ Ingen forskjell fra vanlig kontor
- ○ Lettere, oppdager dataangrep lettere
- ○ Vanskeligere, fordi jeg ikke oppdager dataangrep like lett

ⓘ Dette elementet vises kun dersom alternativet «Ja» er valgt i spørsmålet «Har du hatt hjemmekontor (i noen som helst utstrekning) siden 12.mars 2020?»

Påstander hjemmekontor

	1 Helt uenig	2	3	4	5 Helt enig
Jeg opplever hjemmekontor like trygt som min ordinære arbeids-	○	○	○	○	○

https://nettskjema.no/user/form/preview.html?id=184450#/ 39/40

plass *

Jeg har ikke det tekniske utstyret til å ivareta informasjonssikkerhet på hjemmekontor *	○	○	○	○	○
På hjemmekontor er sannsynligheten for å bli utsatt for dataangrep mindre enn ordinært kontor *	○	○	○	○	○
Mitt hjemmekontor er mer utsatt for dataangrep enn mitt ordinære kontor *	○	○	○	○	○

Husk å trykk "send" når du er ferdig med besvarelsen.

Se nylige endringer i Nettskjema

14.6.2021 Spørreundersøkelse Informasjonssikkerhet – Vis - Nettskjema

plass *

Jeg har ikke det tekniske utstyret til å ivareta informasjonssikkerhet på hjemmekontor *	○	○	○	○	○
På hjemmekontor er sannsynligheten for å bli utsatt for dataangrep mindre enn ordinært kontor *	○	○	○	○	○
Mitt hjemmekontor er mer utsatt for dataangrep enn mitt ordinære kontor *	○	○	○	○	○

Husk å trykk "send" når du er ferdig med besvarelsen.

Se nylige endringer i Nettskjema

https://nettskjema.no/user/form/preview.html?id=184450#/ 40/40