NORDMENN OG DIGITAL SIKKERHETSKULTUR

2018

NorSIS

Norsk senter for informasjonssikring

Ansvarlig: Peggy Heie Sandbekken
Forfattere: Bjarte Malmedal (metode og analyse) og Hanne Eggen Røislien (metode)
Design: Sigve Ekseth Lundsaunet
Informasjonsgrafikk: Mie Kristensen

ISBN: 978-82-93651-02-4

Rapporten er støttet av Justis- og beredskapsdepartementet
Data er innhentet av YouGov

NORDMENN OG DIGITAL SIKKERHETSKULTUR

INNHOLD

Innledning **6**

Metode **8**
Analyse 8

Den norske digitale sikkerhetskulturen **10**
Grunnleggende faktorer 12
Fellesskap 16
Styring og kontroll 20
Tillit 24
Risiko-oppfattelse 28
Optimisme for teknologi og digitalisering 34
Kompetanse 36
Interesse for teknologi og IT 40
Adferdsmønstre 42

Konklusjon **48**

INNLEDNING

DET NORSKE SAMFUNNET BLIR STADIG MER DIGITALISERT. Tidligere manuelle oppgaver og prosesser blir digitalisert, og de digitale tjenestene knyttes hele tiden tettere sammen i nye og komplekse strukturer. Tradisjonelt har nok mange sett på disse nye strukturene som rene teknologiske strukturer. Sammenkoblinger av systemer, tjenester, infrastrukturer og enheter. Det har vært mange trusler mot de digitale strukturene, men helt siden *«Morris-ormen»* så sitt lys i 1988, har man i hovedsak snakket om de teknologiske truslene, og de teknologiske konsekvensene.

Nå som digitaliseringen skjer i hele samfunnet mener NorSIS at vi ikke kan skille mellom teknologien og mennesket. Mennesker har nesten alltid en plass i risiko- og årsakskjedene. I tillegg opplever også menneskene konsekvenser når teknologien brukes til, eller rammes av, kriminelle formål. I tillegg til å utvikle ny kunnskap om hvordan man best skal beskytte teknologien mot digitale trusler, må samfunnet også utvikle ny kunnskap om hvordan mennesket blir mer robust i møtet med teknologi og digitale trusler. Teknologien påvirker samfunnsutviklingen. Dette betyr at teknologien også påvirker den enkelte, men vi vet også at den enkelte kan påvirke digitaliseringen i samfunnet. Dette så vi blant annet i debatten rundt Datalagringsdirektivet for noen år siden. Måten befolkningen engasjerte seg i debatten bidro til å gjøre fordeler og ulemper ved direktivet kjent.

Digital sikkerhetskultur er samfunnets felles verdier, holdninger, normer, kunnskaper og handlinger om det å kunne ta del i et digitalisert samfunn på en trygg måte. Den digitale sikkerhetskulturen skal gjøre både den enkelte, og samfunnet i sin helhet, mer mindre sårbare mot digitale trusler. Dette bidrar til å bygge tillit til de digitale tjenestene slik at samfunnet kan høste alle godene som digitaliseringen kan gi oss.

Det er derfor svært gledelig å se at stadig flere har fokus på digital sikkerhetskultur og på menneskene som bruker digitale tjenester. NorSIS mener at man likevel må være ydmyke for at samfunnet foreløpig ikke vet nok om hvordan utfordringene skal løses. Hjelper det å opplyse de ansatte om trusler og sårbarheter? Hvilke typer opplæring fører til at elever lærer bedre nettvett, og hvilke typer opplæring har minimal effekt? Vil det som fungerer i en bedrift ha samme effekt i andre bedrifter?

NorSIS har siden 2015 kartlagt digital sikkerhetskultur i befolkningen, på skoler og i bedrifter, og vi begynner nå å se hvordan utviklingen er over tid. Dette er svært viktig, for det er kun gjennom en slik kartlegging at en kan oppdage om nøkkel-indikatorer har den utviklingen en ønsker seg. Tillit er en forutsetning for digitaliseringen. Myndighetene må vite om befolkningen har tillit til at opplysningene deres behandles på en trygg måte, og at de får hjelp dersom de blir utsatt for datakriminalitet. En slik kartlegging av befolkningen gir myndighetene en tilbakemelding på om det de gjør for å bygge sikkerhetskultur har ønsket effekt.

Justis- og beredskapsdepartementet jobber med en egen nasjonal strategi for kompetanse innen digital sikkerhet. En del av denne vil omhandle tiltak rettet mot den enkelte innbygger. I årene fremover er det derfor være særdeles viktig å fortsette arbeidet med å kartlegge befolkningens digitale sikkerhetskultur slik at vi kan se om myndighetenes strategier og tiltak har ønsket effekt.

Norske virksomheter innser også at de ansattes digitale sikkerhetskultur har betydning for bedriftens risikobilde. Mange gir opplæring til sine ansatte, og det er på tide at bedriftene også kartlegger effekten av opplæringstiltakene. Hvis effekten uteblir, må de tenke nytt.

I årets rapport ser vi på endringene fra 2015 frem til i dag. På noen områder ser vi endringer, mens på andre områder har det tilsynelatende ikke skjedd noen endringer i løpet av de siste tre årene. Det er likevel ingen grunn til å slå seg til ro med slike funn. Holdningsendringer i samfunnet kan skje sakte, og over mange år. Myndighetene, norske bedrifter og andre som arbeider med digital sikkerhet bør derfor bruke disse resultatene til å evaluere sin egen innsats, og om nødvendig endre kurs.

Vi håper denne rapporten er til nytte for alle som arbeider med digital sikkerhetskultur i Norge.

Rapporten er utarbeidet med støtte fra Justis- og beredskapsdepartementet.

METODE

I vår hovedrapport fra 2016 utviklet NorSIS et konsept for å beskrive digital sikkerhetskultur og en metode for å kartlegge den. Vi henviser til hovedstudien for en utførlig beskrivelse av metoden og det teoretiske grunnlaget for denne.

Denne rapporten baserer seg på data som er innhentet gjennom representative befolkningsundersøkelser utført av YouGov i 2015, 2017 og 2018. Merk at undersøkelsen i 2015 var en befolkningsundersøkelse som YouGov utførte som en del av kvalitetssikringen i prosjektet som ledet frem til hovedstudien i 2016. I etterkant ble enkelte spørsmål endret, fjernet eller lagt til. Alle sammenligninger over tid i denne rapporten gjøres kun for de spørsmål som er like i alle tre undersøkelsene.

Vi benytter en kvalitativ vurdering der flere indikatorer sammen bidrar til en samlet vurdering av de åtte dimensjonene.
I denne rapporten brukes informasjonssikkerhetskultur og digital sikkerhetskultur som synonymer.

ANALYSE

Det er gjennomgående benyttet gjennomsnitt som sentraltendens i analysene. Variablene er stort sett nominale eller ordinale med få responskategorier (færre enn fem). Tallmaterialet i tabellene er testet for signifikans (signifikante avvik). Der er foretatt to forskjellige statistiske tester, Chi2-test og T-test. Det er valgt et konfidensintervall på 95 %.

N=1010.

DEN NORSKE DIGITALE SIKKERHETS-KULTUREN

GRUNNLEGGENDE FAKTORER

KULTUR EN BLANT DE MEST DOMINERENDE FAKTORENE SOM SKILLER NASJONER FRA HVERANDRE. Alle nasjoner har kulturer. Nasjonale kulturer former oss, både hvordan vi er som gruppe og hvordan vi som individer plasserer oss i omgivelsene. Eller sagt på en annen måte: Nasjonale kulturer fungerer som et lim mellom innbyggerne og de er knyttet til våre underliggende verdier, som for eksempel hva vi anser å være normalt versus unormalt, trygt versus utrygt og rasjonelt versus irrasjonelt.

Våre nasjonale kulturer gir oss et sett av verdier som hjelper oss å forstå omgivelsene. De utstyrer oss med et kompass som sier *«hvordan vi gjør ting her»*. Resultatet er at de nasjonale kulturene blir til systemer av delte verdier, meninger og handlingsmønstre. Disse kan variere stort fra nasjon til nasjon. De kulturelle verdiene og normene blir lært tidlig i livet, både gjennom formell utveksling (på skole, i fritidsaktiviteter, på arbeidsplassen etc.) og gjennom uformell sosial interaksjon med venner, foreldre, søsken og andre. Resultatet er at de nasjonale kulturene er dypt forankret i oss, og de varer gjennom generasjoner.

Nasjonale kulturer er selvsagt ikke helt klart definerte, og de kommer ikke som *«one size fits all»*. De består av mange subkulturer, der faktorer som alder, geografi, interesser, kjønn mv. spiller inn. Digital sikkerhetskultur er en slik subkultur, og vi observerer også forskjeller innad i disse, blant annet når en ser på sammenheng med alder eller med ulike bedrifts- og organisasjonskulturer.

«VÅRE NASJONALE KULTURER GIR OSS ET SETT AV VERDIER SOM HJELPER OSS Å FORSTÅ OMGIVELSENE.»

Tidligere ble digitale sikkerhetskulturer utelukkende regnet som en del av organisasjonskulturene, altså noe bedrifter og virksomheter har vært opptatt av. Digital sikkerhetskultur har som et resultat av dette blitt sett på som et verktøy for effektivitet og etterlevelse av regler og krav. På dette området skiller nasjonale kulturer og organisasjonskulturer seg fra hverandre. Nasjonale kulturer er i hovedsak basert på våre felles verdier og normer, mens organisasjonskulturer i hovedsak er basert på felles utførelse av handlinger og oppgaver.

Det finnes flere definisjoner for digital sikkerhetskultur, og selv om det ikke ser ut til å være én definisjon som fagfolk ser ut til å enes om, så omfatter de fleste definisjonene noen nøkkelområder: Det handler om å beskytte informasjonsverdier fra ulike former for trusler som rettes mot innebygde sårbarheter. Digital sikkerhetskultur kan derfor forstås som de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til informasjonsverdier. Digital sikkerhetskultur er derfor et sett med handlingsmønstre, og et sett med idéer, holdninger og kunnskaper.

De fleste studier på digital sikkerhetskultur fokuserer på adferdsdimensjonen. Mer spesifikt, de fokuserer på hvorvidt de folk vil trykke på en *"«phishing-lenke»*, eller om de deler passordet sitt med fremmede. Selv om det er en generell oppfatning om at digital sikkerhetskultur også omhandler verdier og holdninger, så settes disse til side til fordel for et fokus på adferd.
Når en fokuserer utelukkende på adferd betyr

«MINDRE FOKUS PÅ ADFERD, OG MER FOKUS PÅ HOLDNINGER, VERDIER OG FØLELSER SOM KAN SI NOE OM HVA FOLK VIL GJØRE ELLER REAGERE PÅ VISSE SITUASJONER.»

det at vi kan si noe om hva folk gjør eller har gjort. Det sier imidlertid lite om hva folk kommer til å gjøre. Med andre ord, et slikt fokus gir et bilde på sikkerhetsadferd i fortiden. Det er imidlertid et dårlig bilde på hva som vil skje i fremtiden. Samtidig er det vanlig for informasjonssikkerhetsbransjen å forsøke å forutse hva som vil komme til å skje. Sikkerheten må være forebyggende, altså i forkant. Vi ønsker med andre ord å kunne forutsi hvilke tendenser folk vil ha i visse situasjoner. I vår tilnærming til digital sikkerhetskultur har vi derfor valgt å legge mindre fokus på adferd, og mer fokus på holdninger, verdier og følelser som kan si noe om hva folk vil gjøre eller reagere på visse situasjoner.

I vår hovedstudie fra 2016 kartla vi kjerneelementene i den norske digital sikkerhetskulturen. Vi gikk bort fra antakelsen om at digital sikkerhetskultur kan beskrives utelukkende gjennom adferdsmønstre, men vurderte i stedet digital sikkerhetskultur gjennom et utvidet fokus på blant annet verdier, holdninger og følelser knyttet til ulike tema. Temaene spenner vidt, fra statlig styring og kontroll, til det individuelle synet på teknologikompetanse og risiko-oppfattelse.

Alle kulturer balanserer mellom det individuelle og det kollektive, mellom den enkeltes dømmekraft og oppfattelser til de kollektive normene og standardene. Vi er ikke fullstendige individualister, og vi er heller ikke fullstendig innlemmet i et større fellesskap. Når vi skal studere digital sikkerhetskultur betyr det derfor å peke på de faktorene som beskriver en slik kultur i et helhetlig perspektiv, samtidig som vi diskuterer og utfordrer de enkelte delene en digital sikkerhetskultur består av.

Vi har pekt ut åtte kjerneområder, eller dimensjoner, som vi mener beskriver digital sikkerhetskultur på en helhetlig og relevant måte. En kan ikke utelukke at det kan finnes andre dimensjoner som kan være nyttig å betrakte, men for vårt formål anses de utpekte kjerneområdene som tilstrekkelige.

KJERNEOMRÅDER FOR DIGITAL SIKKERHETSKULTUR

Fellesskap
Styring og kontroll
Tillit
Risiko-oppfattelse
Optimisme for teknologi og digitalisering
Kompetanse
Interesse
Adferdsmønstre

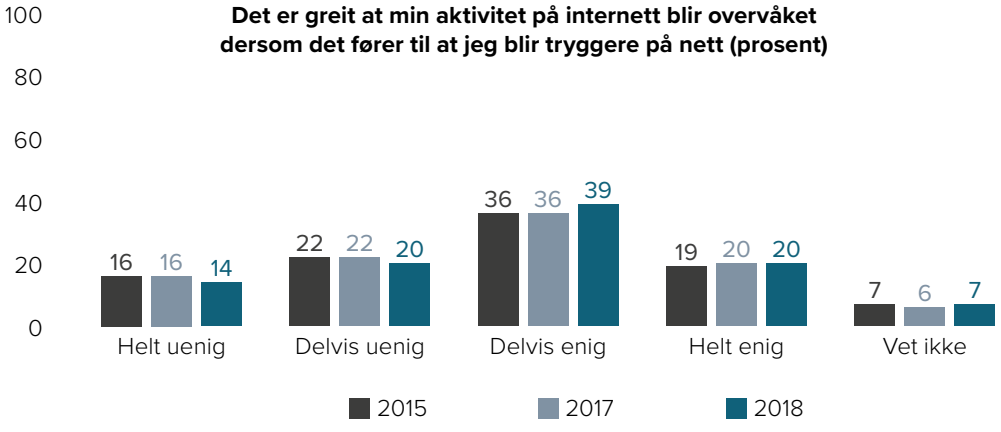
FELLESSKAP

Foto: **Øyvind Knoph Askeland, Norsk Olje og Gass**

KULTURER ER PER DEFINISJON KOLLEKTIVE.
Kulturer består av, og utvikles av, individer. På samme tid bidrar kulturen til å forme individene som er en del av den. Kulturer beskriver det karakteristiske for en gruppe mennesker, herunder deres sosiale vaner, deres holdninger, verdier og prioriteringer. For at en kultur skal være varig krever den lojalitet og solidaritet. Individene må identifisere seg som en del av gruppen, bidra til den og føye seg etter de uttalte og ikke-uttalte normene for adferd og holdninger. Når vi peker ut fellesskap som et av kjerneområdene, ønsker vi primært å fokusere på hvordan individet forholder seg til fellesskapet. Ser den enkelte seg selv som en del av et større «cyber-fellesskap», og blir den enkeltes adferd formet av et felles sett med normer og adferdsmønstre?

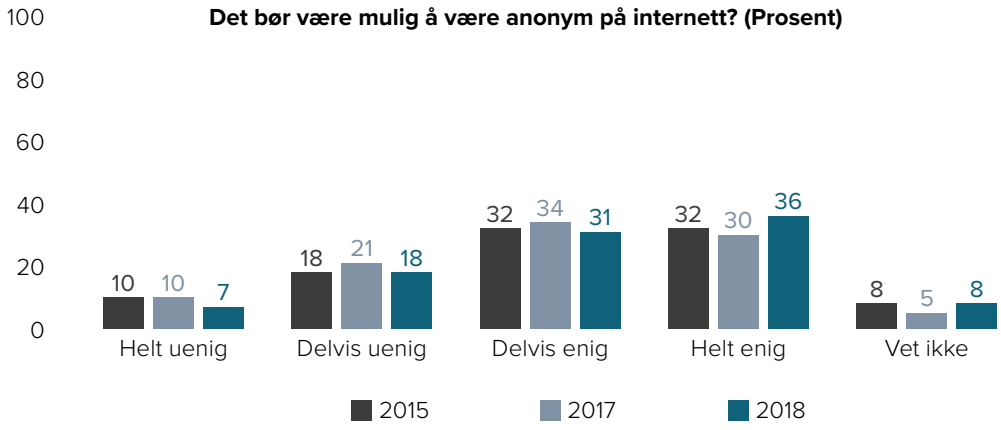
I synet på om hvorvidt fellesskapet skal kunne gjennomføre overvåking og kontroll er flertallet enige i påstanden *«Det er greit at min aktivitet på internett blir overvåket dersom det fører til at jeg blir tryggere på nett.»* 59 % av befolkningen er enten helt eller delvis enige i dette. I spørsmålet ligger det en forutsetning om at en gir fra seg privatliv i bytte mot å bli tryggere på nett. Siden 2015 har spørsmålet om hvorvidt man skal tillate en økt kontroll av hva folk foretar seg på nett vært en del av samfunnsdebatten. Digital grensekontroll, politiets ønsker om økt datalagring og teknologiselskapenes innsamling av data om den enkelte er eksempler på slike diskusjoner. Vi kan imidlertid ikke se en signifikant endring i befolkningens oppfatning om overvåking på internett.

Spørsmålet om anonymitet er beslektet fordi anonymitet kan være en måte å unndra seg kontroll. 67 % sier seg helt eller delvis enige i at det bør være mulig å være anonym på internett, og vi observerer heller ikke her en signifikant endring i perioden 2015–2018.

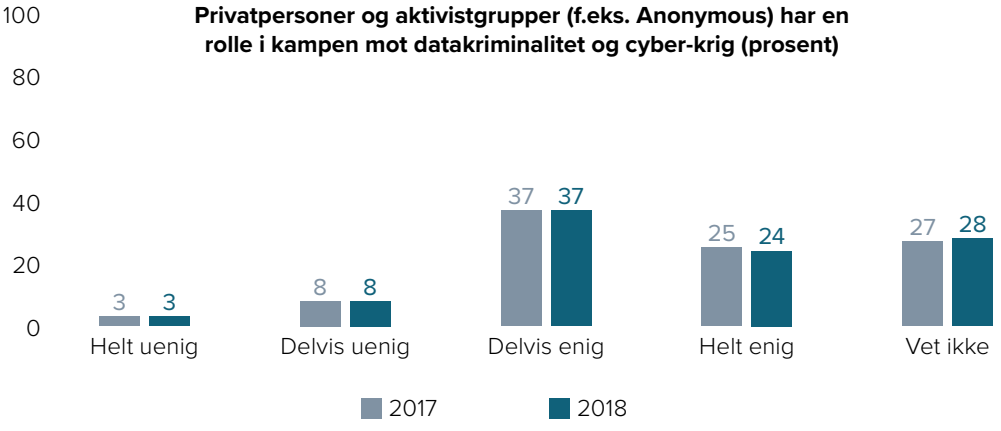


Figur 2:
Det er greit at min aktivitet på internett blir overvåket dersom det fører til at jeg blir tryggere på nett.

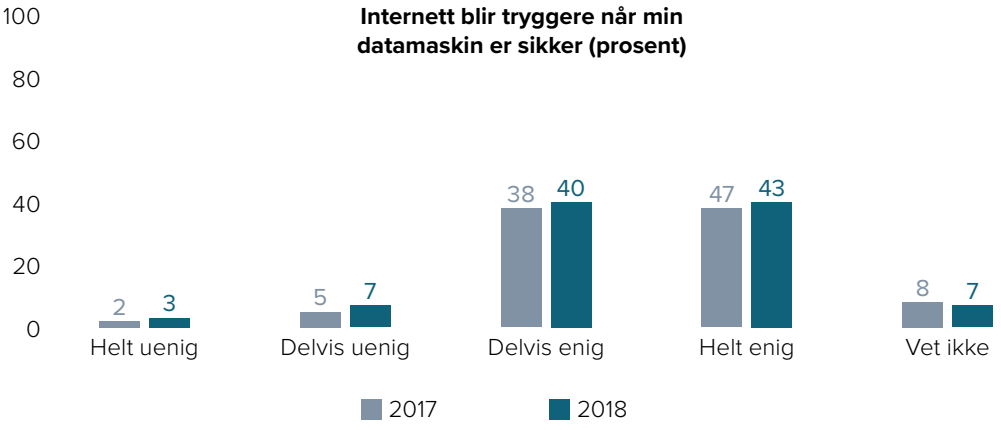
Figur 3: Det bør være mulig å være anonym på internett.



Figur 4: Privatpersoner og aktivistgrupper (f.eks. Anonymous) har en rolle i kampen mot datakriminalitet og cyber-krig



Figur 5: Internett blir tryggere når min datamaskin er sikker.

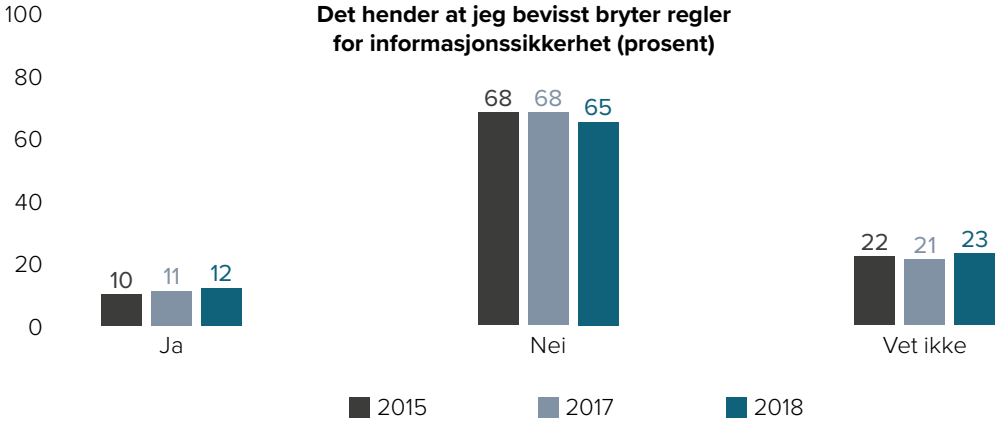


En annen side av dette er om den enkelte aksepterer samfunnets normer for hvem som lager reglene, og hvem som håndhever dem. Den enkeltes rettssikkerhet baserer seg blant annet på at maktutøvelse styres av rettsregler. Når det gjelder datakriminalitet fremsettes det imidlertid påstander om at politiet verken har kompetanse eller ressurser til å etterforske slike saker. Noen mener derfor at det derfor er nødvendig at IKT-kyndige privatpersoner og grupperinger gjør dette. Holdningen om at privatpersoner har en rolle i kampen mot datakriminalitet bryter mot de prinisppene for rettshåndhevelse som fellesskapet har besluttet. Vår undersøkelse viser at hele 61 % er helt eller delvis enig i påstanden «*Privatpersoner og aktivistgrupper (f.eks. Anonymous) har en rolle i kampen mot datakriminalitet og cyber-krig*» . 28 % svarer at de ikke vet.

NorSIS ser det som problematisk at så mange støtter et slikt syn. Det er fordi dette kan bidra til å legitimere en selvtektskultur på nett. At privatpersoner og grupperinger foretar etterforsking av andre, uten at de er underlagt de samme kontrollmekanismene som politiet er i sine etterforskinger er uheldig.

Undersøkelsen ser også på om den enkelte ser seg selv som ansvarlig for den totale tryggheten på nett. Forståelsen av at ens egne datamaskiner og digitale enheter kan forvolde skade på nett, krever både kunnskap, og en forståelse for sammenhenger og årsaksforhold. Dette kalles gjerne for netthygiene. 83 % sier seg helt eller delvis enige i påstanden *«Internett blir tryggere når min datamaskin er sikker.»*

12 % av befolkningen sier at det hender at de bevisst bryter regler for informasjonssikkerhet. Her observerer vi en signifikant forskjell mellom kvinner og menn, der de svarer henholdsvis 6 % og 18 % på dette. Det er også aldersforskjeller. De yngre aldersgruppene (18–40) bryter reglene vesentlig mer enn de eldre (55+), henholdsvis 20 og 4 prosent. Vi finner videre at folk med høyere utdanning oftere bryter reglene enn de som har grunnskole/folkeskole.



Figur 6:
Det hender jeg bevisst bryter reglene for informasjonssikkerhet.

STYRING OG KONTROLL

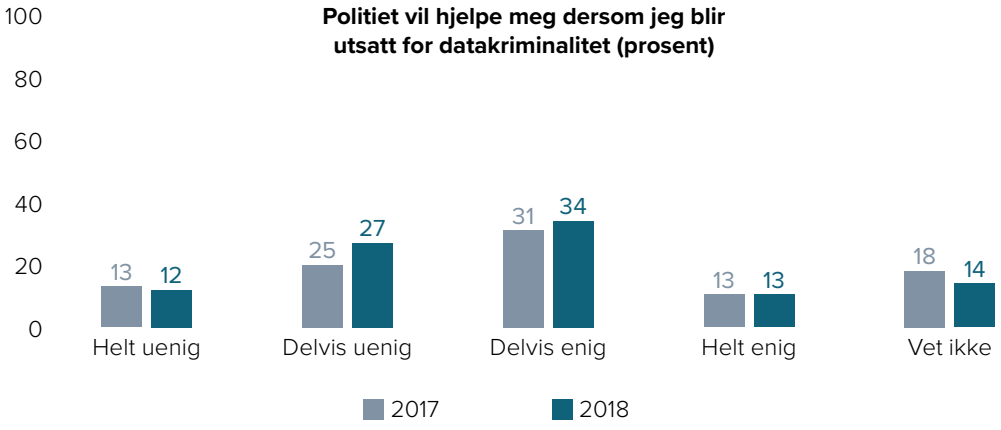
STYRING OG KONTROLL RELATERER SEG TIL FELLESSKAP: Hvordan skal fellesskapet reguleres, og av hvem? I denne sammenhengen fokuserer vi på hvordan befolkningen ser på styring og kontroll i et digitalisert samfunn. Hvem skal trekke opp linjene for hva som er akseptabel bruk av IKT og digitale tjenester, hvor skal linjene trekkes opp og hvordan skal den enkelte rette seg etter disse?

Ved å se på styring og kontroll ser vi også på spørsmål om hvem som skal være ansvarlig for vår trygghet på nett. I diskusjonen omkring sikkerhet, er det alltid et spørsmål om å balansere den enkeltes frihet med vår felles trygghet. «Alle» vil ha frihet, og «alle» vil samtidig være trygge. Hvordan arter denne balansen seg i befolkningens digitale sikkerhetskultur? Hvor mye overvåking er akseptabelt når den enkeltes sikkerhet og trygghet står på spill?

En side ved befolkningens syn på digital styring og kontroll, er synet på overvåking av ens egen aktivitet på nett. Som nevnt over mener 59 % prosent at dette er greit, forutsatt at det fører til at de blir tryggere på nett. Samtidig mener befolkningen i stor grad at det skal være mulig å være anonym på nett. Befolkningens syn på om det skal være mulig å være anonym på nett, altså å kunne unndra seg visse former for styring og kontroll er også nevnt over.

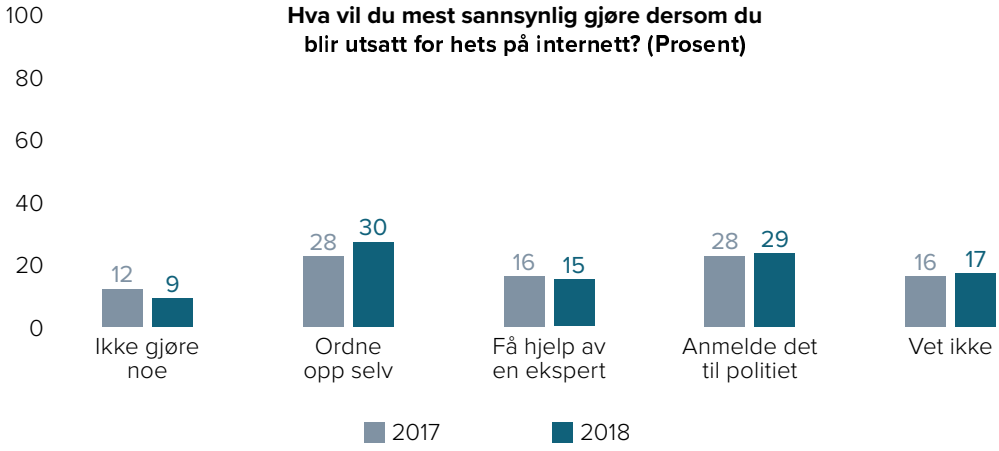
47 % av befolkningen er helt eller delvis enige i påstanden «*Politiet vil hjelpe meg dersom jeg blir utsatt for datakriminalitet.*» Samtidig er 39 % helt eller delvis uenige i denne påstanden. Styring og kontroll vil i noen tilfeller dreie seg om inngripende metoder og maktbruk overfor den enkelte. Det er derfor interesant å se på befolkningens tillit til politiet. Manglende tillit til politiet fører trolig til at flere mener at privatpersoner og aktivister skal ha en rolle i kriminalitetsbekjempelse.

I tillegg til å se på hvorvidt befolkningen tror at politiet kan hjelpe dem dersom de blir utsatt for datakriminalitet, ser vi på om den enkelte vil oppsøke hjelp fra de som er satt til å håndheve kriminalitetsbekjempelse på nett. Hets, nettsvindel og ID-tyverier rammer mange nordmenn hvert år. Dette er ofte forhold som kan være ulovlig og som bør etterforskes av politiet. 29 % svarer at de vil kontakte politiet dersom de blir utsatt for hets på internett. Når det gjelder nettsvindel og ID-tyverier, svarer henholdsvis 64 % og 72 % det samme.

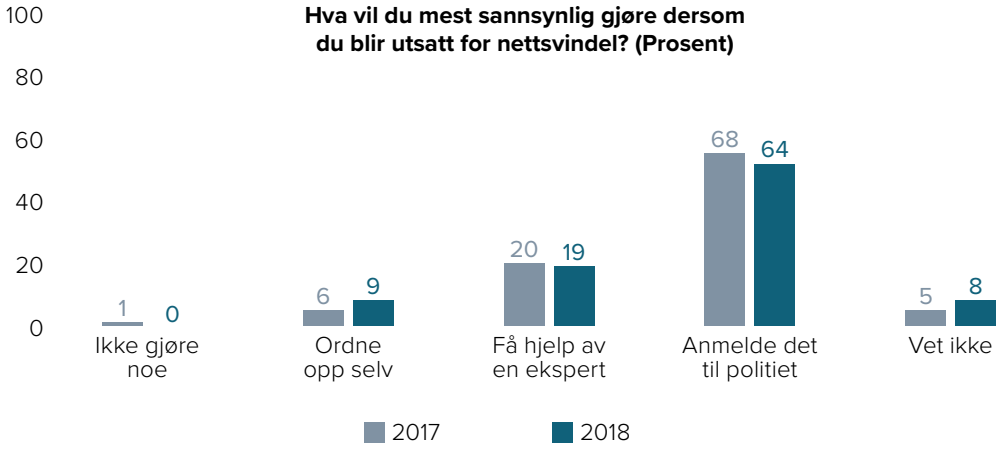


Figur 7: Politiet vil hjelpe meg dersom jeg blir utsatt for cyberkriminalitet

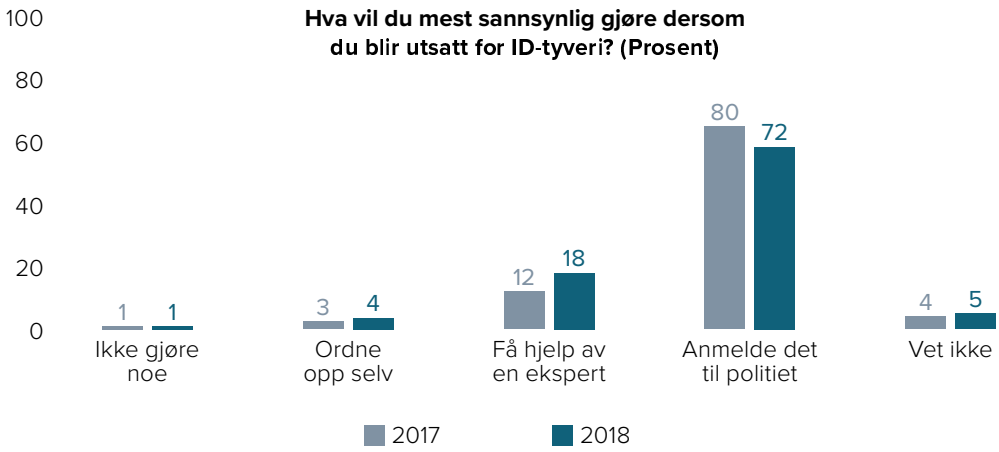
Figur 8: Hva vil du mest sannsynlig gjøre dersom du blir utsatt for hets på internett?



Figur 9: Hva vil du mest sannsynlig gjøre dersom du blir utsatt for nettsvindel?



Figur 10: Hva vil du mest sannsynlig gjøre dersom du blir utsatt for ID-tyveri?



Som nevnt sier 12 % at de noen ganger bryter reglene for informasjonssikkerhet. Det er derfor interessant å finne ut om folk kjenner til om det er satt regler for fellesskapet de er en del av. Når vi spør om arbeidsplassen har regler for informasjonssikkerhet, er svaret primært av interesse for de virksomhetene som bruker vår metode for å kartlegge sin digitale sikkkerhetskultur.

NorSIS erfarer at det er forskjeller mellom ulike virksomheter og bedrifter. Ikke alle har regler for informasjonssikkerhet, og noen legger mer vekt på å forklare betydningen av reglene enn det andre gjør. I 2018 sier 38 % av de som er i arbeid at de er kjent med slike regler på sin arbeidsplass har, mens 14 % sier at de ikke vet om arbeidsplassen har slike regler.

Figur 11: Har arbeidsplassen din regler for informasjonssikkerhet?

Foto: **Bjørn Vidar Leroen, Norsk Olje og Gass**

ET DEMOKRATI FORUTSETTER EN VISS TILLIT MELLOM INNBYGGERNE, mellom innbyggerne og myndighetene, mellom myndighetsorganer, mellom bedrifter, mellom ansatte og arbeidsgivere og så videre. Når stadig mer av vår nasjonale økonomiske vekst og velferd er knyttet til digitalisering av samfunnet, blir tillit på dette området stadig viktigere.

For at myndighetene skal kunne styre effektivt er de avhengig av innbyggernes tilit. I dette ligger det også at myndighetene må kunne styre selv om noen av innbyggerne er uenige i politikken, eller når det skal innføres tiltak som er fremmede eller nye for innbyggerne.

Som en konsekvens av dette er digitaliseringen både avhengig av, og sårbar for, tillit. Digitalisering er en ønsket utvikling for de fleste nasjoner, og gitt den teknologiske utviklingen vi observerer er det nærmest uunngåelig. For innbyggerne kan dette imidlertid føre til visse dilemma. Folk blir ikke bare oppfordret til å ta i bruk teknologi, de blir i noen tilfeller tvunget til det. Å være bankkunde i dag betyr at du må forholde deg til nettbank. Prisene for bank-transaksjoner i tradisjonelle banker øker sterkt, og tilgjengeligheten til bank-filialene reduseres fordi stadig flere av dem legges ned. Kommunikasjonen mellom den enkelte og det offentlige skal primært foregå digitalt. Dersom den enkelte ikke føyer seg etter denne utviklingen, risikerer vedkommende både å glipp av de positive gevinstene ved digitaliseringen, og i noen tilfeller får det store ulemper å ikke rette seg etter det samfunnet har lagt opp til.

Når det digitaliserte samfunnet krever at den enkelte skal ta i bruk digitale tjenester og verktøy, forutsettes det at innbyggerne har tilstrekkelig tillit. Først og fremst må tjenestene være sikre. Innbyggerne vil ikke tolerere mange sikkerhetsbrudd før unngår å bruke de digitale tjenestene, og i verste fall mister tilliten til de som leverer dem.

«FOLK BLIR IKKE BARE OPPFORDRET TIL Å TA BRUK TEKNOLOGI, DE BLIR I NOEN TILFELLER TVUNGET TIL DET.»

Også andre former for tillit spiller inn. Når vi handler varer og tjenester på nettet, overlater vi bank- og kredittkort, og annen personlig informasjon, til andre parter. Når vi velger å gjøre dette, har vi implisitt tillit til at de vil beskytte vår informasjon mot misbruk. Det er likevel en balansegang, for vi vet samtidig at Google, Facebook, Apple og andre bruker denne informasjonen til å profilere sine kunder. Profilene selges og brukes så til målrettet markedsføring. Som forbruker stilles en ovenfor et dilemma: *Må det å kjøpe en bok på Amazon bety at jeg må la Amazon og deres partnere drive målrettet markedsføring ovenfor meg?*

Målrettet markedsføring er på et vis medaljens bakside, når det kommer til digitalisering og tillit. Mange anser målrettet markedsføring som et brudd på tilliten, ettersom leverandørene av digitale tjenester bruker informasjon om den enkelte til sin egen vinning. Dersom dette reduserer tilliten til tjenester og leverandører kan det

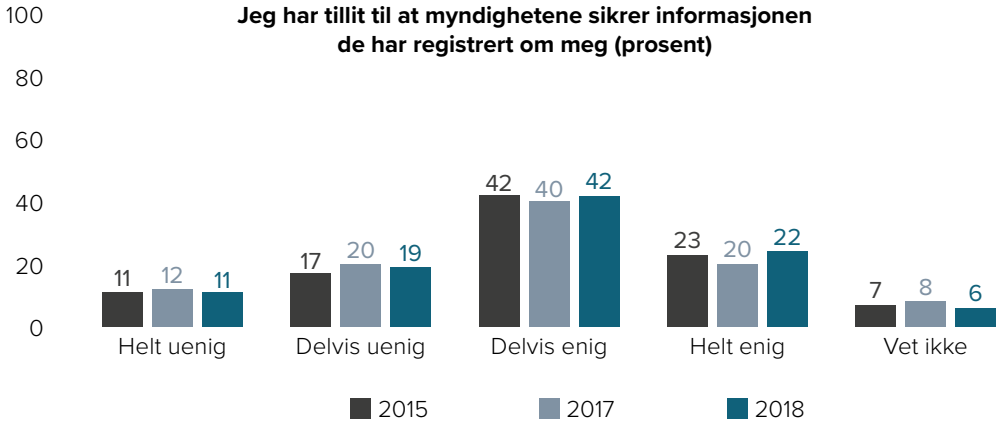
potensielt skade digitaliseringen av samfunnet.

Tillit i denne sammenheng kan være gjensidig tillit mellom enkeltpersoner, virksomheter og myndigheter. Tillit i et digitalt samfunn betyr transaksjoner og handel mellom mennesker som kanskje aldri møtes. Vi gir fra oss penger fordi vi har tillit til at den andre parten leverer det som er avtalt. Vi gir fra oss informasjon til nett-selskaper fordi vi har tillit til at de ikke skal bruke informasjonen til å skade oss.

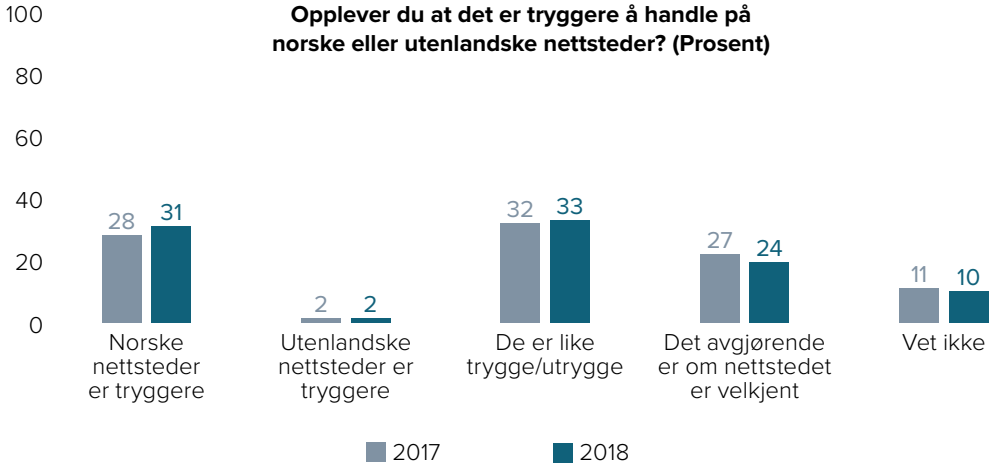
Vi har allerede sett på befolkningens syn på overvåking, anonymitet og kontroll. Tilliten til at politiet skal hjelpe en er relativt lav (47 %), men det er også verdt å legge merke til at langt de fleste sier at de vil be politiet om hjelp dersom de blir utsatt for nettsvindel eller ID-tyveri. Til påstanden *«Jeg har tillit til at myndighetene sikrer informasjonen de har registrert om meg»*, svarer 64 % at de er helt eller delvis enige i dette, mens 30 % svarer at de er helt eller delvis uenige. At en tredjedel av befolkningen ikke har tillit til at myndighetene sikrer informasjonen deres er etter vårt syn svært alvorlig. Det kan motvirke digitaliseringen i samfunnet ved at folk ikke ønsker å ta i bruk de digitale tjenestene som myndighetene legger opp til.

31 % av befolkningen har mer tillit til norske nettsteder enn utenlandske, når det gjelder trygghet. 2 % svarer at de anser utenlandske som tryggere. Her svarer også 33 % at de mener at norske og utenlandske nettsteder er like trygge/utrygge, altså at nasjonalitet ikke spiller noen rolle. 24 % mener at det er avgjørende om nettstedet er velkjent.

Figur 12: Jeg har tillit til at myndighetene sikrer informasjonen de har registrert om meg



Figur 13: Opplever du at det er tryggere å handle på norske eller utenlandske nettsteder?



RISIKOOPPFATTELSE

KOMPETANSE, LÆRING OG RISIKO-OPPFATTELSE ER KNYTTET TIL HVERANDRE.

Et eksempel: Studier viser at en kan finne økt *risiko-adferd* blant mennesker som mener at de har mye kompetanse eller ferdigheter. Med andre ord, mennesker som har mer kompetanse innen informasjonssikkerhet står i fare for å overvurdere sin egen evne til å kontrollere truslene, og de kan dermed være disponert til å ta mer risiko[1].

I en studie er risiko-oppfattelse fremhevet som en nøkkelfaktor for utforming av adferdsmønstre. Studien sier at enkeltpersoner har *«an unrealistic optimism for risks that they perceive to be under their personal control»*[2 3]. De argumenterer videre at *«an individual may view their actions on their personal computer to be under their control, threats may be seen as less risky. Hence, the chance that non-adherence to security policies will result in serious consequences may also be underestimated. This means that individuals might be more likely to engage in risky behavior»*.

Hvordan den enkelte oppfatter risiko er subjektivt, men er likevel en viktig faktor som påvirker hvordan vi tenker og handler når det kommer til digitale trusler. Det er en faktor som kan være vanskelig å tallfeste, beregne og forutse. Likevel vet vi at risikooppfattelsen vil bli påvirket av sikkerhetshendelser, hva vi tror at vi vet om digitale trusler, våre erfaringer på nett osv.

«BEFOLKNINGEN OPPLEVER DET ALTSÅ SOM MER RISIKOFYLT Å BRUKE INTERNETT NÅ ENN TIDLIGERE.»

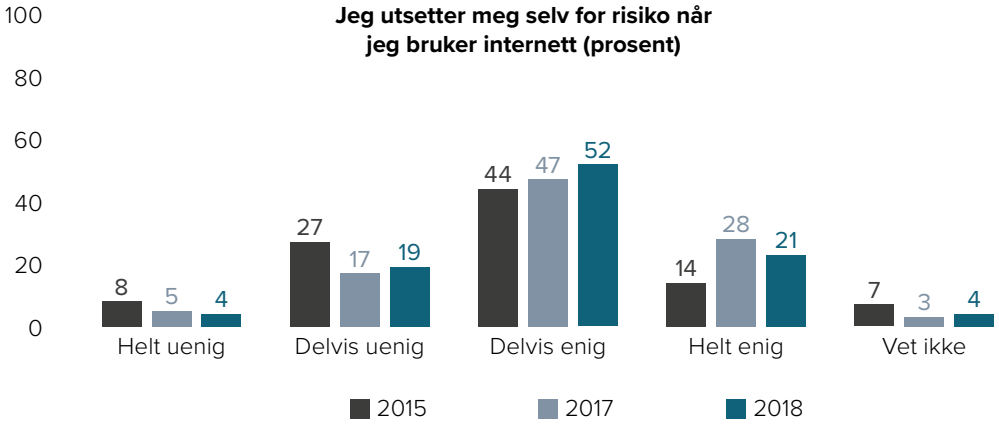
73 % av befolkningen er enten helt eller delvis enig i påstanden *«Jeg utsetter meg selv for risiko når jeg bruker internett.* Her ser vi en signifikant endring fra 2015 til 2018. I 2015 sa 58 % seg helt eller delvis enig i dette, mens det i 2018 er 73 % som svarer det samme. Befolkningen opplever det altså som mer risikofylt å bruke internett nå enn tidligere.

Videre er 61 % helt eller delvis enig i påstanden *«Jeg synes at jeg får tilstrekkelig informasjon om de truslene som finnes på internett.»* 32 % sier seg helt eller delvis uenig i denne påstanden, mens 7 % sier at de ikke vet. Sammenlignet med resultatene fra 2015, er det færre som mener at de får tilstrekkelig informasjon om truslene på nett nå enn tidligere.

1. Parsons, McCormac et al. (2010) *Human Factors and Information Security: Individual, Culture and Security Environment*

2. Ibid.

3. Kreuter, M.W., & Strecher, V. (1995). *Changing inaccurate perceptios of health risk: Results from a randomised trial.* Health Psychology, 14, 55-63



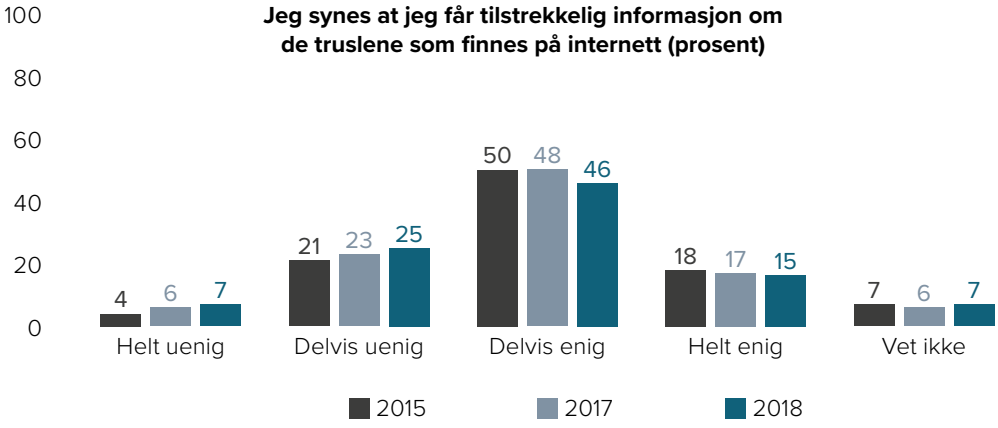
Figur 14: Jeg utsetter meg selv for risiko når jeg bruker internett

73 % av befolkningen er enten helt eller delvis enig i påstanden *«Jeg utsetter meg selv for risiko når jeg bruker internett.»* Her ser vi en signifikant endring fra 2015 til 2018. I 2015 sa 58 % seg helt eller delvis enig i dette, mens det i 2018 er 73 % som svarer det samme. Befolkningen opplever der altså som mer risikofyllt å bruke internett nå enn tidligere.

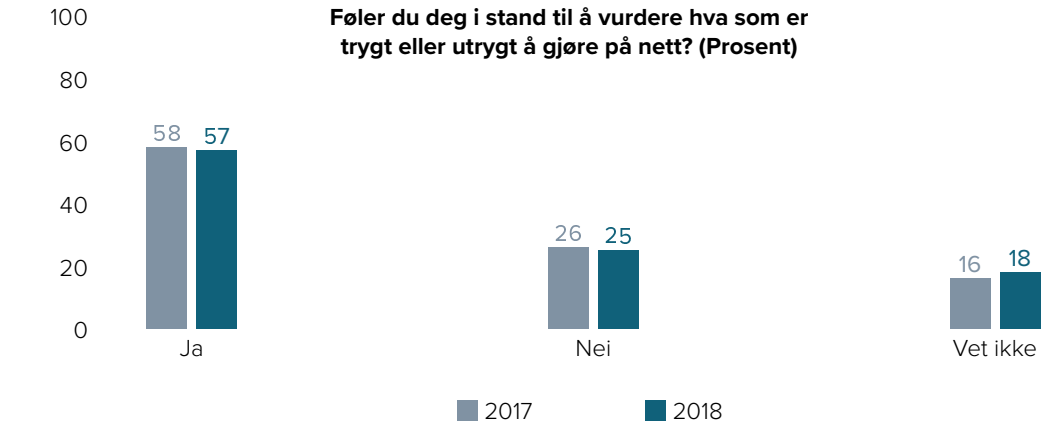
Videre er 61 % helt eller delvis enig i påstanden *«Jeg synes at jeg får tilstrekkelig informasjon om de truslene som finnes på internett.»* 32% sier seg helt eller delvis uenig i denne påstanden, mens 7 % sier at de ikke vet. Sammenlignet med resultatene fra 2015, er det færre som mener at de får tilstrekkelig informasjon om truslene på nett nå enn tidligere.

57 % av de spurte sier at de er i stand til å vurdere hva som er trygt og utrygt på nett, mens 2 5% sier at de ikke er det. 18 % sier at de ikke vet. Vi finner også i år en forskjell mellom aldersgruppene, der 67% av de som er mellom 18–34 sier at de er i stand til å vurdere dette, mens kun 44 % av de som er 55 og over sier det samme.

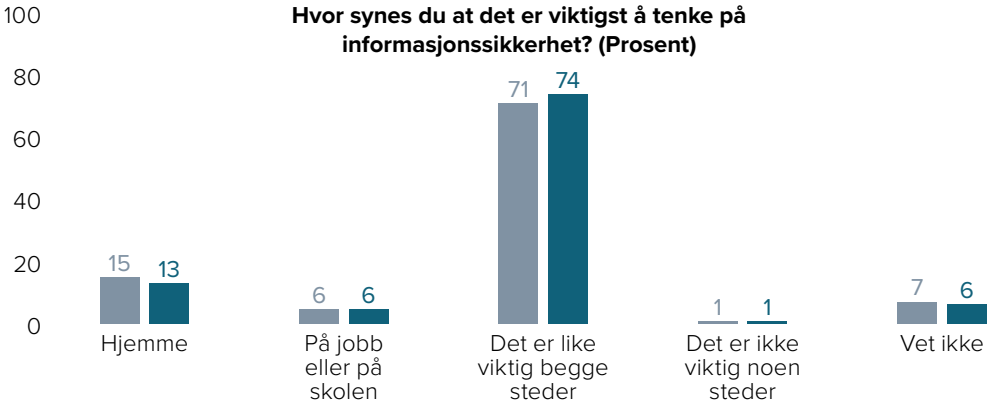
At 74 % mener at det er like viktig å tenke på informasjonssikkerhet både hjemme og på jobb er en indikator på befolkningens risiko-oppfattelse. Vi observerer her at det er 13 % som svarer at det er viktigst hjemme, mens 6 % mener at det er viktigst på jobb eller på skolen.



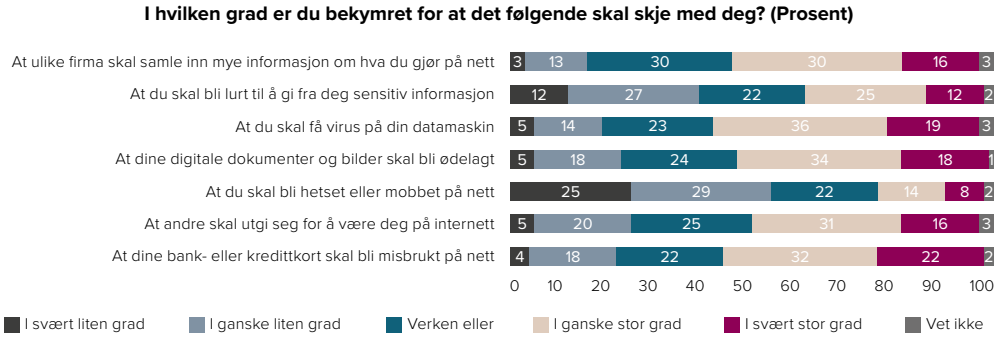
Figur 15: Jeg synes jeg får tilstrekkelig informasjon om de truslene som finnes på internett.



Figur 16: Føler du deg i stand til å vurdere hva som er trygt eller utrygt å gjøre på nett?

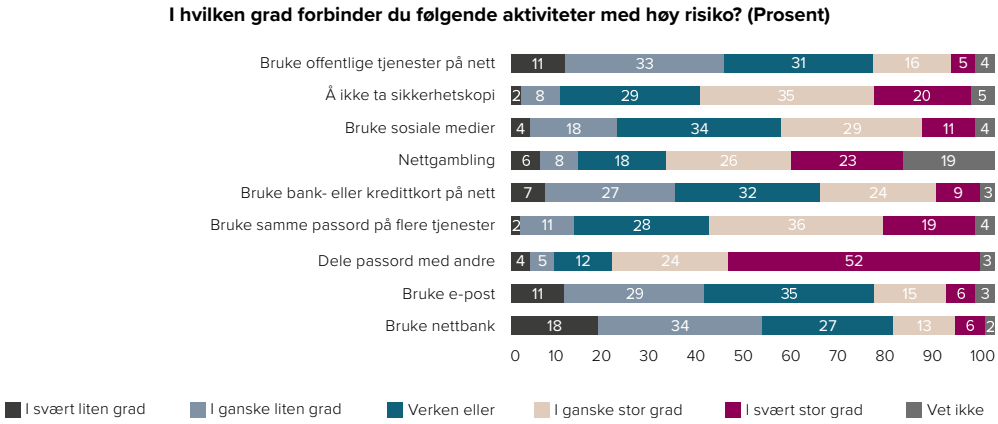


Figur 17:
Hvor synes du at det er viktigst å tenke på informasjonssikkerhet?



Vi spør også i hvilken grad den enkelte er bekymret for typiske trusler som rammer nordmenn på nett.

Figur 18:
I hvilken grad er du bekymret for at det følgende skal skje med deg?



Vi spør også i hvilken grad befolkningen forbinder en del vanlige nettaktiviteter med høy risiko.

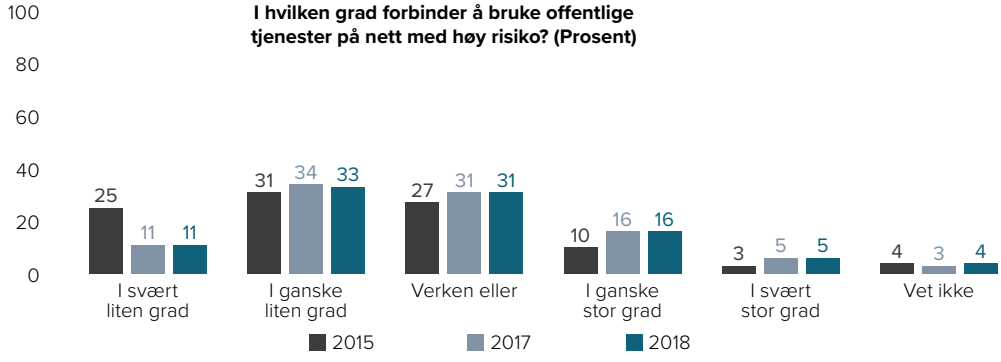
Figur 19:
I hvilken grad forbinder du følgende aktiviteter med høy risiko?

Svarene viser at befolkningens risiko-oppfattelse av det å bruke offentlige tjenester på nett har endret seg siden undersøkelsen i 2015. Da svarte 13 % at de anså risikoen ved bruk av offentlige tjenester på nett å være enten ganske stor eller svært stor. I 2017 og 2018 svarer 21 % det samme. Vi observerer altså en økning i en slik frykt i befolkningen.

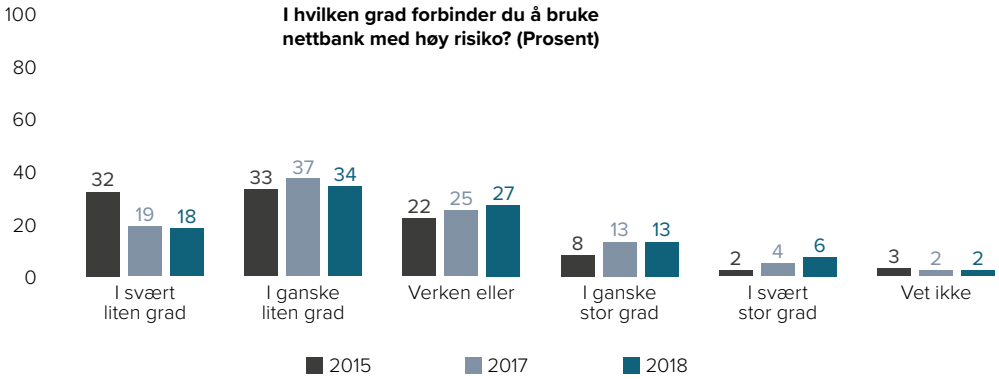
Tilsvarende øker frykten for bruk av nettbank i den samme perioden. I 2015 svarte 10 % at de anså risikoen ved bruk av nettbank å være ganske stor eller svært stor, mens i 2018 svarer 19 % det samme.

Tillit til digitale tjenester er en forutsetning for at befolkningen skal utnytte de muligheter som digitaliseringen gir. På samme tid kan frykt for digitale trusler redusere tilliten og føre til at den enkelte lar være å bruke digitale tjenester. På spørsmålet «*Har kunnskap om trusler eller hacking noen gang fått deg til å la være å bruke en nettjeneste?*», svarer 29 % ja til dette. Frykt for trusler på nett kan bli en motvekt til digitaliseringsarbeidet og kan føre til en nedkjølingseffekt. Det vil si at folk avstår fra å bruke nett-tjenester av frykt for datakriminalitet eller at det de skriver, hvordan de bruker nettet eller hva de legger igjen av spor kan brukes mot dem senere. Politiets bekjempelse av datakriminalitet og opplæring i trygg nettbruk er tiltak som trolig vil motvirke dette.

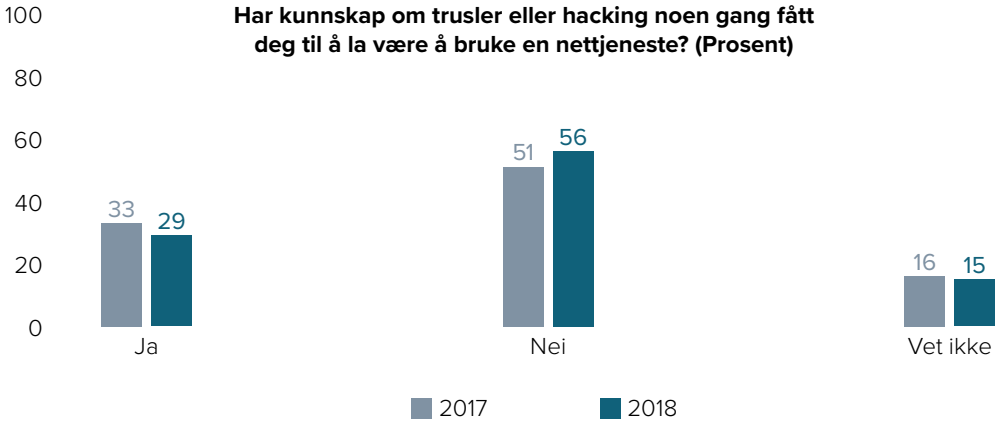
Vi er også interessert i å vite hva den enkelte ser på som den største risikoen på nett, seg selv eller andre. Dette kan tolkes som et uttrykk for ens selvtillit når det gjelder digital sikkerhet. På spørsmålet «*Hva mener du er den største risikoen på nett?*» sier 20 % at de frykter at de selv skal gjøre noe feil, mens 69 % sier at de frykter at noen andre skal gjøre noe mot dem. 11 % sier at de ikke vet. Vi observerer kjønnsforskjeller på dette spørsmålet. 25 % av menn frykter at de selv skal gjøre noe feil, mens 15 % av kvinner mener det samme.



Figur 20: I hvilken grad forbinder du å bruke offentlige tjenester på nett med høy risiko?



Figur 21:
21 I hvilken grad forbinder du å bruke nettbank med høy risiko?



Figur 22:
Har kunnskap om trusler eller hacking noen gang fått deg til å la være å bruke en nettjeneste?

Figur 23:
Hva mener du er den største risikoen på nett?

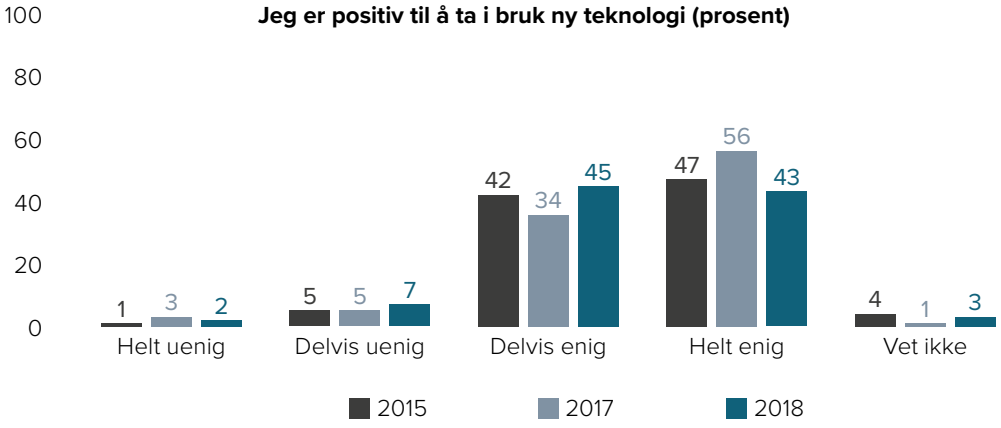
OPTIMISME FOR TEKNOLOGI OG DIGITALISERING

Foto: **Avinor**

DIGITALISERINGEN HJELPER IKKE BARE BEDRIFTER Å BRUKE INFORMASJONS-TEKNOLOGI OG DATA PÅ SMARTERE MÅTER, den sørger også for at den enkelte kan utnytte gevinstene av et digitalisert samfunn. I tillegg er digitaliseringen av samfunnet en stadig viktigere forutsetning for nasjonal økonomisk vekst og veldferd. For digital sikkerhetskultur ønsker vi å se på befolkningens holdninger til denne utviklingen. Med andre ord: Den enkeltes holdning til hvordan digitaliseringen påvirker måten den enkelte forholder seg til bruk av teknologi i samfunnet.

Folk i Norge er generelt svært positive til å ta i bruk ny teknologi. 88% sier at de er helt eller delvis enig i påstanden *«Jeg er positiv til å ta i bruk ny teknologi»,* mens 9 % er helt eller delvis uenig.

Å være positiv til noe betyr ikke nødvendigvis det samme som å være interessert i det. 48 % av befolkningen sier at de er ganske eller svært interessert i teknologi og IT, mens 25 % sier at de er ganske lite eller svært lite interessert i dette. Vi ser nærmere på dette i et senere kapittel.



Figur 24:
Jeg er positiv til å ta i bruk ny teknologi.

KOMPETANSE

ALT DEN ENKELTE FORETAR SEG, enten det er å kontakte det offentlige, kommunisere med andre mennesker eller dele feriebildene med andre på sosiale medier, forutsetter at vedkommende forholder seg til IKT og digitale tjenester. Dette betyr at alle nordmenn må ha et sett med grunnleggende digitale ferdigheter. Spørsmålet er: *Hvor og hvordan får de disse ferdighetene?* Det er et paradoks at myndigheter og bedrifter oppfordrer alle til å ta i bruk digitale tjenester, mens digitale ferdigheter bare i noen i grad inngår i skolens læreplaner eller i bedriftenes opplæringsprogrammer. Folk flest tvinges derfor til å tilegne seg slike ferdighetene på egenhånd.

I alle kulturer lyttes noen mennesker mer til enn andre. Enten det er kjendiser eller eksperter på sine områder. Noen får mer taletid og gjennom det større mulighet til å påvirke oss andre. Disse menneskene har stor påvirkning på hvordan kulturen endres. De folk beundrer og lytter til, påvirker deres verdier og holdninger. Gjennom dette påvirker de hvordan befolkningen forholder seg til andre mennesker og dens adferdsmønstre. Gjennom å fokusere på dette vil vi undersøke hvem som er de sterke røstene når det kommer til læring av informasjonssikkerhet. Lærer ulike grupper i samfunnet av forskjellige typer mennesker?

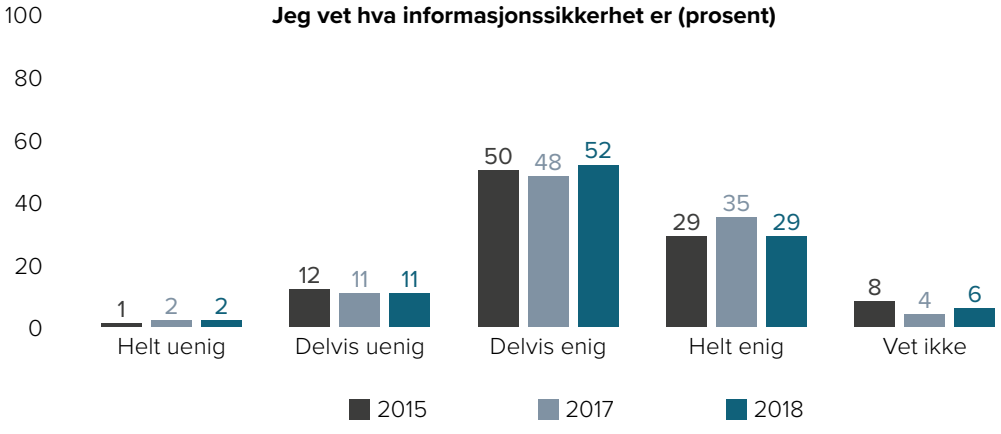
Nordmenn er generelt kunnskapsrike når det kommer til informasjonssikkerhet. De ser også på seg selv som relativt kunnskapsrike, og mener at de kan gjøre riktige vurderinger for sin sikkerhet på nett. 81% er helt eller delvis enig i påstanden *«Jeg vet hva informasjonssikkerhet er.»*

«NORDMENN ER GENERELT KUNNSKAPSRIKE NÅR KOMMER TIL INFORMASJONSSIKKERHET.»

Imidlertid er det kun 23 % av de spurte som sier at de har fått opplæring i informasjonssikkerhet i løpet av de to siste årene. 71 % sier at de ikke har fått opplæring.

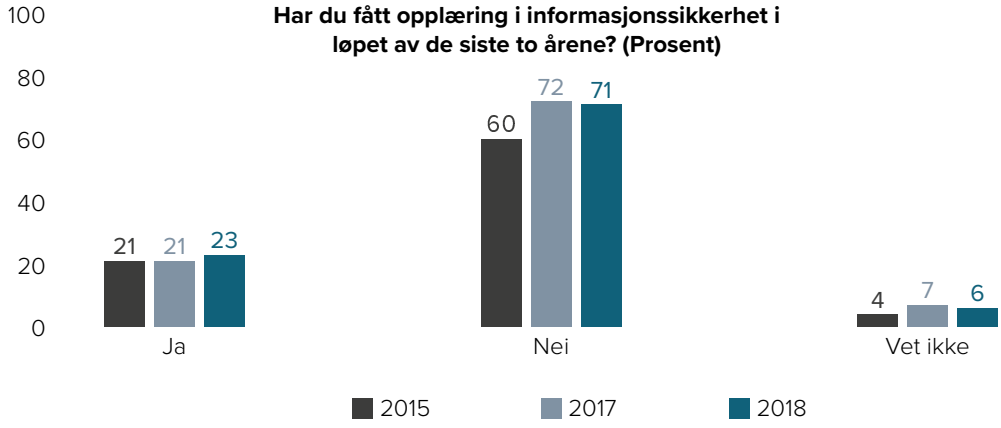
75 % mener at de har fått bedre ferdigheter etter slik opplæring, mens 14% mener at de ikke har fått det.

Generelt mener nordmenn at de kan like mye eller mer enn gjennomsnittet, når det kommer til informasjonssikkerhet. I befolkningen mener 55 % at de kan omtrent det samme som folk flest, mens 24 % mener at de kan mer en gjennomsnittet. 18 % mener at de kan mindre enn gjennomsnittet.

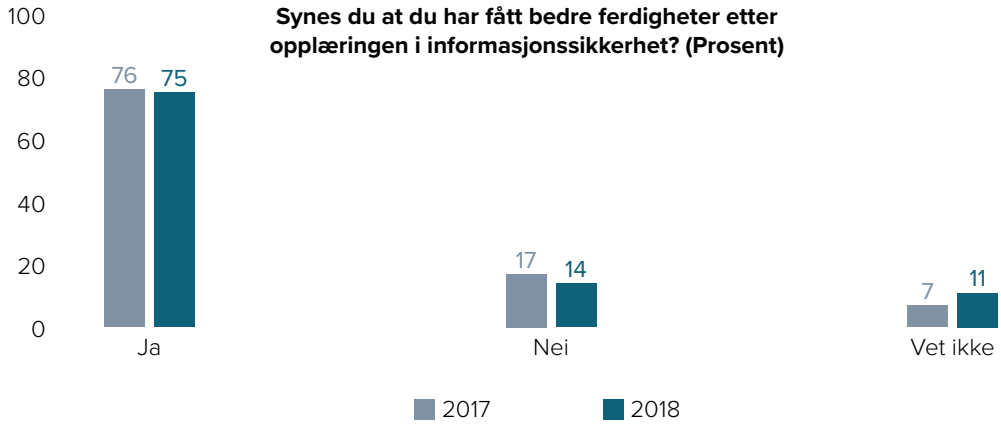


Figur 24: Jeg vet hva informasjonssikkerhet er.

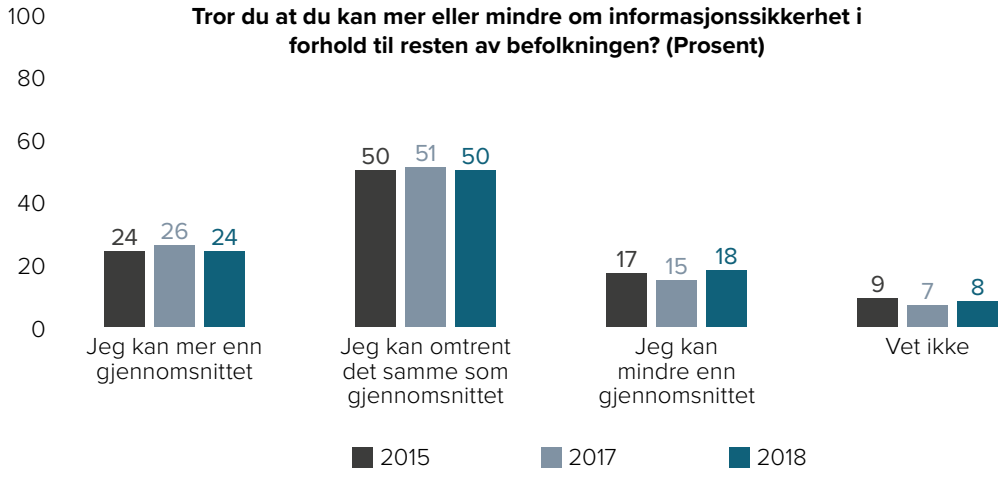
Figur 26: Har du fått opplæring i informasjonssikkerhet i løpet av de siste to årene?

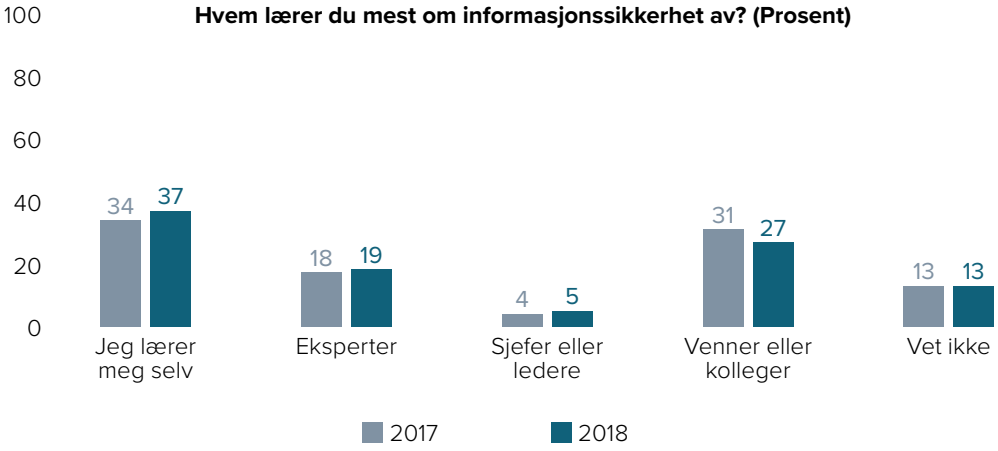


Figur 27: Synes du at du har fått bedre ferdigheter etter opplæringen i informasjonssikkerhet?



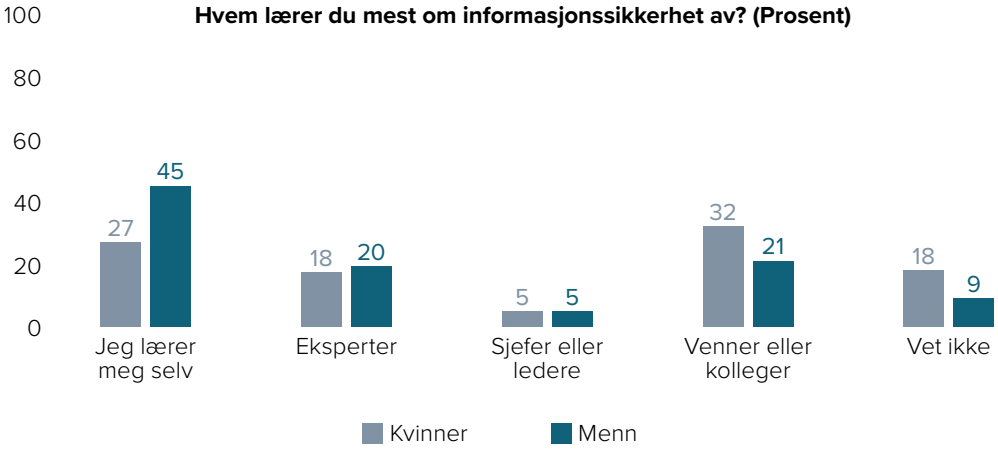
Figur 28: Tror du at du kan mer eller mindre om informasjonssikkerhet i forhold til resten av befolkningen?



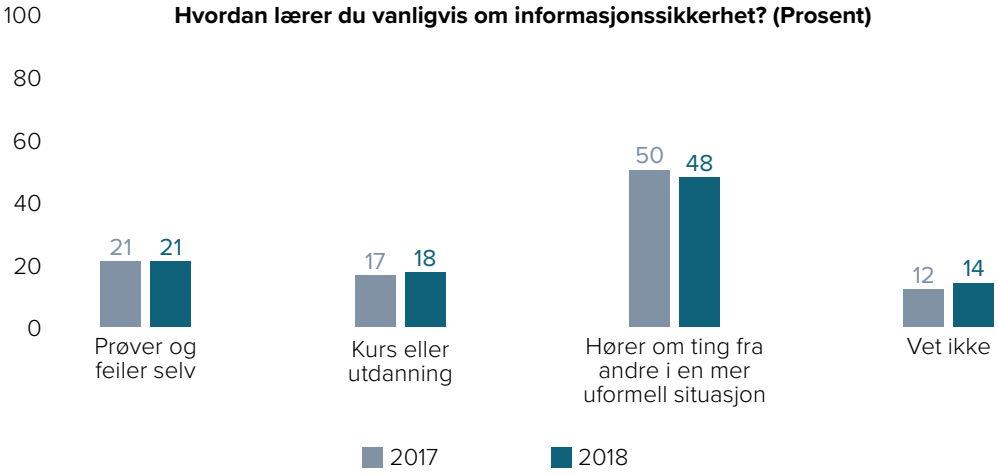


Figur 29:
Hvem lærer du mest om informasjons-sikkerhet av?

På spørsmålet «*Hvem lærer du mest om informasjonssikkerhet av?*» oppgir kun 19 % at de lærer av eksperter. Langt flere lærer av seg selv (37 %) eller av venner og kolleger (27 %). Vi ser en signifikant forskjell på kvinner og menn, der 45 % av mennene svarer at de lærer seg selv, mens 27 % av kvinnene svarer det samme. I hovedstudien (i 2016) fant vi en sammenheng mellom interesse for teknologi og IKT og hvem folk lærer av. Menn er generelt mer interessert i dette, og vi antar at dette er forklaringen på forskjellene her.

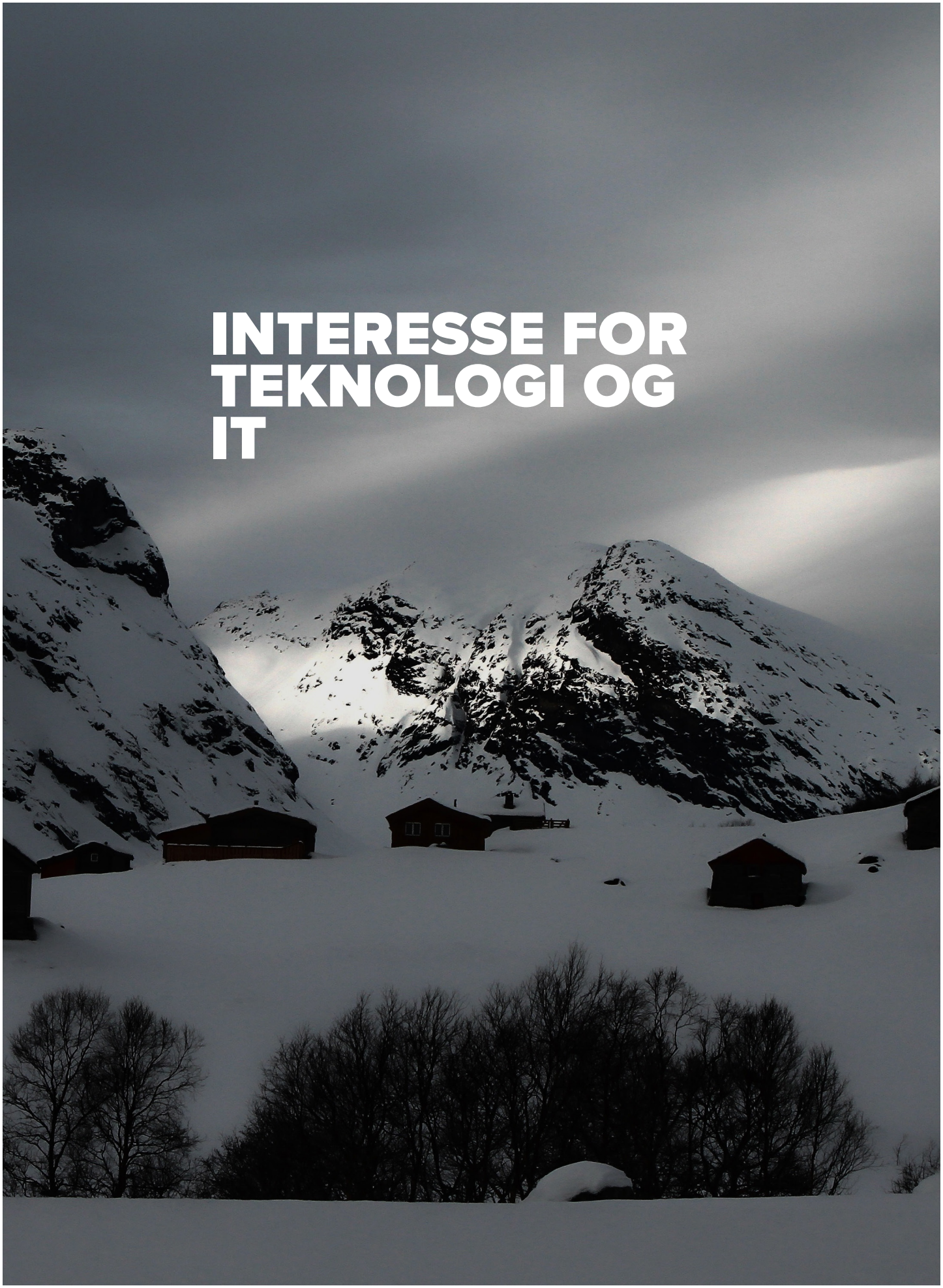


Figur 30:
Hvem lærer du mest om informasjons-sikkerhet av? (Kvinner/Menn)



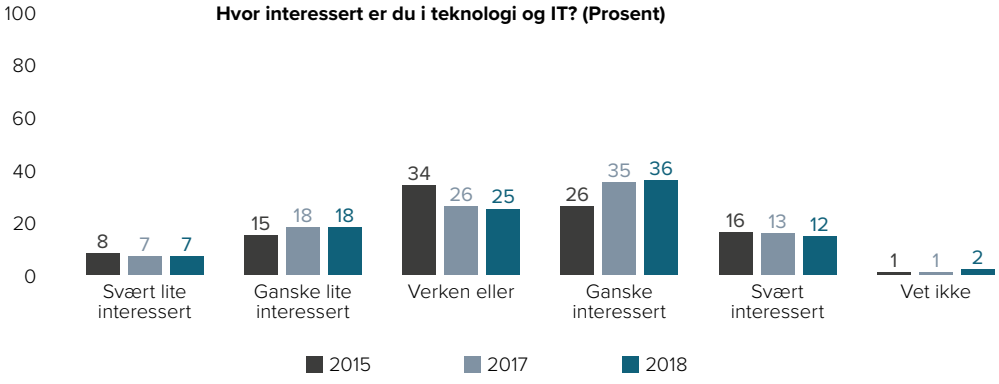
På spørsmålet Hvordan lærer du vanligvis om informasjonssikkerhet? oppgir 48 % at de hører om ting fra andre i en mer uformell situasjon, mens kun 18 % sier at de lærer på kurs eller utdanning. 21 % sier at de vanligvis prøver og feiler selv.

Figur 31:
Hvordan lærer du vanligvis om informasjonssikkerhet?


INTERESSE FOR
TEKNOLOGI OG
IT

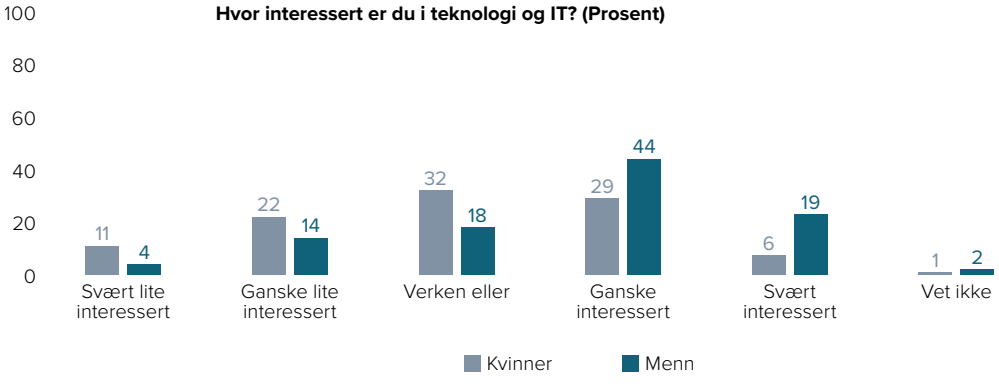
I VÅR HOVEDSTUDIE FRA 2016 slo vi fast at de som har interesse for teknologi og IT har en fordel i forhold til de som ikke har slike interesser. Interesser former våre holdninger, ferdigheter og kunnskaper. Interesse påvirker også hvem en assosierer seg med, og dermed hvem en lærer fra. Med interesse følger det bevissthet, nysgjerrighet og tid. Dette er hjørnestener i all læring. Som en følge av dette mener vi at de som har slike interesser lærer raskere og «riktigere» enn de som ikke har det. Vi mener at interesse er et av kjerneområdene i digital sikkerhetskultur og at det derfor er viktig for deltakelsen i et digitalisert samfunn.

Nesten halve befolkningen (48 %) forteller at de er interessert i teknologi og IT, mens 25 % sier at de er ganske lite eller svært lite interessert i dette.



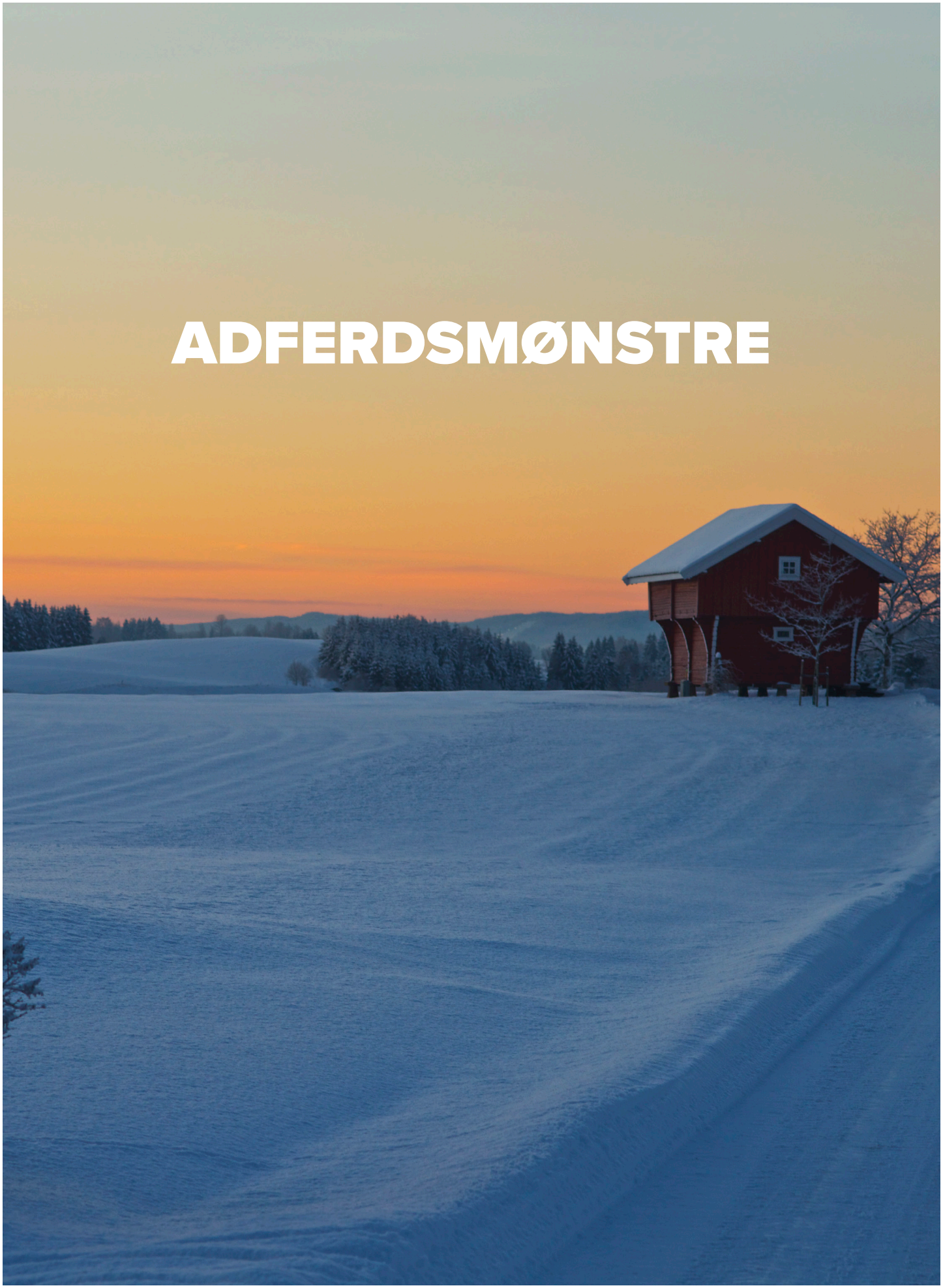
Figur 32:
Hvor interessert er du i teknologi og IT?

Vi observerer her forskjeller mellom kjønnene. Flere menn enn kvinner (19 % vs 6 %) sier at de er svært interessert i teknologi og IT, mens flere kvinner enn menn (11 % vs 4 %) sier at de er svært lite interessert.



Figur 33:
Hvor interessert er du i teknologi og IT? (Kvinner vs menn)

ADFERDSMØNSTRE



DE FLESTE STUDIER PÅ DIGITAL SIKKERHETSKULTUR FOKUSERER PÅ ADFERDSTREKK ELLER ADFERDSMØNSTRE.

Dette er ikke uten grunn. Det er langt enklere å kun se på adferd, og det er jo det vi faktisk gjør som har en direkte og konkret påvirkning på den digitale sikkerheten. For digital sikkerhet er det visse typer adferd det oppfordres til, mens det advareres mot andre typer adferd. Myndighetene, ledende selskaper og eksperter gir råd som i sum kan sees på som en normativ standard for hvordan innbyggerne og ansatte skal oppføre seg på nett. Når det er sagt, ekspertrådene og normene for «sikker adferd» har endret seg over tid. Det er en naturlig konsekvens av den raske utviklingen i teknologien og hvordan man tar teknologien i bruk. Det betyr at det ikke er tilstrekkelig å få opplæring én gang. Opplæring må gjentas. Det du lærte for 10 år siden er ikke bare utdatert, det kan være direkte feil.

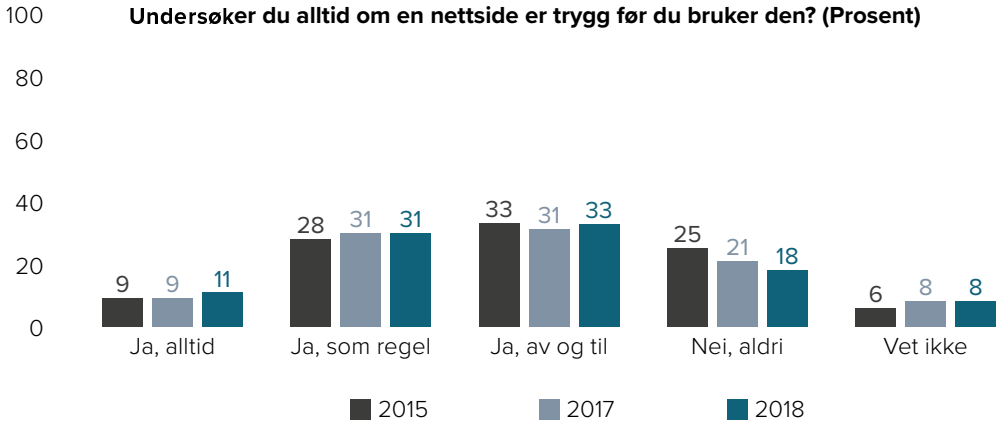
«OPPLÆRING MÅ GJENTAS. DET DU LÆRTE FOR 10 ÅR SIDEN ER IKKE BARE UTDATERT, DET KAN VÆRE DIREKTE FEIL.»

Når vi nå kartlegger digital sikkerhetskultur, legger vi til grunn at det er en rekke ting alle oppfordrers til å gjøre. Man bør ikke dele passordet sitt med andre, man bør ta sikkerhetskopi av viktige data og man bør sikkerhetsoppdatere programmene sine jevnlig. Dette er en del av dagens normative beskrivelse av hva sikker digital adferd er, og man oppfordrer til dette for å redusere faren for datakriminalitet, for tap av informasjon og for at du skal bli utsatt for manipulering og så videre.

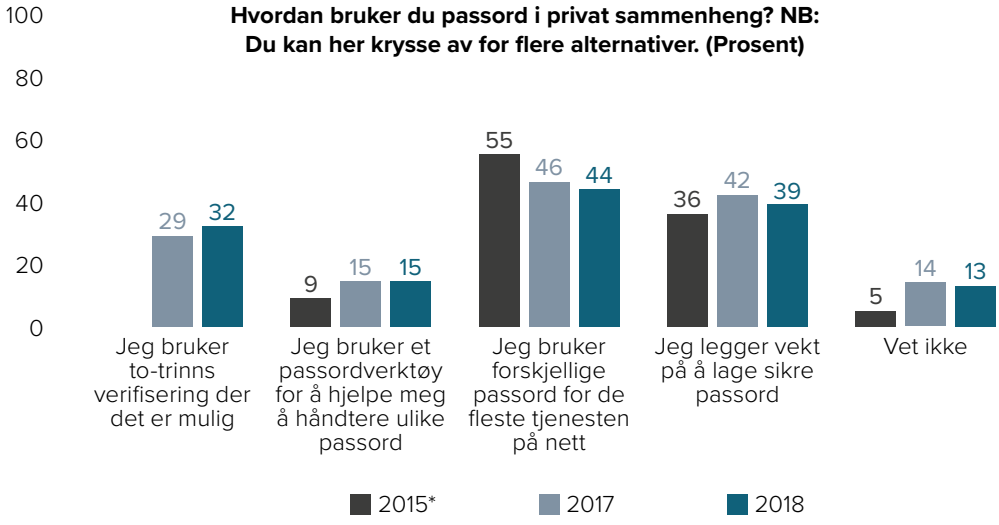
75 % forteller at de undersøker om en nettside er trygg før de bruker den, og 18 % sier at de aldri gjør dette. Tidligere har vi sett at 57 % mener at de er i stand til å vurdere hva som er trygt eller utrygt å gjøre på nett.

NorSIS erfarer at sikker bruk av passord er krevende for mange. Tidligere råd om passord anses idag som skadelig for sikkerheten. Kravene om at passordene skal være bygget opp av tilfeldige bokstaver, tall og spesialtegn (RyDH5#33) og at de må skiftes med jevne mellomrom, fører til at mange bruker det samme passordet over alt. Slike passord er vanskelige å huske for mennesker, og paradoksalt nok ganske lette for en datamaskin å finne frem til. I dag gir vi råd om å bruke lange passord som er lette å huske (strofe fra en bok eller sang), gjerne med en tilpassing til det enkelte nettsted slik at det er mulig å velge forskjellige passord på de fleste nettsteder. Et annet, og kanskje enda viktigere, råd er å skru på *to-trinns-verifisering* der det er mulig. Da vil det ikke være mulig å logge seg inn på nettkontoen, selv om passordet har kommet på avveier. For utfyllende råd om bruk av passord henviser vi til veiledningene på *nettvett.no.*

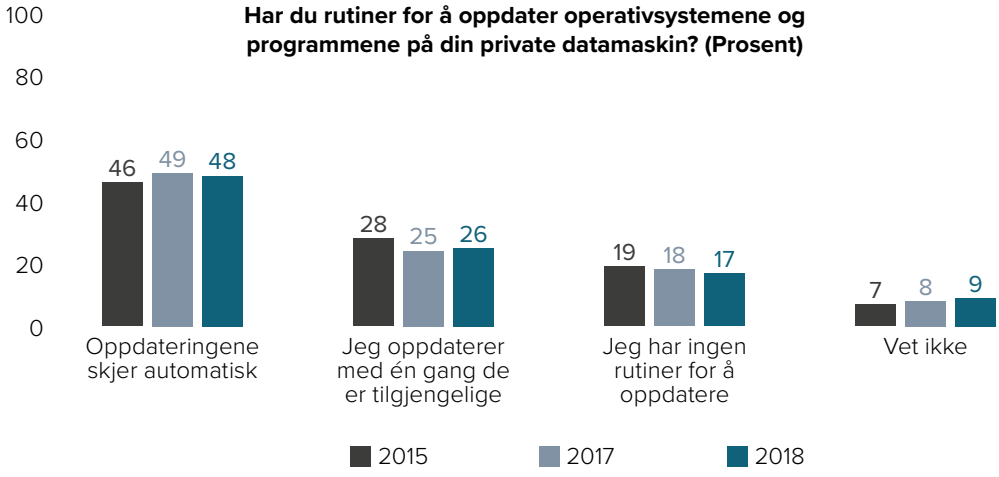
Figur 34: Undersøker du alltid om en nettside er trygg før du bruker den?



Figur 35: Hvordan bruker du passord i privat sammenheng?



Figur 36: Har du rutiner for å oppdatere operativ-systemene og programmene på din private datamaskin?

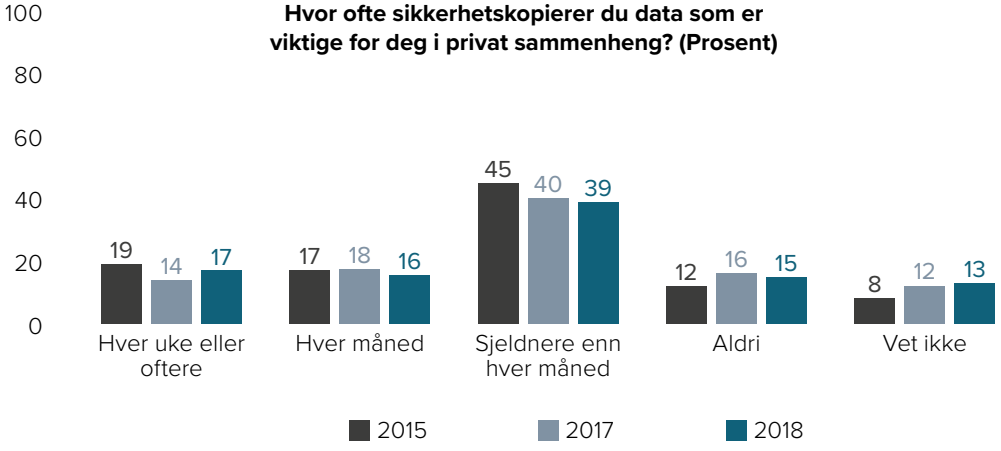


Kun 32 % av befolkningen sier at de bruker to-trinns verifisering der det er mulig. Vi ser her forskjeller mellom kjønnene, der 35 % av menn og 28 % av kvinner sier at de gjør dette. Det er også en forskjell mellom aldersgruppene. De over 55 er dårligst på dette (26 % mot 34 % i de øvrige aldersgruppene).

Bruk av et passordverktøy for å håndtere ulike passord er også noe NorSIS anbefaler, ikke minst fordi disse gir brukeren mulighet til å generere lange og tilfeldige passord som er enda vanskeligere å gjette eller finne frem til. Imidlertid er det kun 15 % av befolkningen som sier at de bruker slike verktøy. Også her er det de som er over 55 som er dårligst på dette. Kun 10 % bruker slike verktøy. En mulig forklaring på at så få oppgir at de bruker slike verktøy kan være at de krever en viss kunnskap. Det kan derfor være en kompetanseterskel som gjør at noen lar være å bruke slike verktøy.

17 % sier at de ikke har noen rutiner for å oppdatere programvare, og 9 % sier at de ikke vet om de har slike rutiner. 48 % sier at oppdateringene skjer autmatisk, og 26 % sier at de oppdaterer selv med én gang oppdateringene er tilgjengelige. NorSIS erfarer at det pågår et skifte når det gjelder sikkerhetsoppdatering av programmer og enheter. Mange enheter (mobiltelefoner, nettbrett), operativsystemer (f.eks. Windows, Mac og Linux) og større programvare begynner å få gode løsninger for automatisk oppdatering. Det betyr at brukeren i liten grad trenger å tenke på det. Enten oppdateres systemene uten noen handlinger fra brukeren, eller så får man et varsel der den enkelte kun trenger å trykke «godta» for at oppdateringen skal skje.

15 % sier at de aldri tar sikkerhetskopi av sine data og 13 % sier at de ikke vet om de gjør dette. De fleste som tar sikkerhetskopi (72 %) sier at de gjør dette sjeldnere enn hver måned.

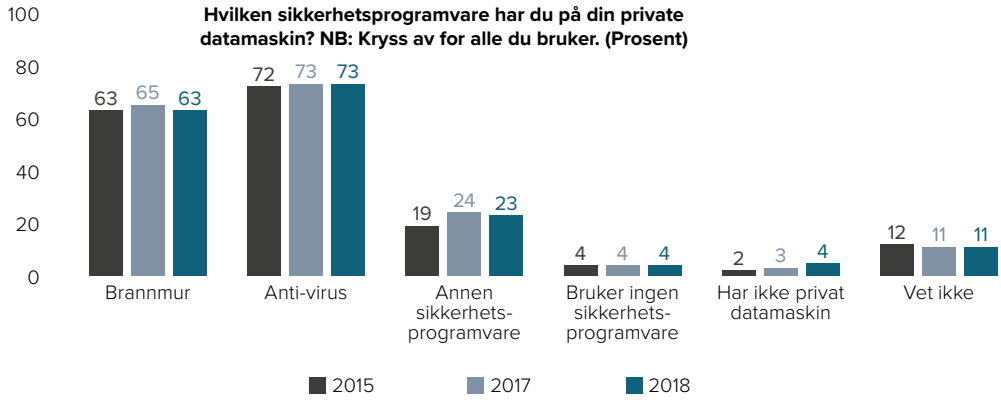


Figur 35: Hvor ofte sikkerhetskopierer du data som er viktige for deg i privat sammenheng?

Sikkerhetsprogramvare som antivirus, brannmurer og VPN-løsninger kan gi beskyttelse mot datakriminalitet og andre uønskede sikkerhetshendelser. Kun 4 % forteller at de ikke bruker noen former for sikkerhetsprogramvare, og 11 % sier at de ikke vet om de bruker slik programvare. 63 % oppgir at de bruker brannmur og 73 % oppgir at de bruker anti-virus.

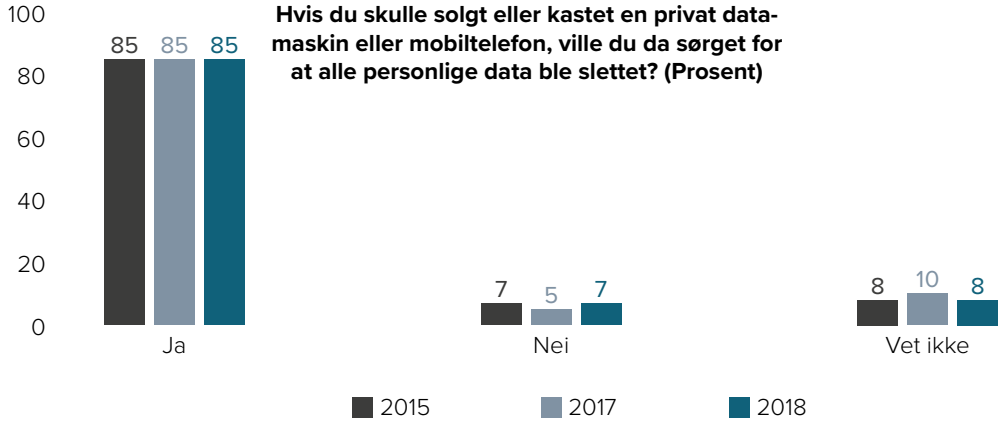
Vi kan anta at det i realiteten er enda flere som har brannmur på sine enheter fordi det er i dag vanlig at dette er en integrert del av alle moderne operativsystemer. Det er derfor ikke sikkert at dette er et valg som den enkelte i realiteten tar selv. Som en følge av det kan også være slik at mange ikke er klar over at de har slik sikkerhetsprogramvare.

Figur 35: Hvilken sikkerhetsprogramvare har du på din private datamaskin?



Nordmenn er generelt opptatt av personvern og å sørge for at deres personlige informasjon ikke kommer i hendene på uvedkommende. Datamaskiner og mobiltelefoner inneholder stadig mer personlig informasjon. Vi er interessert i å vite hvor mange som selv sørger for å slette slik informasjon før de kaster eller selger slike enheter.

Figur 35: Hvis du skulle solgt eller kastet en privat datamaskin eller mobiltelefon, ville du da sørget for at alle personlige data ble slettet?



KONKLUSJON

I RAPPORTEN «NORDMENN OG DIGITAL SIKKERHETSKULTUR 2017» slår vi fast at nordmenn er dårlig rustet til å møte den digitale revolusjonen.

Fordi både trusselbildet og det teknologiske landskapet er i endring, er det nødvendig at befolkningens kunnskap om hvordan en skal beskytte seg mot kriminalitet og andre uønskede hendelser på nett opdateres. Ettersom digitale enheter i de tusen hjem også kan brukes til å angripe grunnleggende samfunnsfunksjoner eller til å begå nettkriminalitet i stor skala, er det imidlertid ikke bare snakk om egenbeskyttelse. Den enkeltes holdninger til og oppførsel knyttet til digital sikkerhet kan derfor får store og direkte konsekvenser for samfunnet som helhet. I samme rapport slår vi også fast at frykt for digitale trusler og mistro til at politiet vil hjelpe dersom noe skjer, er skadelig for digitaliseringen av samfunnet. Årets rapport viser at situasjonen ikke har blitt vesentlig bedre. Konklusjonene fra forrige rapport er derfor fremdeles gyldige.

ØKENDE FRYKT

I årets undersøkelsen observerer vi at befolkningen har en økende frykt knyttet til deler av deres digitale liv. I 2018 mener flere at de utsetter seg selv for risiko på nett enn i 2015. Den gang svarte 58 % at de er helt eller delvis enig i påstanden om at de utsetter seg selv for risiko på nett, mens det i 2018 er 73 % som svarer det samme. Dette er en økning på 15 prosentpoeng. Samtidig opplever færre at de får tilstrekkelig informasjon om digitale trusler. I 2015 sa 68 % seg helt eller delvis enig i at de får tilstrekkelig informasjon om dette, mens det i 2018 er 61 % som sier det samme.

Flere forbinder også det å bruke offentlige tjenester på nett med høy risiko enn tidligere. I 2015 svarte 13 % at de i ganske stor eller svært stor grad forbinder slik bruk med høy risiko, mens det i 2018 er 21 % som svarer det samme. En økning på 8 prosentpoeng. Denne observasjonen understøttes også av at 30 % av de spurte ikke har tillit til at myndighetene sikrer informasjonen de har registrert om dem.

Vi gjør en tilsvarende observasjon for det å bruke nettbank, i 2018 forbinder flere det å bruke nettbank med høy risiko enn tidligere. I 2015 svarte 10 % at de forbinder slik bruk med høy risiko, mens det i 2018 er 19 % som svarer det samme. Det er en økning på 9 prosentpoeng.

NorSIS mener det er uheldig at flere oppfatter det mer risikabelt å nettbank og andre digitale tjenster enn tidligere. Vi vet imidlertid ikke nok om bakgrunnen for denne økningen. En mulig forklaring er at risikoen knyttet til slik bruk faktisk har økt. NSM skriver i sin rapport Risiko 2018 at Norge står overfor økende risiko for å bli rammet av sikkerhetstruende hendelser, men rapporten sier ikke spesifikt at dette gjelder bruk av nettbank eller offentlige tjenester på nett.

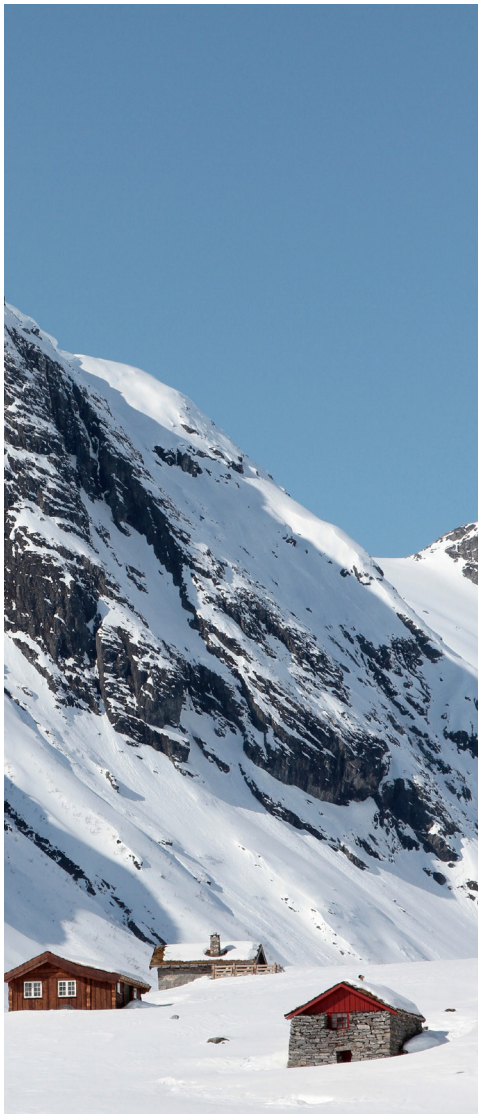
Vi kan imidlertid ikke utelukke at risikoen faktisk øker, og at endringen i befolkningens oppfatning kommer som en følge av dette.

En annen mulig forklaring er at folk tror at risikoen øker, uten at den faktisk gjør det. Dette er i så fall også problematisk, for det kan tyde på at informasjonen omkring slik risiko enten er mangelfull eller feilaktig. NorSIS antar at kunnskap om risiko spiller en rolle her, og minner om at mindre enn en fjerdedel av befolkningen sier at de har fått opplæring i digital sikkerhet i løpet av de siste to årene. Kunnskap alene styrer ikke nødvendigvis hva befolkningen mener om risiko, men NorSIS mener likevel at det er av svært stor betydning at flere nordmenn før opplæring i nettvett.

Vi ønsker at nordmenn skal utvise sikker adferd på nett, og på den måten forebygge uønskede hendelser. Men på tross av god forebygging, går det noen ganger galt. Når dette skjer er samfunnets motstandsdyktighet mot digitale trusler også avhengig av hva den enkelte vet om slike trusler, og hvordan de forholder seg til dem.

I september 2018 observerte NorSIS en stor økning av forsøk på utpressing av norske innbyggere. Mange, trolig flere tusen, mottok en epost der avsender hevdet å ha brukt datamaskinens kamera til å filme vedkommende mens han eller hun onanerte foran skjermen.

Avsenderen truet med å dele filmen med mottagerens venner på facebook, dersom det ikke ble betalt inn et større beløp til utpresseren innen en gitt frist.



Vår felles digitale sikkerhetskultur påvirker hva den enkelte gjør når en får slike trusler. Blir man engstelig for at utpresseren faktisk sitter på en slik video, og derfor betaler det som kreves? Gjenkjenner man det som en falsk trussel og sletter eposten? Søker man hjelp fra eksperter for å finne ut hva dette er? Informerer man sine venner om at dette er en trussel som også kan ramme dem, og gir råd om hva de bør gjøre?

Å redusere frykten for å bruke digitale tjenester bør være et mål for samfunnet. Det er mange som deler ansvaret for å oppnå dette. Myndighetene må sørge for at det finnes tidsriktig informasjon om trusselbildet. Deretter må de sammen med sikkerhetsbransjen og andre aktører som arbeider for digital sikkerhet, sørge for gode og effektive tiltak som både enkeltpersoner og bedrifter kan bruke for å møte truslene som finnes.

«HOVEDINNTRYKKET FRA ÅRETS UNDERSØKELSE ER AT DET IKKE ER STORE ENDRINGER I BEFOLKNINGENS SIKKERHETSKULTUR FRA UNDERSØKELSENE I 2015 OG 2017.»

PÅ STEDET HVIL

Hovedinntrykket etter årets undersøkelse er at det jevnt over ikke er store endringer i befolkningens sikkerhetskultur fra undersøkelsene i 2015 og 2017. Selv om vi skal være tilfreds med at det ikke har blitt verre på noen områder, er vi ikke tilfreds med at det ikke har blitt bedre. Særlig på områder der vi forventer en positiv fremgang.

Det er fremdeles færre enn 25 % av de spurte som sier at de har fått opplæring i løpet av de to siste årene. Videre er det kun en tredjedel av de spurte som sier at de bruker to-trinnsbekreftelse der det er mulig. Dette til tross for at det er et av de aller viktigste tiltakene man kan gjøre for å beskytte seg mot mange former for digitale trusler. Vi observerer ut fra dette, lite bevegelse i både holdninger og adferd rundt digital sikkerhet fra 2015 til 2018.

Undersøkelsen i seg selv gir ikke svaret på hvorfor det er slik. Det er mange aktører i Norge som bidrar til å gi befolkningen økt kunnskap og større bevissthet rundt digitale trusler. Myndighetene, skolene, virksomheter i offentlig og privat sektor, bransjeorganisasjoner, aktører i sikkerhetsbransjen og enkeltpersoner bidrar alle til dette. Når vi likevel ikke finner noen endringer i befolkningen på flere viktige områder, er det riktig å stille spørsmål ved om den samlede innsatsen har den effekten som samfunnet har behov for.

Dette er selvsagt en svært sammensatt og kompleks problemstilling. Å endre holdninger og adferd er utfordrende. Det gjør heller ikke oppgaven enklere at det ikke foreligger noe tydelig og omforent målbilde for digital sikkerhetskompetanse i befolkningen. I forbindelse med lansering av ny nasjonal strategi for digital sikkerhet, vil Justis- og beredskapsdepartementet også gi ut en egen kompetansestrategi. Hvordan denne følges opp, vil ha stor betydning for befolkningens digitale sikkerhetskultur i tiden fremover.

NorSIS forutsetter at strategimålene er tydelige, og at departementet evaluerer måloppnåel-

sen i årene fremover. Våre årlige undersøkelser om nordmenns digitale sikkerhetskultur bør inngå som et viktig grunnlag i evalueringene.

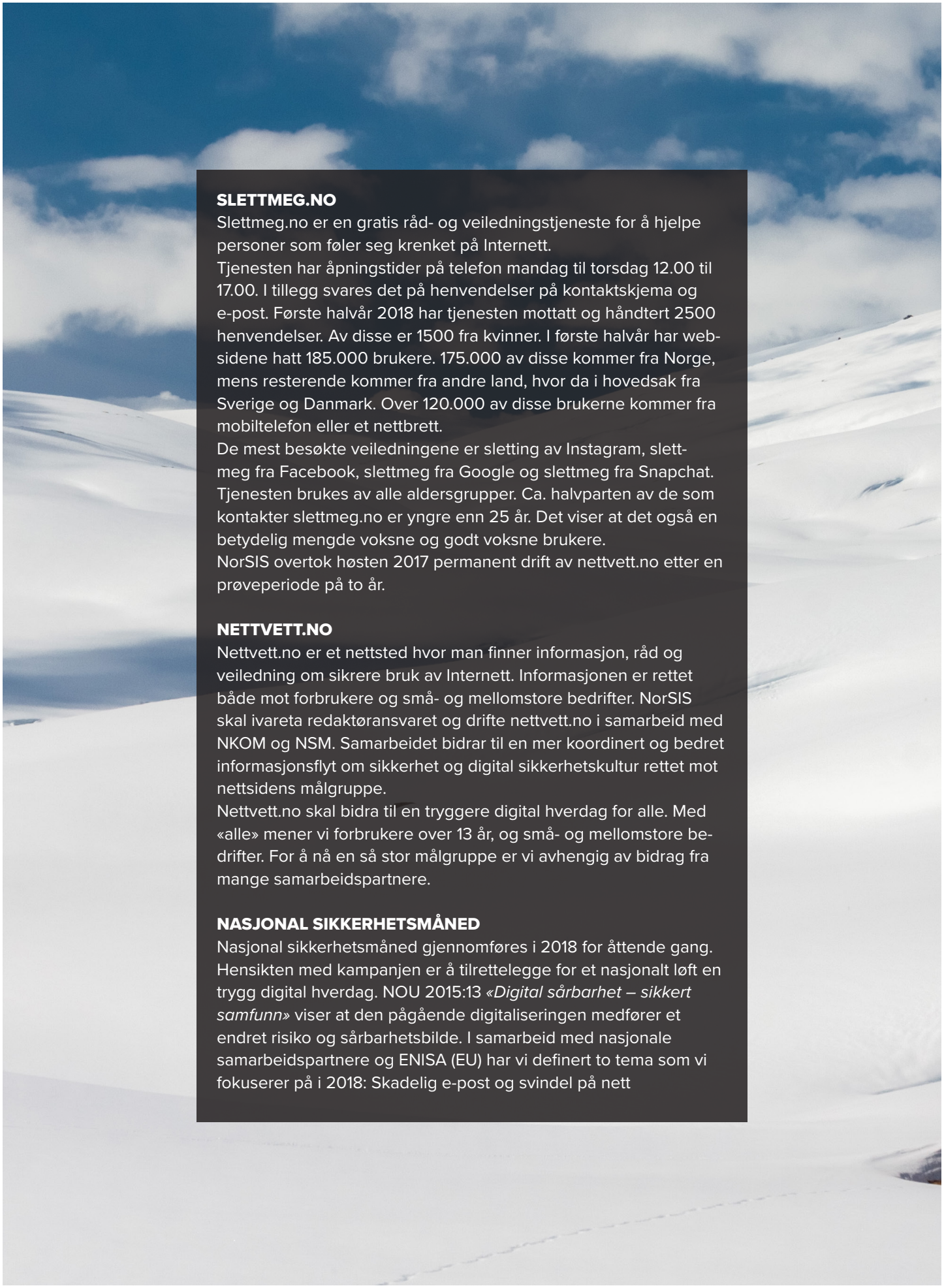
For å skape de endringene vi mener er nødvendige, er det imidlertid ikke bare regjeringen og departementene som må ha en mer målrettet innsats. Det er mange som har en stemme i det offentlige ordskiftet. Disse bidrar til å lære opp og til å endre holdninger og adferd hos folk flest. NorSIS mener myndighetsaktørene, slik som *Nasjonal sikkerhetsmyndighet, Nasjonal kommunikasjonsmyndighet, Direktoratet for sikkerhet og beredskap* og *Utdanningsdirektoratet,* har et særskilt ansvar å utvikle og evaluere tiltak for å endre befolkningens digitale sikkerhetskultur. NorSIS anbefaler også at alle aktører som gir råd og opplæring til den enkelte innbygger har tydelige mål for sine aktiviteter og at disse også er gjenstand for evaluering.

NorSIS har gjennom sitt oppdrag et tydelig medansvar for å bidra til befolkningens kunnskaper, holdninger og en adferd som gjør dem til trygge digitale innbyggere. NorSIS har samarbeidsavtaler med flere av de nevnte myndighetsaktørene, og det er viktig at NorSIS sammen med sine partnere evaluerer egen og felles tilnærming til å løse utfordringen slik at effekten av dette arbeidet styrkes. NorSIS har tradisjonelt tilnærmet seg de ulike målgruppene på forskjellige måter. Norske bedrifter har fått anledning til å gjennomføre sikkerhetsopplæring i forbindelse med Nasjonal sikkerhetsmåned som koordineres av NorSIS. I Nasjonal sikkerhetsmåned gis bedriftene mulighet til å kjøpe en tidsriktig opplæringspakke. Denne er gratis for bedrifter med opp til 20 ansatte. Kanalene for å nå den enkelte innbygger har i hovedsak vært medieoppslag i sosiale medier, aviser, radio og fjernsyn, og gjennom veiledninger på *nettvett.no.*

NorSIS tar nå nye grep for å sikre at den enkelte får mulighet til å skaffe seg mer og bedre informasjon om hvordan de bør forholde seg til digitale trusler. Som en del av Nasjonal sikkerhetsmåned i 2018 utvides opplæringstilbudet til også å omfatte den enkelte innbygger, ikke bare ansatte i norske bedrifter. Vi mener at dette vil føre til at befolkningen i enda større grad følger de råd og anbefalinger som gis.

Om den nye nasjonale kompetansestrategien, og den samlede innsatsen fra alle sikkerhetsaktørene, gjør Norge til et trygt sted å være en digital innbygger vil vise seg i årene som kommer. NorSIS vil på sin side kontinuerlig evaluere effekten av egne tiltak. Vi vil også arbeide for at alle sikkerhetsaktører har et oppdatert situasjonsbilde på nordmenns digitale sikkerhetskultur.

NORSK SENTER FOR INFORMASJONSSIKRING, 2018



SLETTMEG.NO

Slettmeg.no er en gratis råd- og veiledningstjeneste for å hjelpe personer som føler seg krenket på Internett.
Tjenesten har åpningstider på telefon mandag til torsdag 12.00 til 17.00. I tillegg svares det på henvendelser på kontaktskjema og e-post. Første halvår 2018 har tjenesten mottatt og håndtert 2500 henvendelser. Av disse er 1500 fra kvinner. I første halvår har websidene hatt 185.000 brukere. 175.000 av disse kommer fra Norge, mens resterende kommer fra andre land, hvor da i hovedsak fra Sverige og Danmark. Over 120.000 av disse brukerne kommer fra mobiltelefon eller et nettbrett.
De mest besøkte veiledningene er sletting av Instagram, slettmeg fra Facebook, slettmeg fra Google og slettmeg fra Snapchat.
Tjenesten brukes av alle aldersgrupper. Ca. halvparten av de som kontakter slettmeg.no er yngre enn 25 år. Det viser at det også en betydelig mengde voksne og godt voksne brukere.
NorSIS overtok høsten 2017 permanent drift av nettvett.no etter en prøveperiode på to år.

NETTVETT.NO

Nettvett.no er et nettsted hvor man finner informasjon, råd og veiledning om sikrere bruk av Internett. Informasjonen er rettet både mot forbrukere og små- og mellomstore bedrifter. NorSIS skal ivareta redaktøransvaret og drifte nettvett.no i samarbeid med NKOM og NSM. Samarbeidet bidrar til en mer koordinert og bedret informasjonsflyt om sikkerhet og digital sikkerhetskultur rettet mot nettsidens målgruppe.
Nettvett.no skal bidra til en tryggere digital hverdag for alle. Med «alle» mener vi forbrukere over 13 år, og små- og mellomstore bedrifter. For å nå en så stor målgruppe er vi avhengig av bidrag fra mange samarbeidspartnere.

NASJONAL SIKKERHETSMÅNED

Nasjonal sikkerhetsmåned gjennomføres i 2018 for åttende gang. Hensikten med kampanjen er å tilrettelegge for et nasjonalt løft en trygg digital hverdag. NOU 2015:13 *«Digital sårbarhet – sikkert samfunn»* viser at den pågående digitaliseringen medfører et endret risiko og sårbarhetsbilde. I samarbeid med nasjonale samarbeidspartnere og ENISA (EU) har vi definert to tema som vi fokuserer på i 2018: Skadelig e-post og svindel på nett

Teknologiveien 22
2815 Gjøvik
Org.nr. 995195003
ISBN: 978-82-93651-02-4

Telefon: 40 00 58 99
www.norsis.no
post@norsis.no