NORDMENN OG DIGITAL SIKKERHETSKULTUR 2020

Kommentar til årets befolkningsundersøkelse
av Bjarte Malmedal

NorSIS
Norsk senter for informasjonssikring

INNHOLD

Ansvarlig utgiver: Norsk senter for informasjonssikring
Forfatter: Bjarte Malmedal
Design: Nano Design
Foto: Getty Images
ISSN: 2535-7816

Undersøkelsen er gjennomført av analyseinstituttet YouGov. Det er i uke 14-15 gjennomført til sammen 1000 CAWI[1] -intervjuer i et landsrepresentativt utvalg 18+ år.

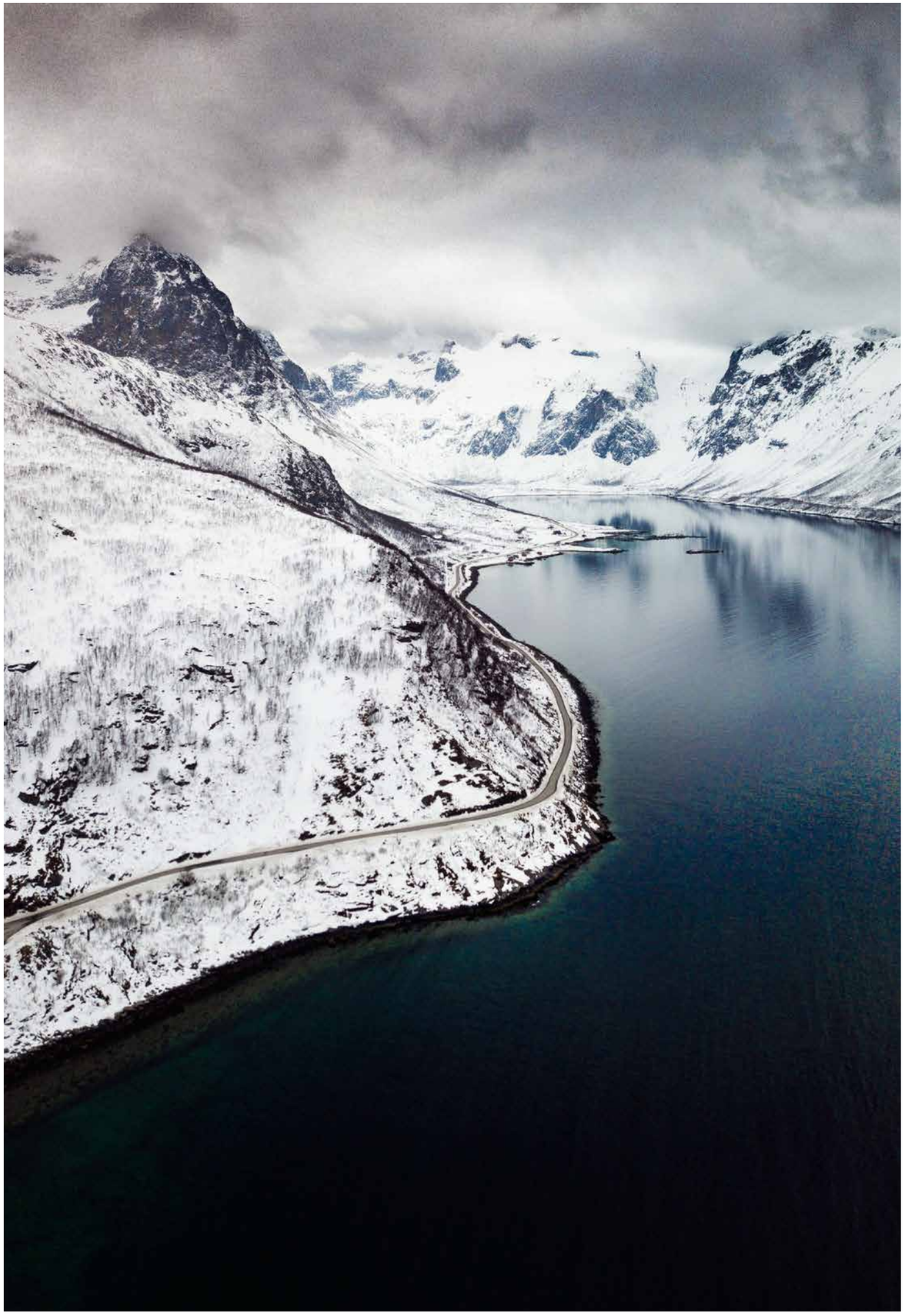
INNLEDNING

Det er viktig å vite hvordan befolkningen og virksomheter forholder seg til digitalisering og opplæring innen informasjonssikkerhet. Norsk senter for informasjonssikring (NorSIS) har derfor siden 2016 årlig gitt ut en rapport hvor befolkningens digitale sikkerhetskultur blir kartlagt over tid.

I den store undersøkelsen, som ligger til grunn for rapporten, blir mer enn 1500 nordmenn stilt en rekke spørsmål om deres digitale sikkerhetskultur. Kommentarer og analyse av tallmateriale er gjort av Bjarte Malmedal. Han har tidligere jobbet for NorSIS med undersøkelsen og har vært med å utvikle metodene som er benyttet i rapporten.

Den årlige undersøkelsen, samt Malmedals analyser av denne, gir et verdifullt innblikk i hvordan det står til med nordmenns digitale sikkerhetskultur og hvordan den har utviklet seg over tid.

God lesing,
fra oss i NorSIS!



FORORD

av forfatter Bjarte Malmedal

Norsk Senter for informasjonssikring har siden 2016 gitt ut årlige rapporter om befolkningens digitale sikkerhetskultur. I et samfunn som bare blir mer og mer digitalisert, er kunnskap om hvordan befolkningen forholder seg til digital sikkerhet viktig. Det er mye som står på spill, for digital kriminalitet kan ramme både enkeltmennesket og norske virksomheter. Det kan være svært alvorlig for den som blir rammet, men digital sikkerhet handler også om mer: selve deltakelsen i et trygt digitalt samfunn.

I de tidligere rapportene har vi sett at den enkeltes holdninger til det digitale og til digital sikkerhet er en faktor som påvirker digitaliseringen. Kunnskap om hva man skal gjøre for å passe på sin egen og andres sikkerhet, frykt og tillit til hverandre og til digitale tjenester og de normene som oppstår i samfunnet omkring hvordan vi skal oppføre oss på nett bidrar til å forme hvilke digitale tjenester vi bruker, og hvilke vi skyr unna. Kultur er et menneskelig fenomen. Vi mennesker blir påvirket av kulturen vi er en del av, og vi påvirker samtidig den samme kulturen. Kulturen endrer oss, og vi endrer kulturen.

2020 er et år preget av stor endring i hvordan vi forholder oss til det digitale. Da Covid-19 inntok Norge i mars medførte det strenge tiltak i samfunnet. Man kunne blant annet ikke lenger reise fritt der man ønsket, eller samles i større grupper. Hjemmekontor og arbeid over digitale løsninger ble raskt noe svært mange måtte forholde seg til.

Endringer i hvordan vi bruker digitale løsninger, og de påfølgende endringene i trusselbildet, er en av grunnene til at rapportene om digital sikkerhetskultur er viktige. For det første gir årlige kartlegginger av digital sikkerhetskultur en innsikt i hvordan befolkningen påvirkes av hendelser i samfunnet. For det andre kan slike kartlegginger avdekke områder som politisk ledelse, sikkerhetsmyndigheter, sikkerhetsbransjen og næringslivet kan bli nødt til å gjøre noe med.

Årets undersøkelse avdekker neppe alle svar om hvordan endringene i 2020 vil påvirke oss på sikt. Undersøkelsen indikerer imidlertid at nordmenn har endret syn på digital sikkerhet etter at Covid-19 kom til Norge i starten av året. Jeg regner med at fremtidige undersøkelser vil gi oss verdifulle svar om langtidseffektene dette har hatt.

Jeg har også lagt til to tematiske områder i årets undersøkelse. For det første ser jeg nærmere på hvordan Covid-19 har påvirket befolkningens holdninger til digital sikkerhet. For det andre løfter jeg frem den kognitive motivasjonsfaktoren mestringsforventning (eng: Self-efficacy) som er en sterk prediktor for atferdsendring.

Som seniorrådgiver i NorSIS fikk jeg anledning til å forfatte deres tidligere rapporter om digital sikkerhetskultur i befolkningen. Da jeg ble spurt om å gi min tolkning av årets befolkningsundersøkelse, så jeg det både som en stor ære og en mulighet til å bidra med min fagkompetanse innen digital sikkerhet.

Jeg håper at årets rapport er til nytte for alle som arbeider med digital sikkerhetskultur.

Bjarte Malmedal

METODE

I hovedstudien fra 2016 utviklet NorSIS et konsept for å beskrive digital sikkerhetskultur og en metode for å kartlegge den. Jeg henviser til hovedstudien[2] for en grundigere beskrivelse av metoden og det teoretiske grunnlaget for den. Denne rapporten baserer seg på data som er innhentet gjennom befolkningsundersøkelser utført av YouGov i 2015 og 2017-2020.

Befolkningsundersøkelsen i 2015 var en pilot-undersøkelse som ble gjennomført som en del av kvalitetssikringen i prosjektet som ledet frem til hovedstudien. Enkelte spørsmål ble i etterkant endret, fjernet eller lagt til. I årets undersøkelse er ytterligere spørsmål fjernet, endret eller lagt til. Når jeg i denne rapporten gjør sammenligninger over tid, er det kun for de spørsmål som er like i alle undersøkelsene. Jeg benytter en kvalitativ vurdering der flere indikatorer sammen bidrar til en samlet vurdering.

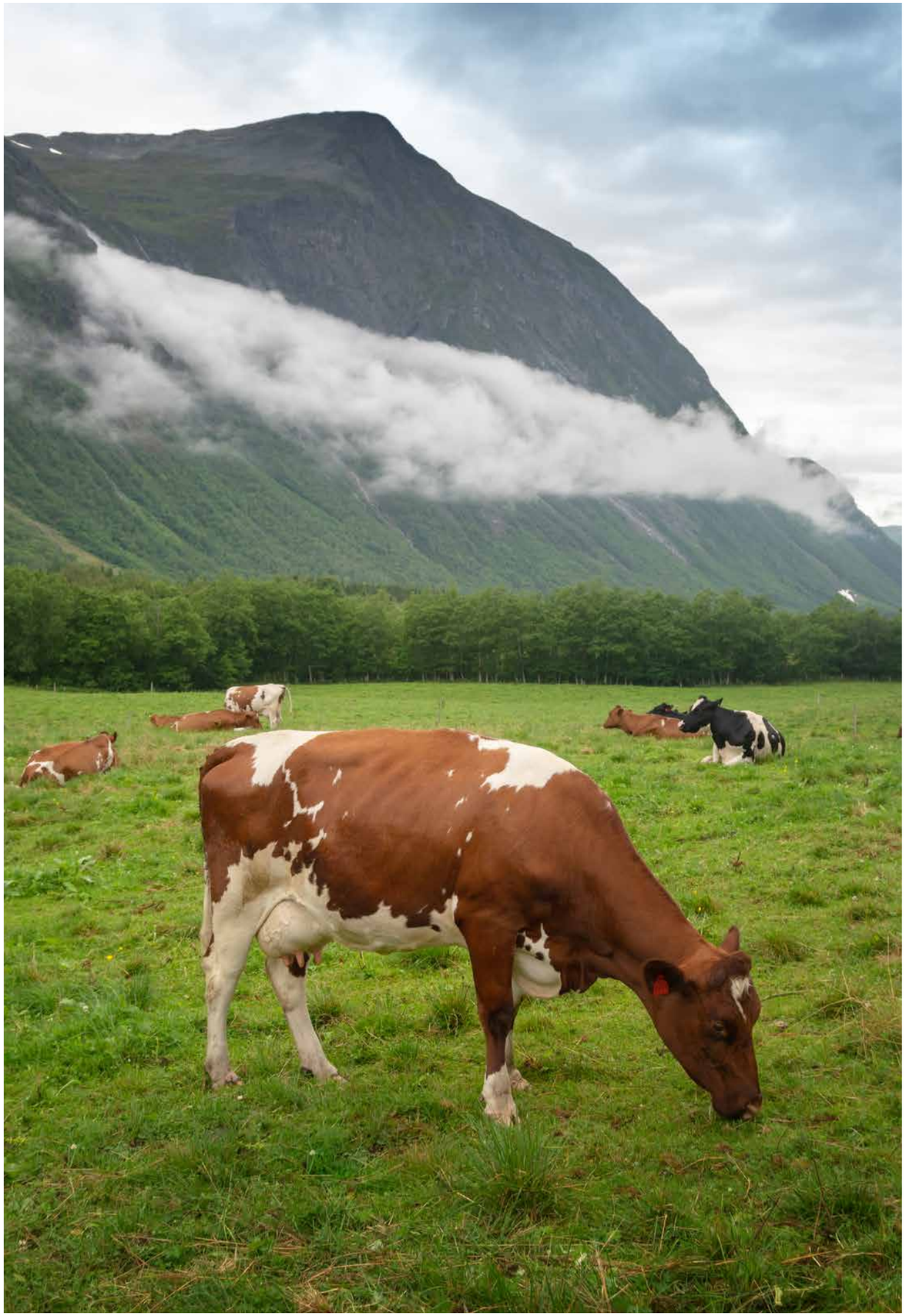
NorSIS har i 2019 og 2020 ledet et delprosjekt i Digitaliseringsdirektoratet, der målet var å tilpasse metoden for kartlegging i befolkningen, til bruk i virksomheter i statsforvaltningen. Leveransene i delprosjektet har vært et grunnlag for å revidere metoden for befolkningsundersøkelsene, og både struktur og indikatorer (spørsmålene som stilles) har i år blitt endret i noen tilfeller. Denne revisjonen både styrker kvaliteten i datainnsamlingen, og forenkler bruken av rapporten. I denne rapporten brukes digital sikkerhetskultur og informasjonssikkerhetskultur som synonymer.

Analyse

Årets undersøkelse er gjennomført i uke 14-15 i 2020 blant medlemmer av YouGov sitt forbrukerpanel i Norge. Dette er et landsrepresentativt utvalg mellom 18 og 74 år.

Data vektes med dimensjonene kjønn, alder og geografi på bakgrunn av et ideal fra Statistisk Sentralbyrå, slik at resultatene er representative for befolkningen med hensyn til ovennevnte målgruppe.

Det er gjennomgående benyttet gjennomsnitt som sentraltendens i analysene. Variablene er stort sett nominale eller ordinale med få responskategorier (færre enn fem). Tallmaterialet er testet for signifikante avvik mellom grupper ved bruk av T-test. Det er valgt et konfidensintervall på 95%. Feilmarginen er ca. 3%. R=1000. YouGov runder av alle resultater til nærmeste heltall.



DIGITAL SIKKERHETSKULTUR

Digital sikkerhetskultur er våre felles verdier, holdninger, normer, kunnskaper og handlinger som bidrar til at vi unngår å bli rammet av digitale trusler. Sosiale normer regulerer hvordan mennesker oppfører seg i ulike situasjoner. Alle grupper har normer, enten det er mindre grupper, eller samfunnet som helhet. Vi sier gjerne at man i slike grupper har en kultur, og de sosiale normene er en veiviser for gruppen. De er et sett med regler for hvordan man gjør ting i gruppen, og et kompass som hjelper den enkelte til å forstå hva som er rett og galt, eller trygt og utrygt. Normene utgjør et lim mellom menneskene i gruppen. De hjelper oss til å definere oss selv inn som en del av et fellesskap, eller ut av det. Normene får ting gjort[3]; de hjelper grupper av mennesker til å gjøre ting på samme måte, og de hjelper oss å gjøre ting mer effektivt og nøyaktig.

NorSIS har utviklet en metode for å kartlegge digital sikkerhetskultur, og denne ligger til grunn for denne rapporten.

Digital sikkerhetskultur består av følgende områder:

- Holdninger til digitalisering og digital sikkerhet
- Tillit og risikooppfattelse
- Synet på styring og kontroll
- Sikkerhetsatferd
- Kunnskap, læring og interesse

Holdninger til digitalisering og digital sikkerhet

Noen kulturer er mer individualistiske, det vil si at de setter individet mer i fokus, mens andre kulturer er mer orientert mot fellesskapets behov. I konteksten digital sikkerhetskultur kan det bety at enkelte velger å følge regler for digital sikkerhet, selv om de kan virke hemmende på dem. Eller at den enkelte velger å stå frem når de har gjort en sikkerhetstabbe slik at fellesskapet kan kunne lære av det, selv om det er belastende for den det gjelder.

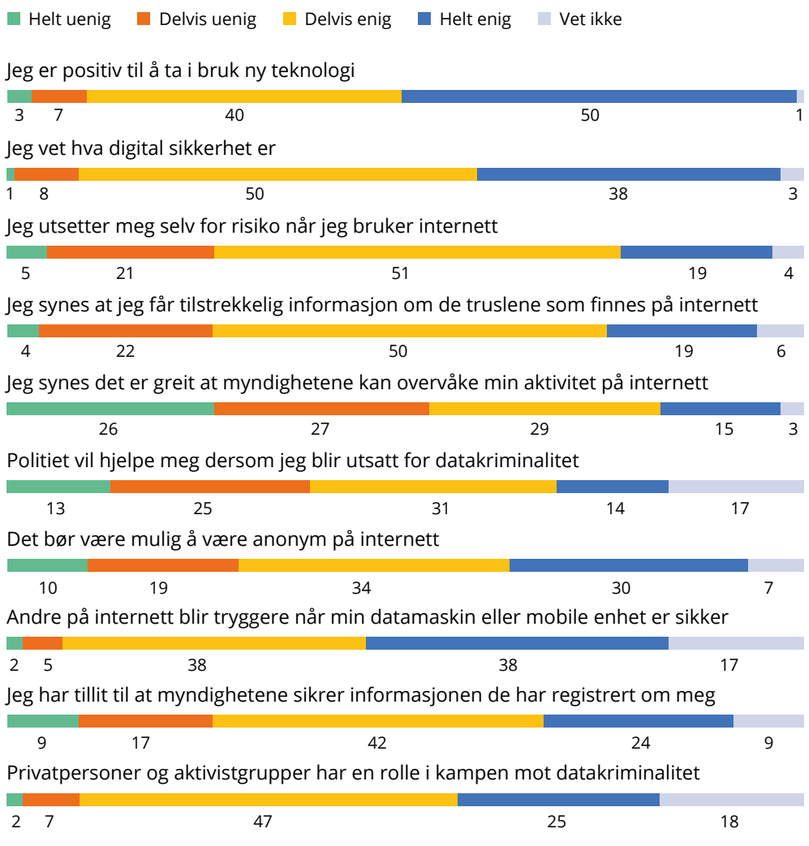
Arbeid med digital sikkerhetskultur handler derfor blant annet om hvordan man forholder seg til fellesskapet. Som samfunn bør vi ha tanker om hva det *digitale fellesskapet* skal være. Dette uttrykkes gjerne ved å definere hvilke felles normer og atferdsmønstre en ønsker at samfunnet skal ha innen digital sikkerhet. Noe av dette handler om hvilket ansvar man ønsker at den enkelte skal ta for den digitale sikkerheten til fellesskapet han eller hun er en del av. Debattsidene i fagpressen eller innlegg i sosiale medier er synlige tegn på hvordan enkeltmennesker tar ansvar for normdannelsen i det digitale fellesskapet. Våren 2020 har vi sett at mange bidrar med synspunkter på hvordan man skal arbeide med sikkerhet i en tid hvor mange jobber hjemmefra.

Vi har sett innlegg for og imot den nye loven for Etterretningstjenesten (digitalt grenseforsvar). En kan også se hvordan de mer etablerte strukturene påvirker synet på grensegangen mellom hva som er fellesskapets ansvar og hva som er den enkeltes ansvar. For eksempel i hvordan forsikringsselskapene trekker opp ansvarsgrensene, eller politiets prioriteringer når noe har skjedd.

Digital sikkerhetskultur handler også om den enkeltes optimisme for teknologi og digitalisering. Holdningene til digitalisering og digitale tjenester påvirker måten man forholder seg til teknologi. Mistillit til digitale tjenester, eller frykt for sikkerhetshendelser og datakriminalitet, er noen av utfordringene som de fleste må forholde seg til. Hvordan digitale tjenester utvikles og tilbys, hvordan sikkerheten ivaretas, hvilke sikkerhetshendelser som skjer og hvordan de blir håndtert, vil påvirke holdningene til det digitale. I 2020 har vi blant annet sett dette komme til uttrykk i diskusjonene omkring Smittestopp-appen til Folkehelseinstituttet. Den enkeltes holdning til det digitale blir derfor en faktor som både kan bidra til å beskrive den digitale sikkerhetskulturen, og en faktor som kan påvirke bruken av digitale tjenester i positiv eller negativ retning.

I undersøkelsen bes respondentene ta stilling til følgende påstander:

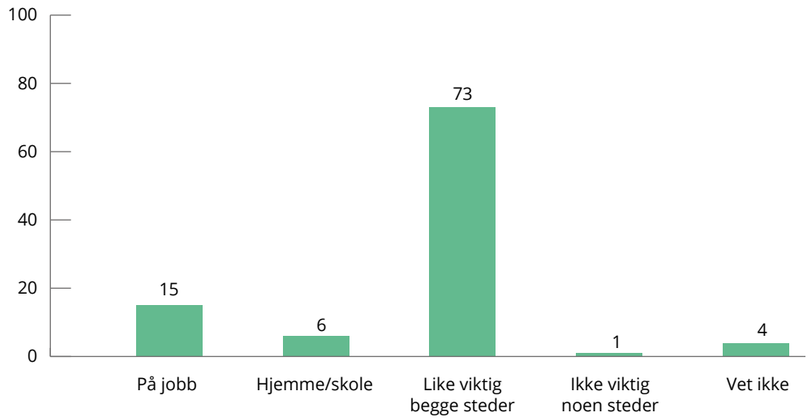
Hvor enig eller uenig er du i følgende påstander? (Prosent)



Det er ingen vesentlige endringer i resultatene sammenlignet med undersøkelsen i 2019.

Respondentene blir også bedt om på svare på hvor de synes det er viktigst å tenke på informasjonssikkerhet.

Hvor synes du at det er viktigst å tenke på informasjonssikkerhet? (Prosent)

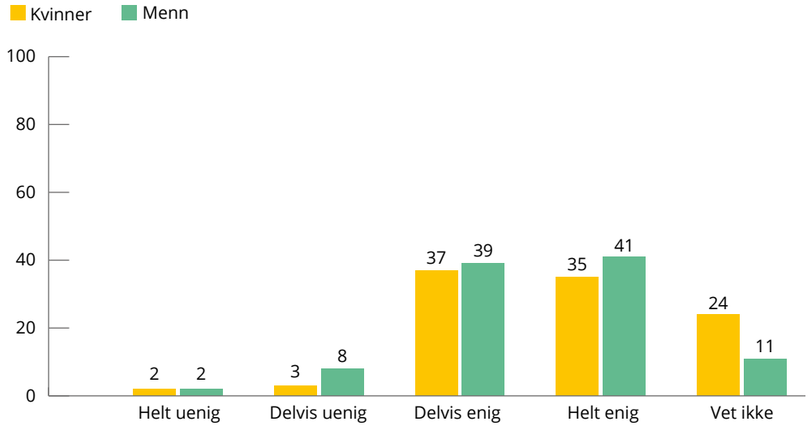


De fleste svarer at det er like viktig begge steder, mens mer enn dobbelt så mange svarer «Hjemme» enn de som svarer «På jobb eller skolen». Dette kan være et uttrykk for at de truslene som kan ramme den enkelte direkte også er de som oppleves som mest viktig. En annen forklaring kan være at mye av undersøkelsen dreier seg om privat bruk, og at det bidrar til å skape et «ønskverdighetsbias[4]» hos de som svarer.

Tre av fire svarer imidlertid at det er like viktig begge steder. Dette er et godt utgangspunkt for å innse at sikkerheten hjemme og på jobb eller skole påvirker hverandre gjensidig. Dersom man gjenbruker passord hjemme og på jobb, vil det kunne medføre en økt risiko dersom for eksempel Netflix-passordet kommer på avveie, og man har brukt det samme passordet på jobb. For en angriper kan dette være en enkel måte å skaffe seg tilgang til arbeidsplassens datasystemer. Bruk av privat utstyr til arbeidsoppgaver er et annet eksempel der dårlig sikkerhet hjemme, kan føre til problemer på jobb.

I undersøkelsen ønsker man å vite mer om hvordan befolkningen vurderer hvilken effekt det har på fellesskapet at de selv har fokus på sikkerhet. Respondentene bes derfor om å ta stilling til påstanden *«Andre på internett blir tryggere når min datamaskin eller mobile enhet er sikker»*.

Andre på internett blir tryggere når min datamaskin eller mobile enhet er sikker. Kjønnsforskjeller. (Prosent)



Her forekommer det signifikante kjønnsforskjeller, primært at kvinner i større grad svarer at de ikke vet. Det finnes åpenbart ikke et riktig eller galt svar her. Noen digitale angrep er bare mulig dersom andre ikke har sikret sine digitale enheter, men det er selvsagt slik at andre kan være like utsatt for risiko på nett, selv om du har gjort alt du kan for å sikre dine enheter. Det er likevel interessant å observere at de fleste er enten helt eller delvis enige i påstanden. Dette kan tyde på at det er en utbredt forståelse i befolkningen om at det vi gjør for å sikre oss selv, også vil kunne ha en betydning for sikkerheten til andre.

Årets undersøkelse avsluttes med et åpent spørsmål til respondentene: *Hva mener du er hovedutfordringen med digital sikkerhet?* Generelt peker svarene i retning av følgende hovedkategorier:

- Den enkelte har for lite informasjon eller for dårlige ferdigheter til å kunne beskytte seg selv
- De eksterne truslene (for eksempel kriminelle) er så avanserte at man ikke klarer å beskytte seg selv
- Utviklingen går for raskt, eller det er for komplekst å sørge for god beskyttelse

Her gjengis et utvalg av svarene på dette spørsmålet:

- Den eldre generasjonen har og får lite informasjon om det.
- Digital sikkerhet forandrer seg fort
- Svindlerne blir dyktigere
- Å kunne vite hvilke nettsteder som er sikre.
- At folk ikke vet nok om det
- For liten enhetlig informasjon til oss forbrukere
- At det finnes ingen absolutt sikkerhet og at offentlige institusjoner ønsker at programmer skal ha bakdører sånn at de kan snike seg inn
- For øyeblikket er Koronaviruset en stor utfordring, noe som kan skape mange utfordringer, samtidig som det utgjør en trussel for bedriftenes digitale sikkerhet.
- Kunnskapen er gammel allerede
- Utviklingen går fortere enn myndigheter og andre sikkerhetsfirma klarer å henge med. Hackere og banditter ligger langt fremfor.
- Folk som ikke vet hva de holder på med
- Personlig egnethet
- At folk flest forstår seg lite på datateknologi, og at det blir stadig vanskeligere å se forskjell på ekte og uekte nettsider/eposter osv.
- Man vet man blir overvåket uansett, så man velger kanskje å ikke tenke så mye på digital sikkerhet fordi man ikke kommer noen vei med det allikevel
- Kanskje å definere klart hva 'digital sikkerhet' er?
- Utenlandske aktører og etterretning
- «Spesialister» som lever av å lure andre og for lav kompetanse og kapasitet hos politiet
- Angrepsflaten
- Sortere hva som er skadelig og ikke. Ved flere anledninger mottar man e-poster som utgir seg for å være fra Apple, Amazon, Posten Norge o.l. Disse e-postene ser mer og mer profesjonelle ut og det er en økende vanskelighet å vurdere om e-postene er fra faktisk firma eller et forsøk på svindel.
- Internasjonalt samarbeid om økt digital sikkerhet
- Litt for mange ukritiske og naive personer bak ett tastatur i de norske hjem.
- Å få anmeldt en inntrengere som prøver å stjele informasjonen din
- At de fleste vanlige mennesker er enkle mål for hackere.
- At jeg gjør en feil som kan gjøre det lettere for andre og utnytte meg. Og det samme gjelder vel for bedrifter
- Folk som har lave digitale ferdigheter som ikke har digital kildekritikk
- Overvåkning, at andre lagrer informasjon om meg og hva jeg gjør på nett. f.eks. Politi, myndigheter, sosiale medier eller andre privatpersoner
- At det er vanskelig å se at avsender av Mail og telefonnumre er andre enn hva de utgir seg for å være. Og at det er mye styr med mange og sterke passord. Klarer aldri å huske nye. Skjønner ikke hvordan man bruker uavhengige passord-kontrollprogrammer.
- Kriminelle tar hele tiden i bruk nye metoder, så det er viktig å holde seg oppdatert for å være sikker på nett
- Altfor stort. Dersom noen vil lure deg, er det mulig selv om du passer på.

SYNET PÅ STYRING OG KONTROLL

Fellesskapets normer blir til gjennom at fellesskapet kommer frem til hva som skal være lov og ulovlig, hva som er trygt og utrygt og hva som er ønsket og uønsket. Fellesskapet reguleres, enten gjennom nedskrevne lover og regler, eller gjennom dannelse av uskrevne normer for hvordan man skal gjøre ting i dette fellesskapet.

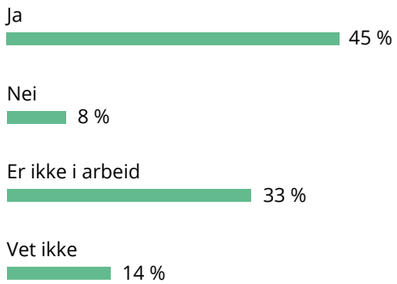
For digital sikkerhetskultur handler dette om hva som skal være lov og ikke lov i det digitale rom, eller hvilken type sikkerhetstenkning og -atferd vi har i Norge. I denne undersøkelsen ønsker man å finne ut hvilke holdninger befolkningen har til styring og kontroll innenfor det digitale. I kjernen av dette ligger det en balanse i at vi ønsker å bli passet på i det digitale rom, samtidig som vi ønsker oss frihet til å gjøre det vi selv ønsker.

Et av områdene undersøkelsen går inn i, er synet på overvåking og anonymitet på nett. Dette er relatert til hvordan fellesskapet skal kunne kontrollere om befolkningen føyer seg etter de reglene som er bestemt. Et annet område er hvem som skal være ansvarlig for vår trygghet på nett. Hvilke oppgaver forventer befolkningen av politiet skal løse, og hva forventes det av den enkelte?

Det oppstår fra tid til annen samfunnsdebatter omkring styring og kontroll. I løpet av det siste året har vi blant annet fått en debatt om et nytt lovforslag for Etterretningstjenesten som vil gi tjenesten et utvidet mandat til å samle inn nettdata som passerer grensene våre (digitalt grenseforsvar). Våren 2020 fikk vi også en debatt om Folkehelseinstituttets «Smittestopp», en app som samler inn posisjonsdata og varsler eieren av mobiltelefonen om vedkommende har oppholdt seg i nærheten av en person som er bekreftet smittet av Covid-19. I begge debattene har mange ment at denne type styring og kontroll er for inngripende i den enkeltes personvern, og de har argumentert mot lovforslaget og appen.

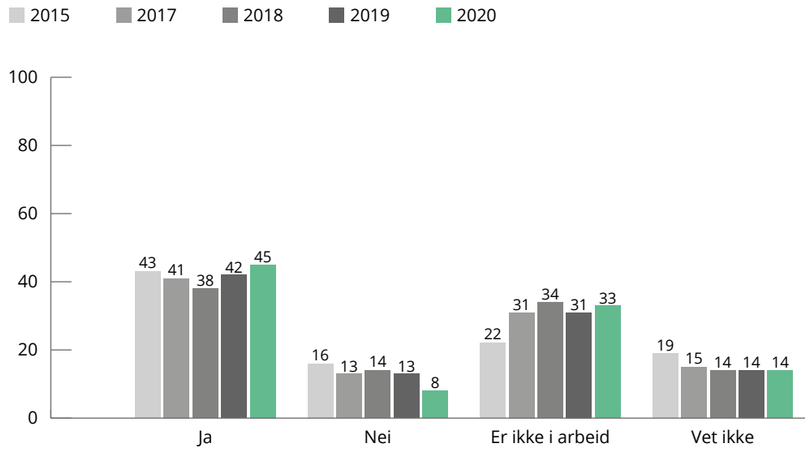
Styring og kontroll handler blant annet om hvilke normer som er etablert. De skriftlige normene finner vi gjerne som regler for bruk av digitale tjenester, for eksempler regler for bruk av epost, regler for bruk av internett og sosiale medier og så videre.

Har arbeidsplassen din regler for digital sikkerhet?



Undersøkelsen går ikke nærmere inn på om dette betyr at arbeidsplassen faktisk ikke har regler, eller om de har regler som den ansatte ikke kjenner til. I begge tilfeller har imidlertid den ansatte ikke en opplevelse av at dette er noe arbeidsgiver faktisk styrer, dersom de har svart Nei på dette spørsmålet. Dette er åpenbart uheldig fordi slike regler er helt sentrale i å opprette og kommunisere bedriftens normer. Uten kjennskap til reglene er det svært vanskelig for en ansatt å vite hva som er tillatt, og hva som ikke er tillatt.

Har arbeidsplassen din regler for digital sikkerhet? (Prosent)



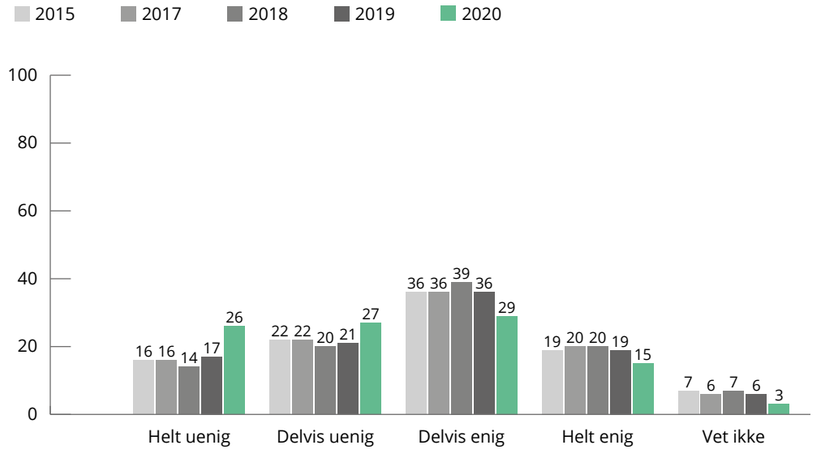
Når vi betrakter svarene over tid, ser vi at det er en økende tendens at respondentene svarer «Ja» på dette spørsmålet, og en synkende tendens til at de svarer «Nei». Dersom denne tendensen fortsetter vil det være positivt for utvikling av digital sikkerhetskultur i bedriftene og i samfunnet forøvrig, fordi slike regler er viktige verktøy for normdannelsen.

Samfunnet har åpenbart også andre regler for digital sikkerhet enn de som arbeidsgivere har. Vi har bestemmelser i lovverket, og vi må forholde oss til de reglene som for eksempel forsikringsselskapene eller tilbydere av digitale tjenester har fastsatt. Dersom de mener at du har opptrådt uaktsomt kan du blir nødt til å dekke større deler av tapene selv. Vi går i denne undersøkelsen ikke videre inn på denne type styring av det digitale sikkerhetsområdet.

Undersøkelsen ser derimot på hva befolkningen mener om enkelte former for kontroll av aktiviteten på nett. Et spørsmål som stadig går igjen i debattene om kontroll på nett, handler om overvåking. Respondentene ble bedt om å ta stilling til påstanden *«Jeg synes det er greit at myndighetene kan overvåke min aktivitet på internett»*.

Merk at påstanden er endret fra tidligere undersøkelser, hvor den var formulert slik: «Det er greit at min aktivitet på internett blir overvåket dersom det fører til at jeg blir tryggere på nett.» Endringen omfatter altså at man nå presiserer hvilken overvåkingsaktør vi henviser til (myndighetene og ikke for eksempel Facebook), og at vi ikke lenger har med betingelsen «... dersom det fører til at jeg blir tryggere på nett.» Vi mener at endringen gjør at det blir enklere å forstå hva som menes med spørsmålet, og at det i mindre grad er ledende siden betingelsesleddet er tatt bort.

Jeg synes det er greit at myndighetene kan overvåke min aktivitet på internett. (Prosent)



Man observerer en økning i de som har svart at de er enten helt eller delvis uenig i påstanden, altså en økning i de som har motforestillinger mot å bli overvåket. Tilsvarende synker andelen som er enig i påstanden, og andelen for de som ikke er sikker.

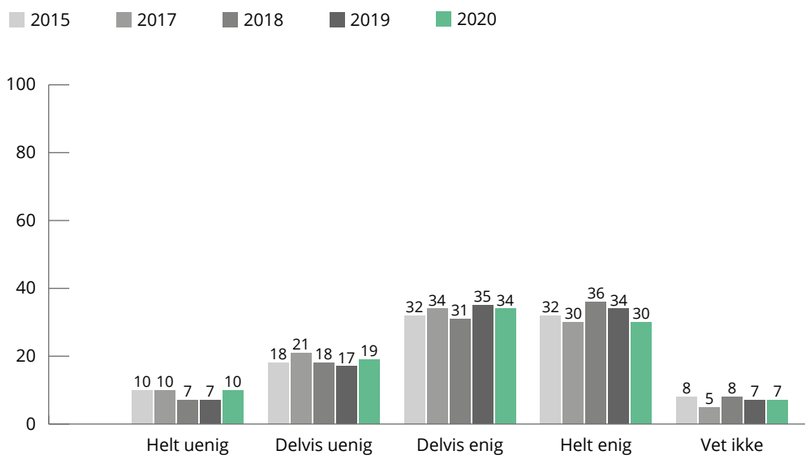
Siden spørsmålet er endret i årets undersøkelse, kan en ikke utelukke at det er årsaken til endringene. Samtidig har det pågått en debatt, både politisk og i fagpressen, omkring den mulige overvåkingen av norske statsborgere som den nye loven for Etterretningstjenesten kan åpne for. Dette er en debatt som også har et potensiale til å endre folks holdninger til dette spørsmålet.

Påstanden *«Det bør være mulig å være anonym på internett»* er beslektet med den forrige, altså om det skal være mulig å unndra seg den type kontroll som overvåking muliggjør. Det er ikke signifikante endringer fra forrige undersøkelse, men registrerer at det fortsatt er 64 % som enten er helt eller delvis enige i denne påstanden.

Undersøkelsen gir ikke svar på hvorvidt respondentene mener at man ønsker å være anonym hele tiden, eller om det kun er snakk om de gangene man oppsøker informasjon eller tjenester som den enkelte vurderer som sensitivt. Tolkningen er at de som er enige i påstanden ønsker at muligheten skal være der, mens de som er uenige mener at man ikke skal kunne være anonym og dermed unndra seg kontroll.

Dette er et komplisert spørsmål, for det er mange grunner til at den enkelte kan ønske å bruke nettet uten at noen skal kunne se dem i kortene. Det kan dreie seg om kildevern og varslingssaker, helserelatert informasjon eller seksualitet og pornografi. På den andre siden kan

Det bør være mulig å være anonym på internett. (Prosent)



anonymitet være helt ødeleggende for politiets evne til å etterforske alvorlig kriminalitet. Vi vet også at mange barn dessverre opplever digital mobbing fra anonyme kontoer.

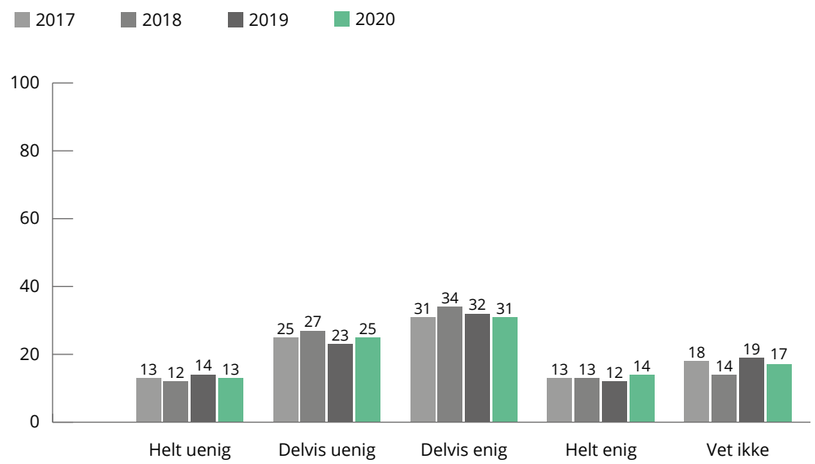
En annen side ved dette er hvem en forventer skal stå for styring og kontroll. Å følge med på at reglene overholdes, og å etterforske og sanksjonere mot brudd på reglene er en del av dette bildet. Samfunnets normer er blant annet nedtegnet i lovverket, og det er vanligvis politiets oppgave å etterforske brudd på lover og forskrifter. Når respondentene bes om å svare på påstanden *«Politiet vil hjelpe meg dersom jeg blir utsatt for datakriminalitet»* så ønsker man å vite mer om deres syn på politiets evne til å følge opp datakriminalitet.

Det er ingen signifikante endringer fra tidligere års undersøkelser, men det er fortsatt nær 40 % som er helt eller delvis uenig i denne påstanden. NorSIS har i tidligere rapporter påpekt at det er uheldig at så mange ikke har tiltro til at politiet vil hjelpe de som blir utsatt for datakriminalitet.

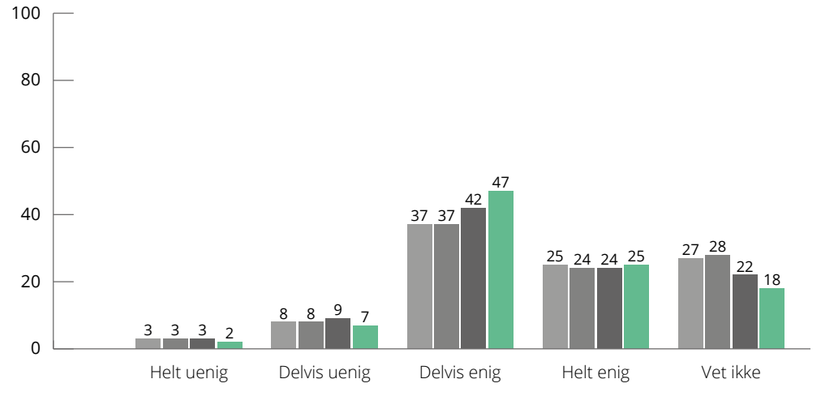
Respondentene bes også om å ta stilling til påstanden *«Privatpersoner og aktivistgrupper har en rolle i kampen mot datakriminalitet»*. Merk at denne påstanden er endret i årets undersøkelse. Tidligere var påstanden formulert slik: *«Privatpersoner og aktivistgrupper har en rolle i kampen mot datakriminalitet og cyber-krig»*. Å fjerne *«cyber-krig»* vurderes å ikke signifikant endre meningsinnholdet i påstanden.

Det er en økning i de som er delvis enige i påstanden. Denne utviklingen er uheldig fordi den kan representere en legitimering av selvtekt på nett. Digital etterforsking kan være svært inngripende for den det gjelder, og det er særdeles viktig at vi kan stole på at de som driver med slik etterforsking holder seg innenfor rammene av det som er tillatt. Et eksempel på hvor krevende det kan være å holde seg innenfor det man anser å være tillatt, er hendelsen hvor en ansatt i Kripos brukte en ansiktsgjenkjennings-app i etterforskingen

Politiet vil hjelpe meg dersom jeg blir utsatt for datakriminalitet. (Prosent)

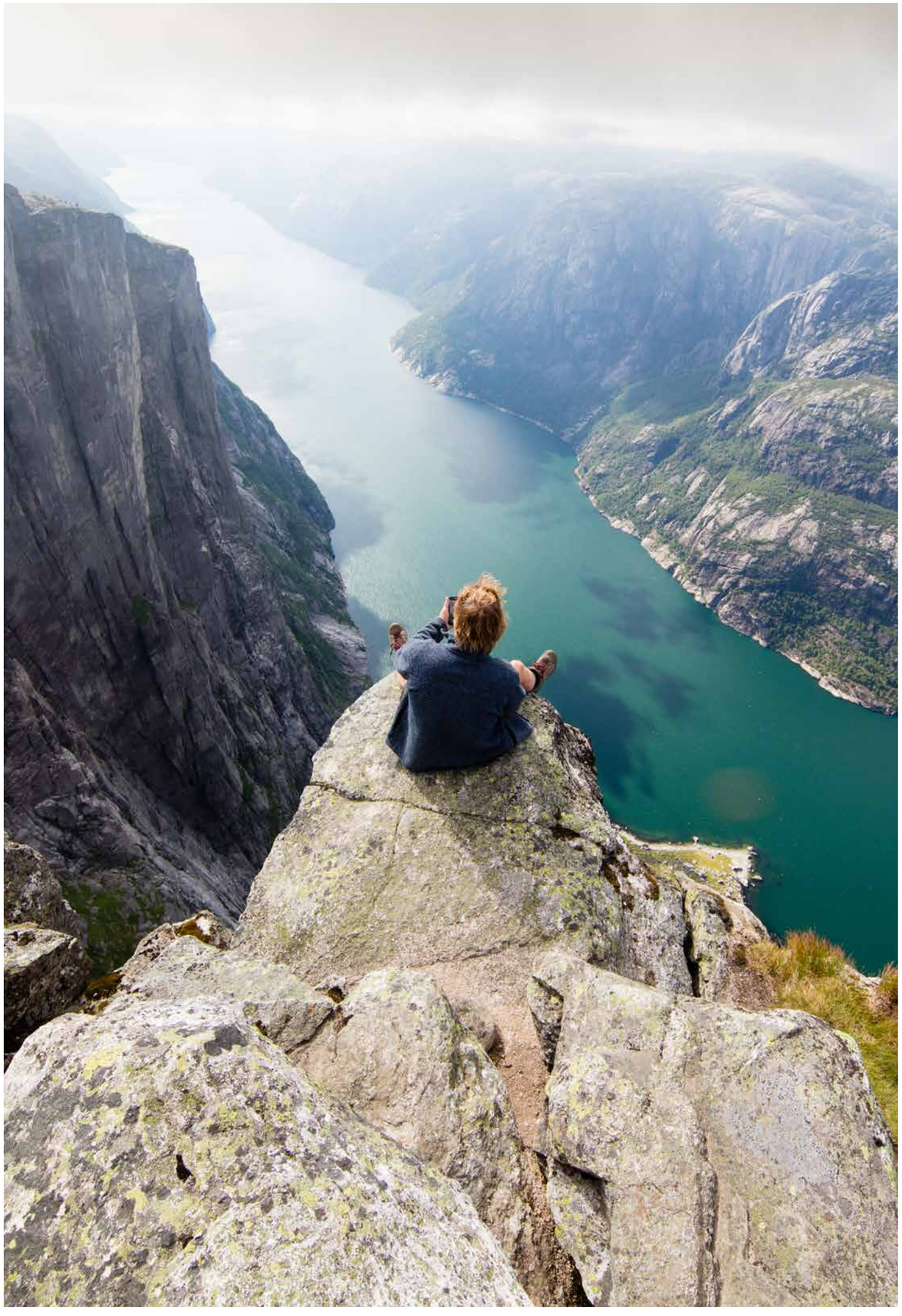


Privatpersoner og aktivistgrupper har en rolle i kampen mot datakriminalitet. (Prosent)



av overgrepssaker[5]. Praksisen fikk sterk kritikk, og i Sverige har politiet fått forbud om å bruke tjenesten.

Denne og andre saker viser at det er all grunn til å være bevisst på hvem som kan etterforske lovbrudd og hvilke metoder de skal få lov til å bruke. En stadig legitimering av selvtekt på nett kan føre til at rettssikkerheten til den enkelte blir redusert, og myndighetene bør derfor arbeide for å motvirke denne trenden.



TILLIT OG RISIKOOPPFATTELSE

Tillit og risikooppfattelse er psykologiske dimensjoner som også er knyttet til digitalisering og digital sikkerhet. Tillit er en grunnleggende faktor som må være på plass for at vi skal kunne delta i digitaliseringen på en hensiktsmessig måte. Vi må ha tillit til at data om oss blir beskyttet slik at de ikke faller uvedkommende i hende. Vi må ha tillit til at den vi overgir dataene til kun bruker dem til det som er avtalt, og ikke til noe som ikke er i vår interesse. Vi må også ha tillit til at de digitale tjenestene virker slik vi har forutsatt, og at de ikke inneholder feil som kan true vår sikkerhet.

Risikooppfattelse er tett knyttet til det samme. Som digitale brukere står vi hele tiden ovenfor valg, der en vurdering av risiko inngår i beslutningsprosessen. Skal jeg åpne dette vedlegget? Skal jeg gjenbruke passordet jeg har på jobb? Skal jeg legge inn betalingskortet på denne nettsiden? Skal jeg laste ned denne appen, og akseptere at den sporer hvor jeg er til enhver tid?

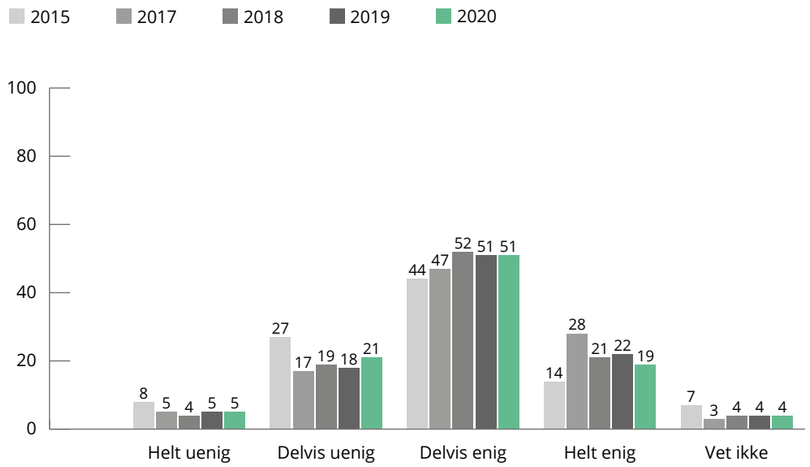
I mange sammenhenger har vi ikke noe valg. Vi er nødt til å bruke Altinn slik den er, og banken krever at vi bruker Bank-ID eller tilsvarende for å logge oss på. Det betyr imidlertid ikke at den enkelte har tillit til løsningen. Manglende tillit fører ikke nødvendigvis til at man unngår å bruke en tjeneste, spesielt der man ikke har et reelt valg. Det kan likevel være slik at mangel på tillit utgjør et potensiale for at man unngår å bruke tjenester dersom det oppstår alternativer, og at det er en drivkraft for å lete etter andre (og muligens mindre sikre) måter å gjøre ting på. Dersom målet er at brukerne av en tjeneste skal være fornøyde, bør tillit til sikkerheten til tjenesten tas inn som en faktor.

For andre tjenester, der man har et valg om man skal bruke tjenesten eller ikke, er tillit og risikooppfattelse svært viktig. NorSIS har i tidligere rapporter påpekt at manglende tillit til digitale tjenester kan føre til en nedkjølingseffekt. Motstanden mot FHIs Smittestopp er kanskje et eksempel på at manglende tillit førte til at man ikke fikk det antallet brukere som løsningen faktisk krever for at den skal virke etter hensikten. I begynnelsen av mai 2020 rapporterte FHI at det var ca. 750.000 brukere av Smittestopp. FHI uttalte selv at det måtte være ca. 2.100.000 brukere for at appen skal være effektiv. Hele forklaringen kan neppe tillegges manglende tillit, men debatten omkring appen kan tyde på at det er en signifikant faktor.

Undersøkelsen ser nærmere på hvordan befolkningen opplever tillit og risiko, knyttet til bruk av digitale tjenester og vanlige digitale trusselscenarier.

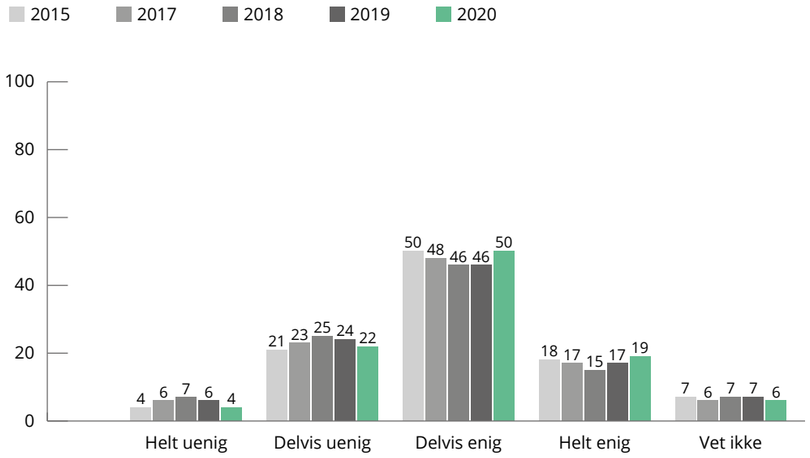
Respondentene er bedt om å ta stilling til påstanden «*Jeg utsetter meg selv for risiko når jeg bruker internett*» for å avdekke deres generelle holdning til risiko knyttet til deres nettbruk. Det er ingen signifikante endringer fra tidligere år, og fremdeles 7 av 10 som mener at de blir utsatt for risiko.

Jeg utsetter meg selv for risiko når jeg bruker internett. (Prosent)



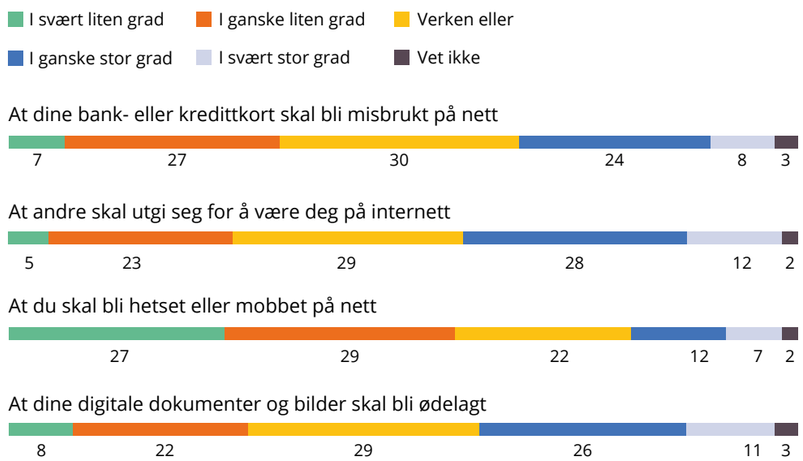
Kunnskap om trusler er nødvendig for å kunne vite hvordan man best skal beskytte seg. Flertallet av respondentene er enige i påstanden «*Jeg synes at jeg får tilstrekkelig informasjon om de truslene som finnes på internett*».

Jeg synes at jeg får tilstrekkelig informasjon om de truslene som finnes på internett. (Prosent)



Det er imidlertid 26 % som svarer at de er enten helt eller delvis uenige i påstanden. En målrettet innsats for å hjelpe denne gruppen til å tilegne seg mer kunnskap om truslene kan ha betydning for hvordan de vil beskytte seg mot digitale trusler. Respondentene er videre bedt om å vurdere hvor stor risikoen er for at noen av de vanligste digitale truslene skal skje med dem.

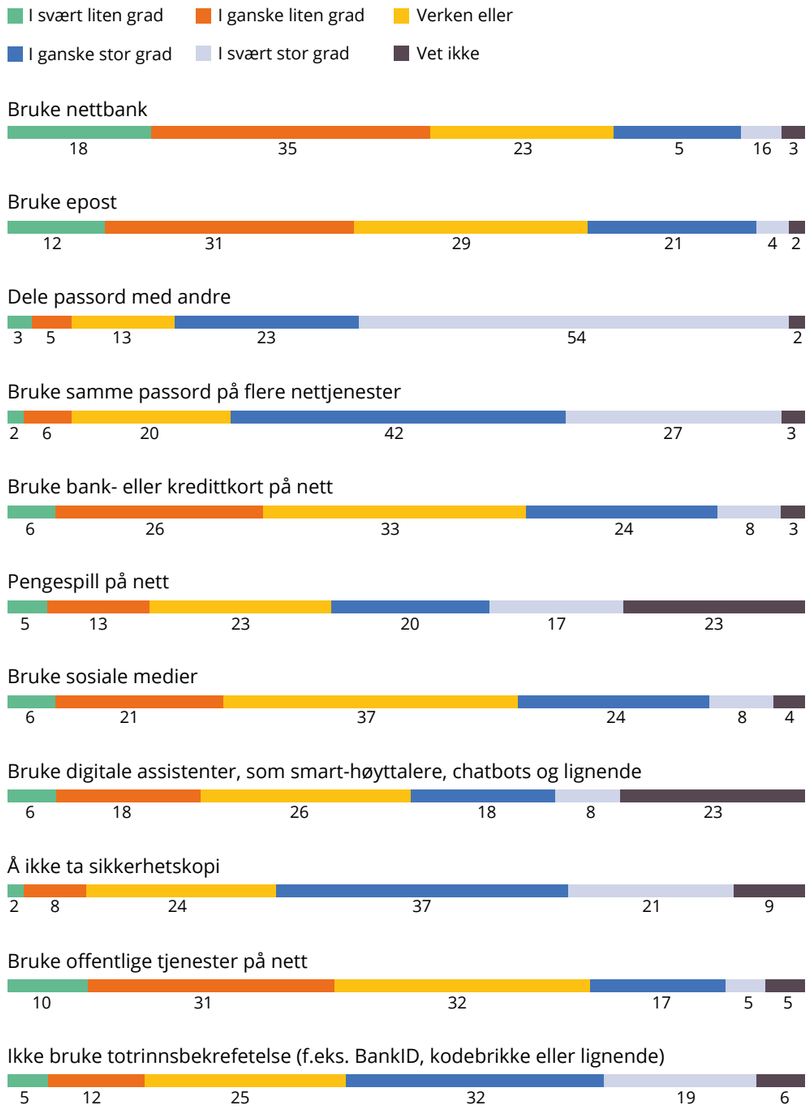
I hvilken grad er du bekymret for at følgende skal skje med deg? (Prosent)



Det er noen aldersforskjeller når det gjelder synet på slik risiko. De over 55 år er for eksempel mer bekymret for at *bank- eller kredittkortene skal bli misbrukt på nett eller at de skal få virus eller lignende på datamaskinen*, mens samme aldersgruppe er mindre bekymret for å bli hetset eller mobbet på nett enn det aldersgruppen 18-34 år er.

Bruk av digitale tjenester kan også være forbundet med risiko, og respondentene er derfor bedt om å vurdere hvor stor risikoen er ved bruk av ulike tjenester.

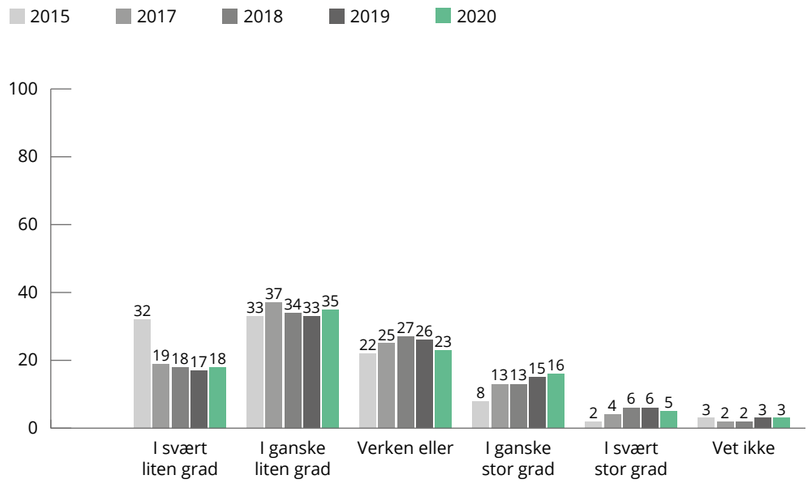
I hvilken grad forbinder du følgende aktiviteter med høy risiko? (Prosent)



Ved å stille disse spørsmålene forventer en nødvendigvis ikke at respondentene har kunnskap om den reelle risikoen ved de ulike aktivitetene. Risikooppfattelse er subjektivt, og lar seg påvirke av både eksterne (f.eks. ting man opplever eller hører om) og interne (f.eks. personlighetstrekk[6]) forhold. Det er likevel nyttig å vite hvordan befolkningen ser på dette, for opplevelse av risiko kan føre til ønsket eller uønsket atferd. Dersom mange opplever at det å ikke bruke totrinnsbekreftelser ikke er knyttet til risiko, kan det være vanskelig å få dem til å ta det i bruk. Dersom mange opplever at det å bruke digitale assistenter er risikofylt, kan det føre til at mange lar være å bruke disse, selv om de kanskje ville være til nytte for dem.

Å bruke nettbank er noe de aller fleste må forholde seg til. Ca. en av fem oppgir at de i ganske stor eller svært stor grad forbinder bruk av nettbank med høy risiko. Det er ingen signifikante endringer fra undersøkelsen i 2019, men dersom en sammenligner med undersøkelsen i 2017 ser man en økning fra 17 % til 21 %.

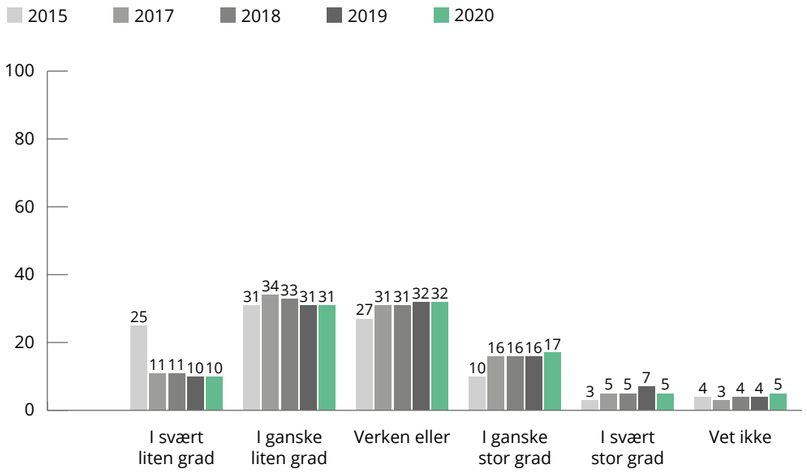
I hvilken grad forbinder du å bruke nettbank med høy risiko? (Prosent)



Å bruke offentlige tjenester på nett er noe nordmenn ofte ikke enkelt kan velge bort. Stadig mer av kommunikasjonen mellom det offentlige og den enkelte skjer over nettbaserte tjenester. Selv om man ofte har mulighet til å benytte seg av personlig oppmøte eller å sende inn skjema på papir, er det myndighetenes uttalte strategi at tjenestene skal utvikles i digital retning[7].

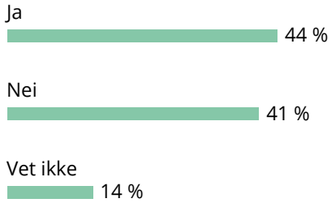
Respondentene er bedt om å vurdere i hvilken grad de forbinder det å bruke offentlige tjenester med høy risiko. 22 % av de som svarer angir at de i ganske stor eller svært stor grad forbinder slik bruk med høy risiko. Dette er noe det offentlige må ta hensyn til når de digitaliserer sine tjenester, og bidra aktivt til at befolkningen også har tillit til sikkerheten for tjenestene.

I hvilken grad forbinder du å bruke offentlige tjenester på nett med høy risiko? (Prosent)



NorSIS har gjennom flere år satt fokus på «digital nedkjølingseffekt», altså at frykt og mistillit til digitale tjenester skal føre til at man lar være å bruke dem. Respondentene er derfor bedt om å svare på om kunnskap om trusler eller hacking noen ganger fått dem til å la være å bruke en nettjeneste.

Har kunnskap om trusler eller hacking noen ganger fått deg til å la være å bruke en nettjeneste?

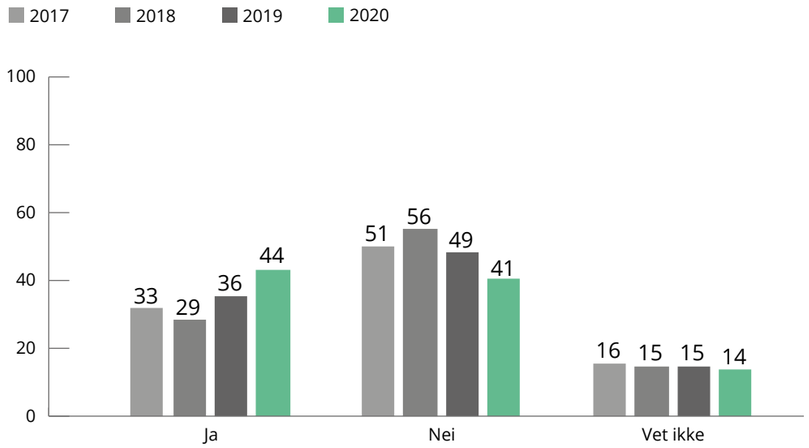


I årets undersøkelse svarer 44 % at de har latt være å bruke nettjenester med bakgrunn i kunnskap om trusler eller hacking. Når en ser dette spørsmålet over tid, ser man en signifikant økning fra tidligere år.

Dette tyder på at den digitale nedkjølingseffekten er økende. En slik utvikling er bekymringsfull, fordi digitalisering er en ønsket strategi for både myndighetene og det private næringsliv. At frykt for digitale trusler skal bidra til at digitaliseringen bremser opp er ikke ønskelig. Det bør derfor være en prioritert oppgave for myndighetene og andre som utvikler digitale tjenester å motvirke denne utviklingen.

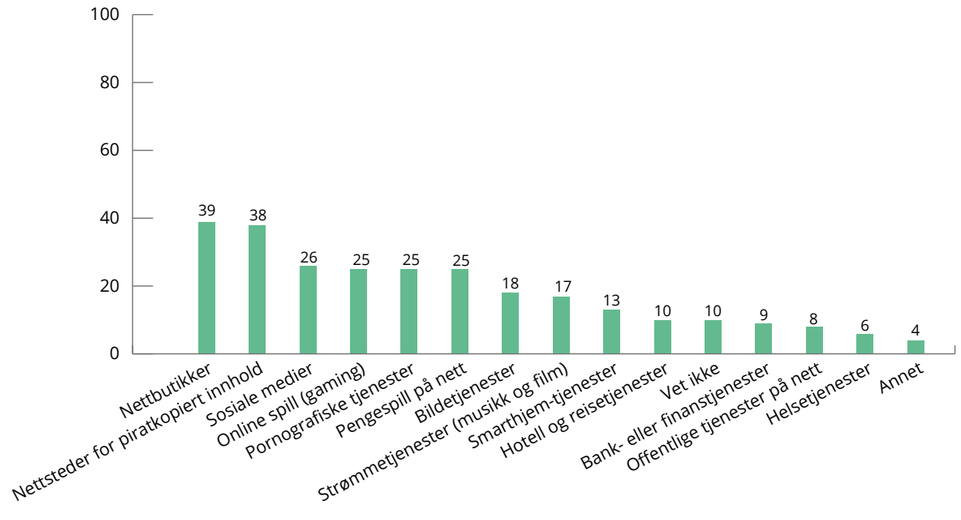
En mulig innvending mot denne anbefalingen er at truslene faktisk er reelle, og at det er til det beste for den enkelte at de avstår fra å bruke tjenestene. Utfordringen med dette er at det kan være nærmest umulig for den enkelte å vite om risikooppfattelsen er korrekt eller ikke. Et målrettet arbeid med å både øke sikkerheten for tjenestene og å fjerne truslene kan forhåpentligvis bidra til at alle kan føle større trygghet på nett.

Har kunnskap om trusler eller hacking noen gang fått deg til å la være å bruke en nettjeneste? (Prosent)



Årets undersøkelse går også inn på hvilke tjenester respondentene oppgir å ha latt være å bruke, som følge av kunnskap om trusler eller hacking.

Hvilke typer nettjeneste har du latt være å bruke som følge av kunnskap om trusler eller hacking? Respondenten kunne her krysse av for flere alternativer. (Prosent)



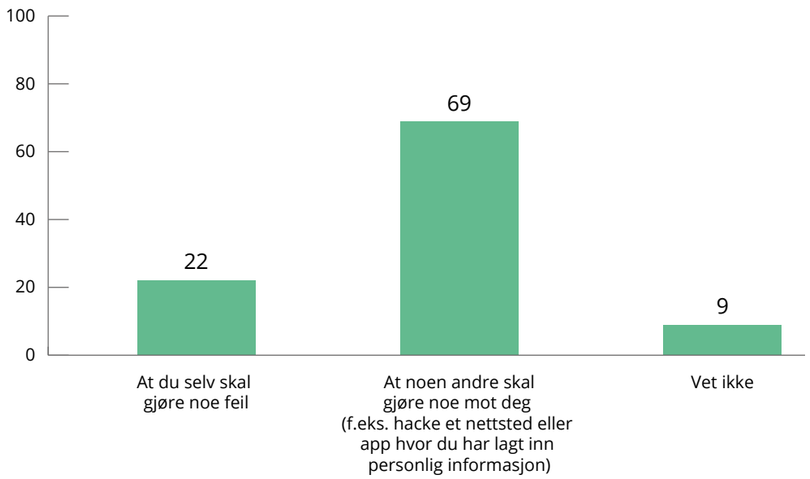
Respondentene fikk også her mulighet til å oppgi «Annet» dersom svaralternativene ikke passet. Blant disse svarene finner vi for eksempel:

- Fildeling
- Nettsider som ikke er sikret med https
- Offentlige nett
- Programvare som optimaliserer data-maskinens ytelse
- Sikkerhetsmeldinger (som dukker opp på nettsider)

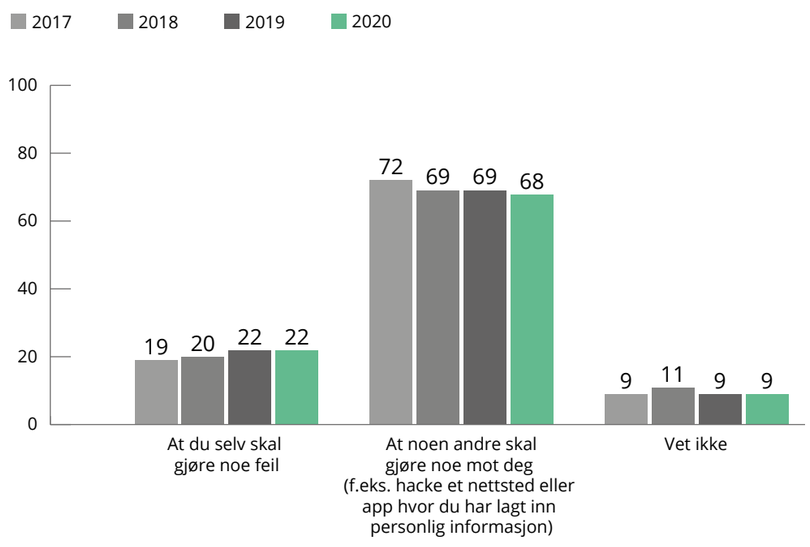
Respondentene er også bedt om å ta stilling til om kilden til risikoen i hoved-sak er plassert hos dem selv, eller hos noen andre.

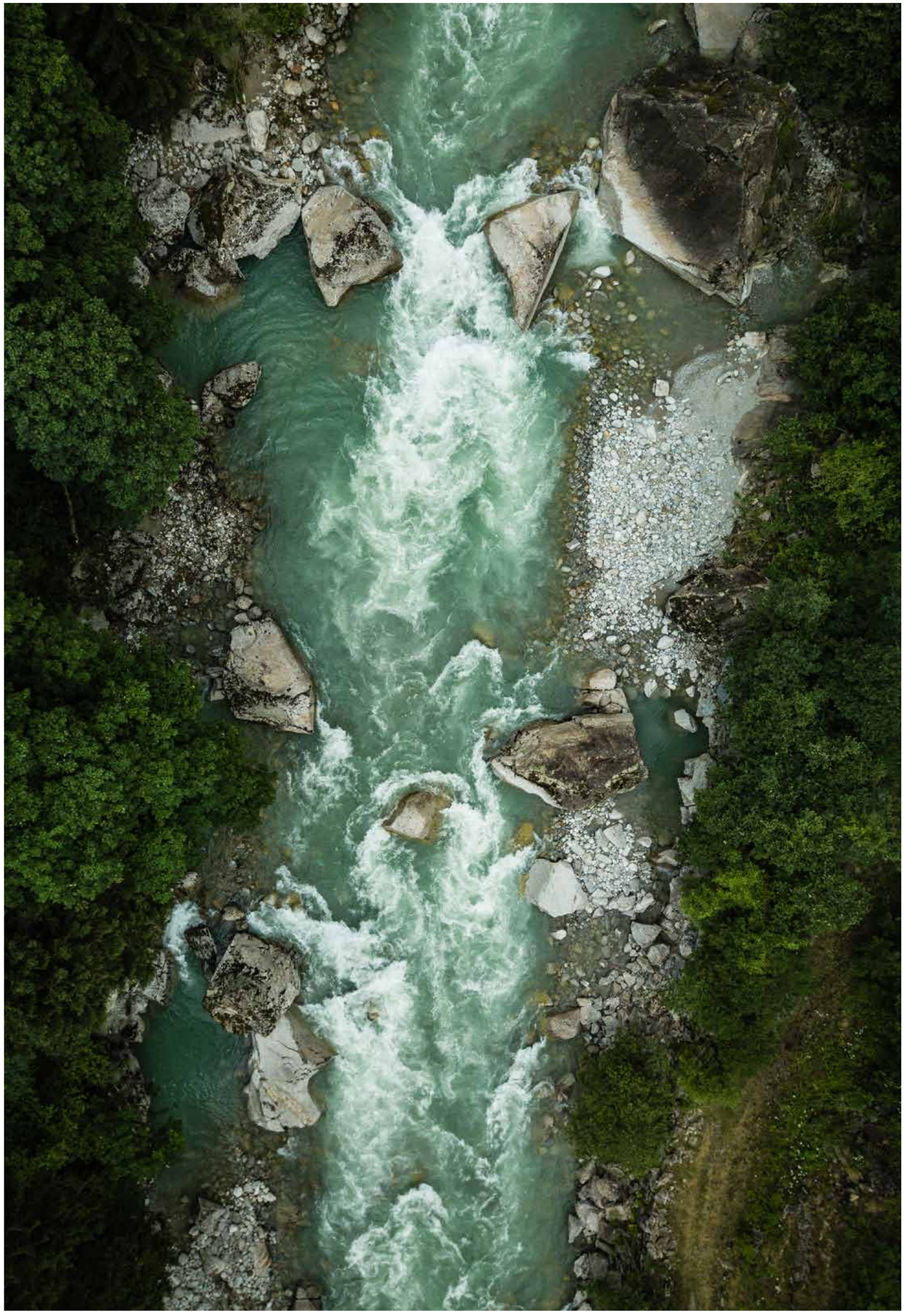
Det er ingen signifikante endringer dersom en betrakter dette over tid.

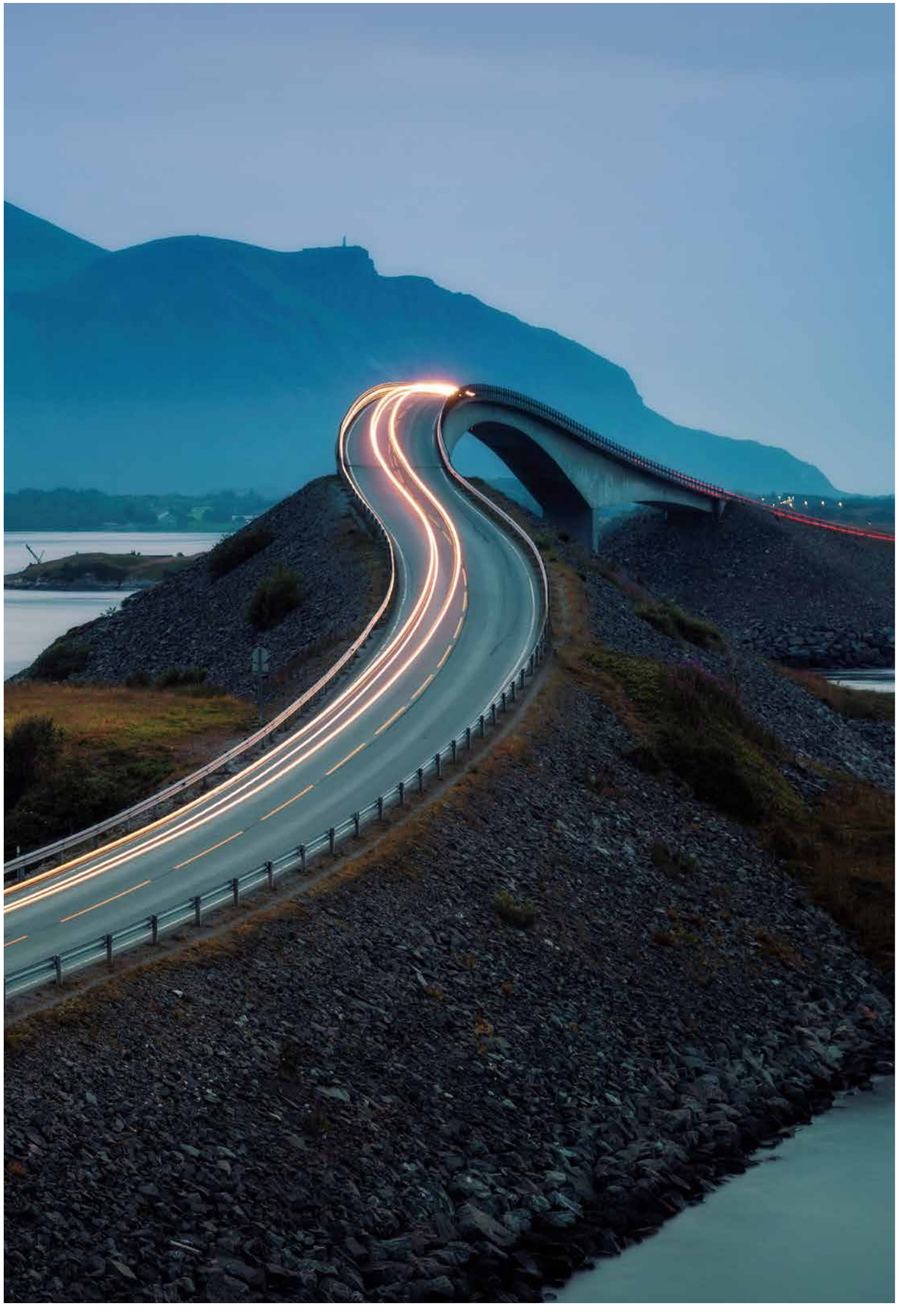
Hva mener du er den største risikoen på nett? (Prosent)



Hva mener du er den største risikoen på nett? (Prosent)







KUNNSKAP, INTERESSE OG LÆRING

Samfunnet forventer at den enkelte skal ta et ansvar for sin egen digitale sikkerhet. Man skal ikke opptre uaktsomt. Det innebærer at den enkelte må kunne noe om hva det vil si å være aktsom.

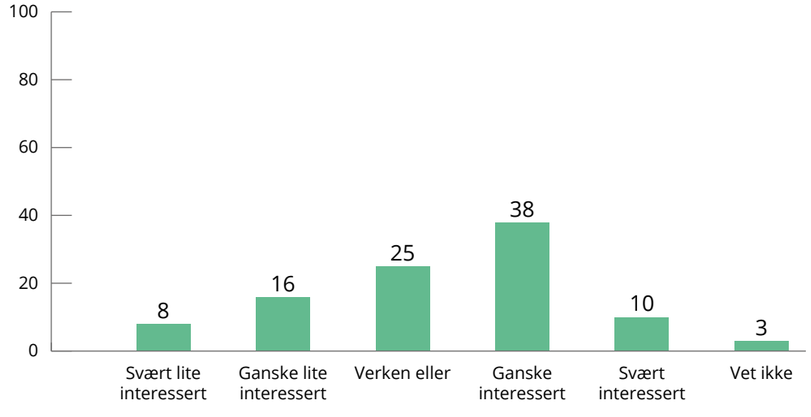
Når man blir bedt om å «ikke bruke farlige nettsider» eller «bruke sikre passord», så forutsetter det at den enkelte har kunnskap til å kunne skille en ufarlig nettside fra en som er farlig. Man må vite hva som gjør et passord sikkert, før man kan lage et.

Kunnskap er derfor en helt sentral faktor i digital sikkerhetskultur. Kunnskap kan endre måten vi tenker omkring digital sikkerhet, og ikke minst hvordan vi oppfører oss i møte med det digitale og med digitale trusler. Undersøkelsen ser også nærmere på hvordan nordmenn lærer om digital sikkerhet og hvem de lærer dette av.

Kunnskap og læring er ganske sammensatt på dette feltet. Det begynner å komme en del på plass i læreplaner i grunnskolen og høyere utdanning. Tidligere undersøkelser viser imidlertid at mange av de som får opplæring i digital sikkerhet, får opplæringen på jobb. I tillegg til organisert opplæring er mange aktører synlige i mediebildet, som tilbyr kunnskap om digital sikkerhet. Nasjonal sikkerhetsmyndighet, Slettmeg.no (NorSIS), Du Bestemmer (Utdanningsdirektoratet og Datatilsynet) og Ung.no (Bufdir) er eksempler på slike aktører. Også enkeltpersoner kan komme til i mediene med kunnskaper om hva man bør og ikke bør gjøre på nett.

Det har betydning hva folk lærer, og av hvem. Ikke alle typer opplæring passer for alle, så vi trenger kunnskap om hva som fungerer for ulike grupper.

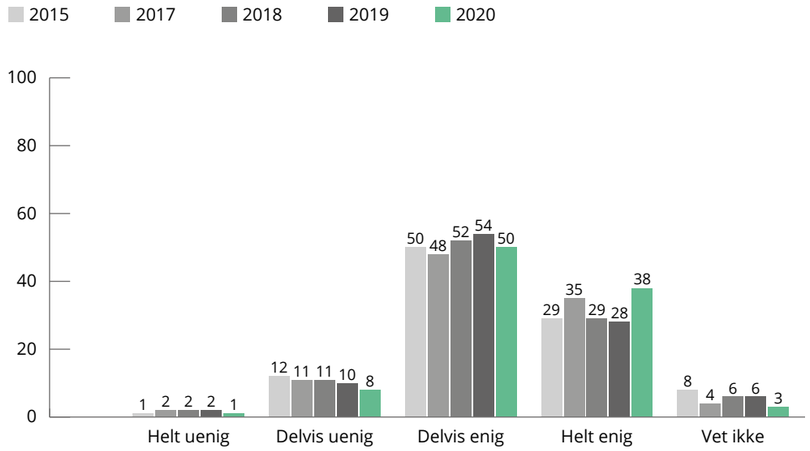
Hvor interessert er du i teknologi og IT? (Prosent)



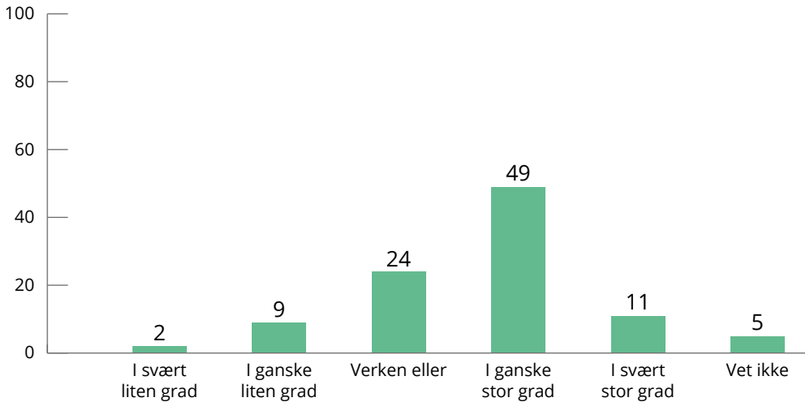
Interesse er en viktig faktor når det kommer til kunnskap og hvordan man skaffer seg kunnskapen. Fra tidligere undersøkelser vet man at det er en sammenheng mellom interesse for teknologi og IT, hvordan man lærer om digital sikkerhet og om man har en sikker atferd på nett.

Til påstanden *Jeg vet hva informasjonssikkerhet er,* svarer 88 % at de er helt eller delvis enige i dette. Det er verdt å merke seg at andelen som har svart at de er helt enige har økt fra 28 % til 38 % siden 2019. Det er også verdt å merke seg at det er en gruppe på ca. 10 % som er enten helt eller delvis uenige i påstanden.

Jeg vet hva informasjonssikkerhet er. (Prosent)



I hvilken grad er du i stand til å vurdere hva som er trygt eller utrygt å gjøre på nett? (Prosent)



At man har hørt om digitale trusler eller andre ting som kan gå galt, er ingen garanti for at man selv vet hvordan man skal oppdage hva som er trygt og utrygt. Respondentene blir derfor bedt om å angi i hvilken grad de er i stand til å vurdere hva som er trygt eller utrygt å gjøre på nett. Omtrent en fjerdedel plasserer seg i midtpunktet «Verken eller», mens ca. 10 % mener at de i svært liten eller ganske liten grad vil kunne vurdere dette. Flertallet (60 %) mener imidlertid at de er i stand til å vurdere hva som er trygt og utrygt på nett.

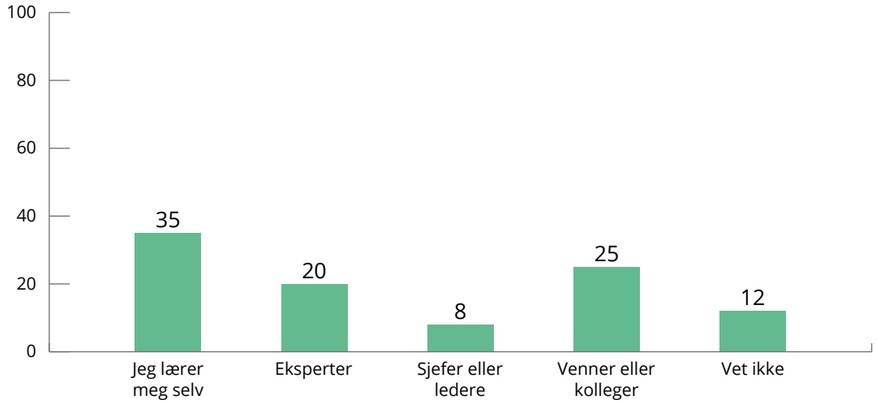
Spørsmålet om hvem man lærer om digital sikkerhet fra er av betydning fordi innholdet i det som læres antas å variere basert på hvem som lærer det bort. Presumptivt vil eksperter i større grad lære bort det «riktige» fordi de er oppdaterte på fagfeltet. Ettersom det som anses å være korrekt kunnskap endrer seg over tid, er dette av betydning.

Å lære seg selv kan være en god måte å lære på, spesielt når det kombineres med en interesse for fagfeltet og tilgang til gode kunnskapskilder.

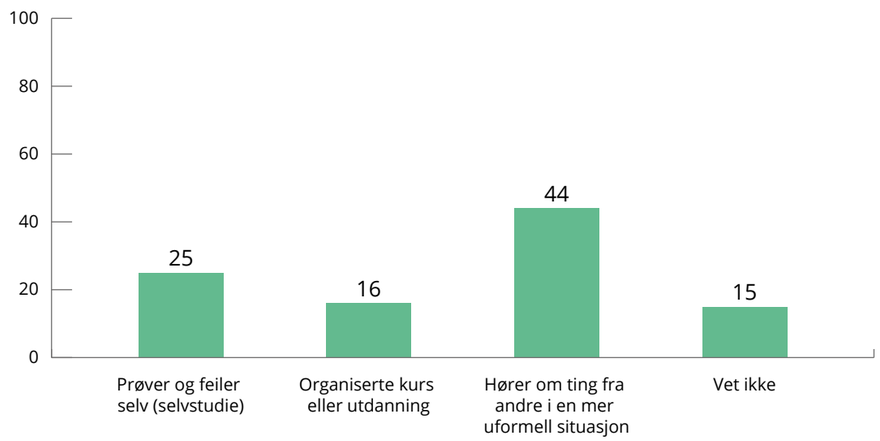
Hvordan man lærer knyttes til det samme. Det anses som ønskelig at man får kunnskap gjennom organiserte kurs eller utdanninger, fordi det legges til grunn at pensum da er kvalitetssikret.

Nær halvparten av respondentene oppgir at de hører om ting fra andre i en mer uformell situasjon, mens bare 16 % lærer vanligvis gjennom organiserte kurs eller utdanning.

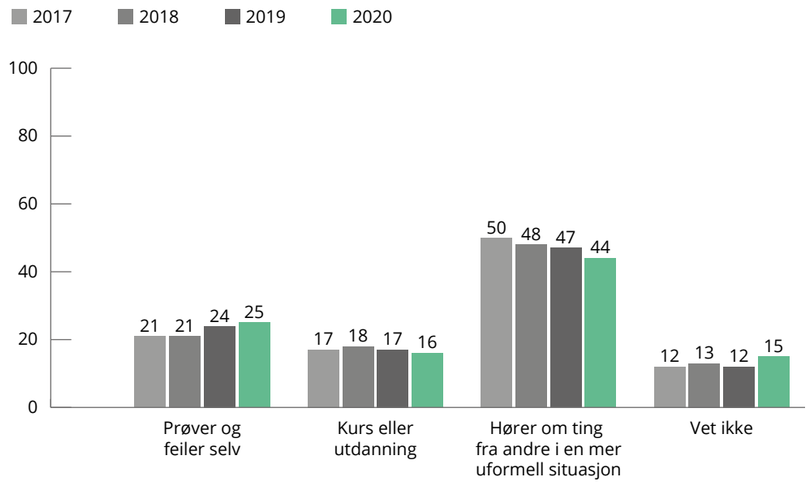
Hvem lærer du mest om informasjonssikkerhet av? (Prosent)



Hvordan lærer du vanligvis om digital sikkerhet? (Prosent)



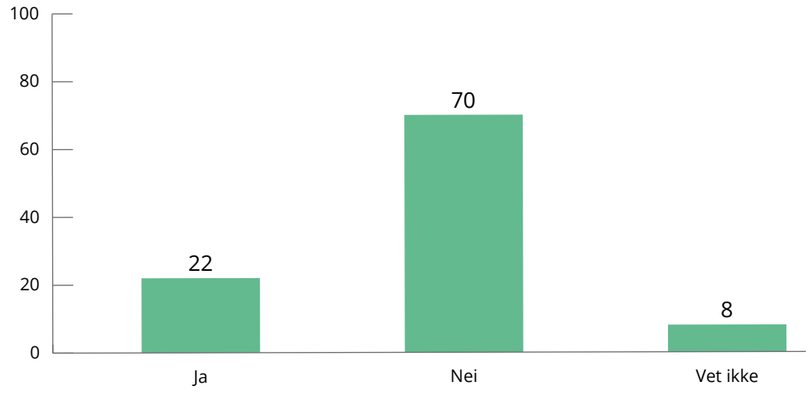
Hvordan lærer du vanligvis om informasjonssikkerhet? (Prosent)



Når en ser på dette spørsmålet over tid er det ingen signifikante endringer blant respondentene.

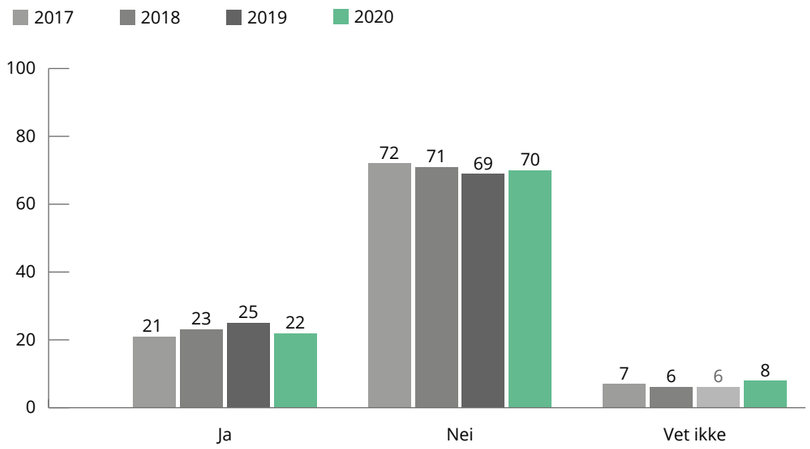
Undersøkelsen ser også på om respondentene har fått organisert opplæring i digital sikkerhet i løpet av de siste to årene.

Har du fått organisert opplæring i digital sikkerhet i løpet av de siste to årene? (Prosent)



Av de som har svart, har 22 % fått slik opplæring, mens 70 % ikke har det. Når en ser på dette spørsmålet over tid er det heller ikke her noen signifikante endringer blant respondentene.

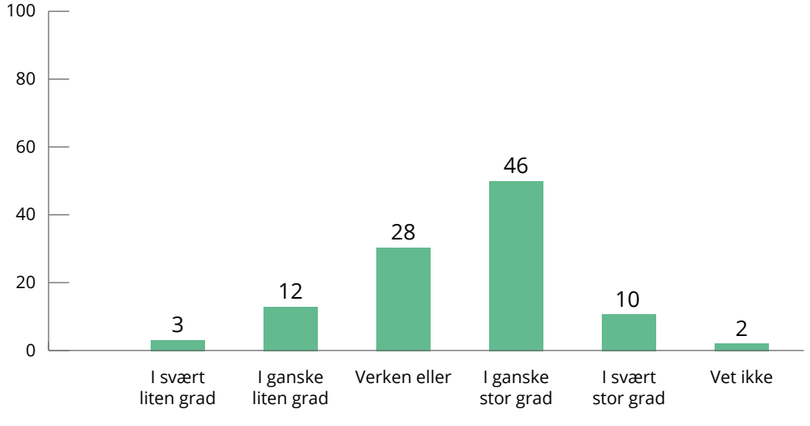
Har du fått organisert opplæring i informasjonssikkerhet i løpet av de siste to årene? (Prosent)



Tidligere undersøkelser viser at det stort sett er arbeidsgivere som tilbyr opplæring i digital sikkerhet, men det blir nå stadig fler opplæringstilbud til ulike grupper i samfunnet. NorSIS tilbyr for eksempel gratis nettbasert opplæring til eldre, små- og mellomstore bedrifter, skoleelever, foreldre og lærere. Grunnleggende opplæring er med andre ord tilgjengelig, bare man vet hvor man skal lete.

Det er interessant å vite om de som har fått opplæring har en opplevelse av at den var nyttig for dem. Respondentene er derfor bedt om å angi i hvilken grad de har fått bedre ferdigheter etter organisert opplæring i digital sikkerhet. Mer enn halvparten (56 %) mener at de i stor grad har fått bedre ferdigheter, mens 15 % mener at de i liten grad har fått det.

I hvilken grad synes du at du har fått bedre ferdigheter etter organisert opplæring i digital sikkerhet? (Kun de som har svart «Ja» til at de har fått organisert opplæring i løpet av de siste to årene. Prosent)

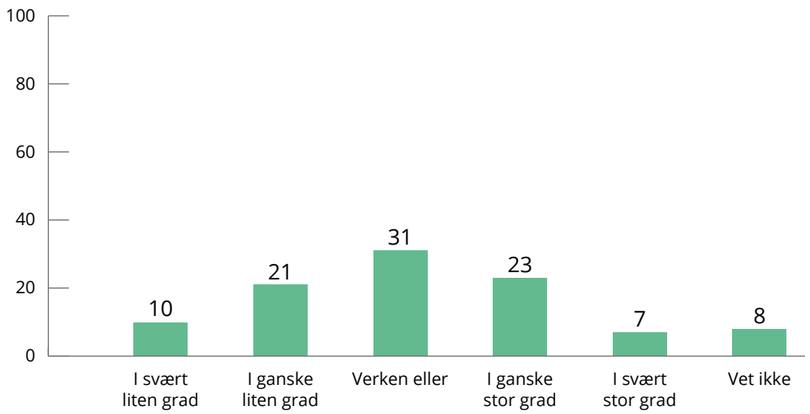


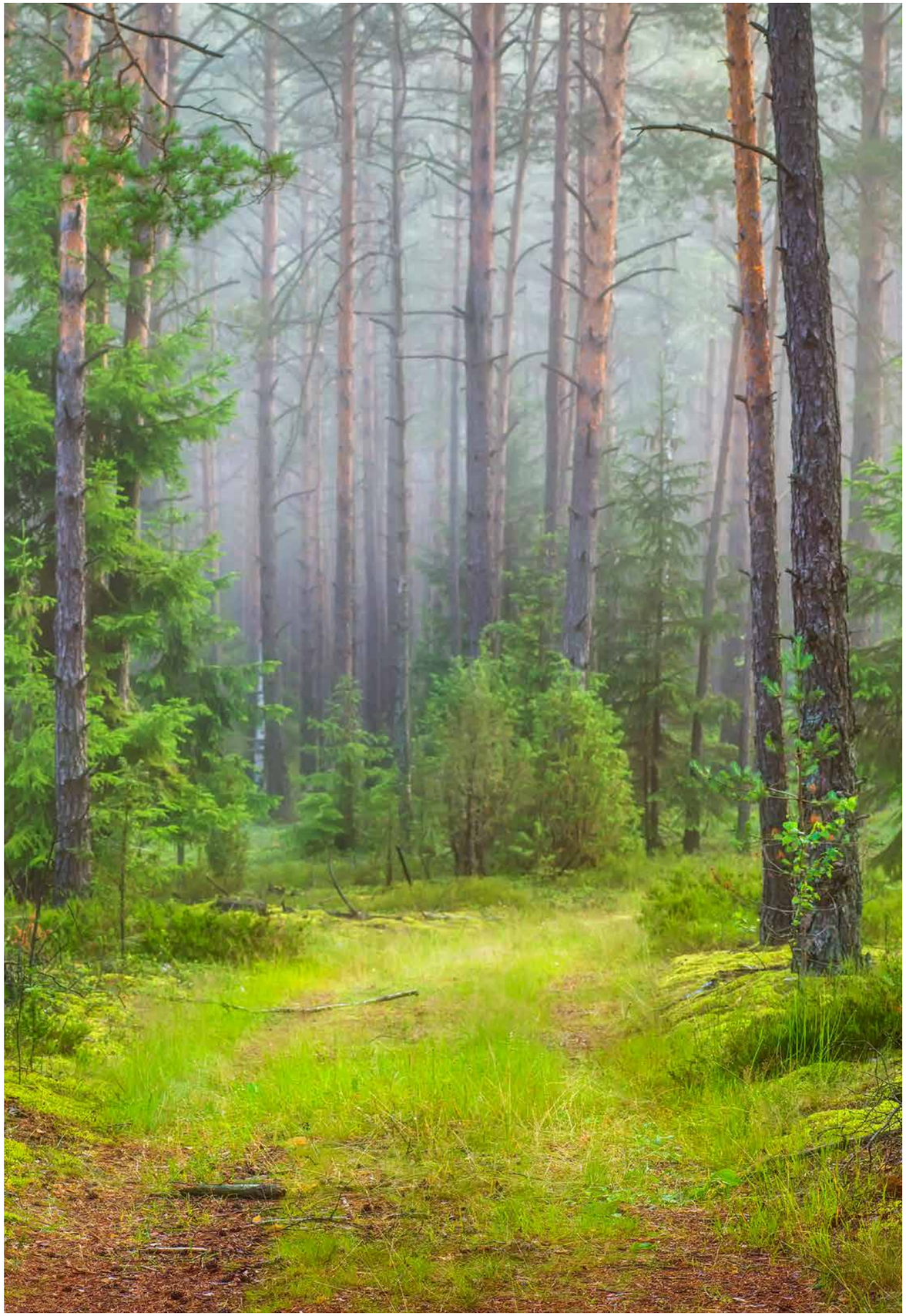
Resultatene gir grunn til å evaluere opplæringen som blir gitt. At bare litt over halvparten av de spurte mener at opplæringen i ganske stor eller svært stor grad har gitt dem bedre ferdigheter fremstår som lavt. Denne undersøkelsen gir ikke svar på hvorfor respondentene har svart slik, men det antas at noe av forklaringen handler om at opplæringen i for liten grad er tilpasset den enkeltes kunnskapsnivå.

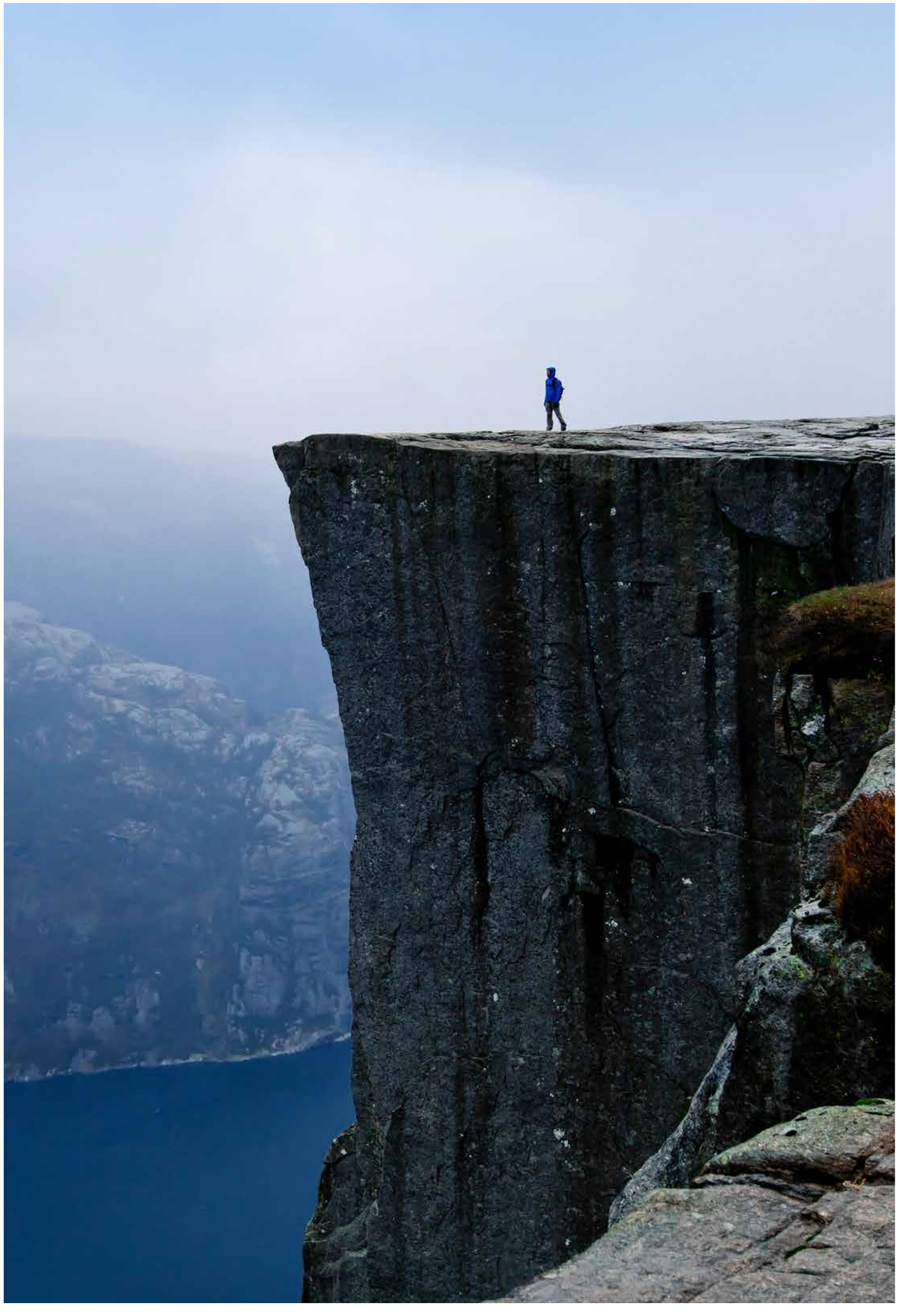
Undersøkelsen går også inn på i hvilken grad den enkelte selv oppsøker informasjon som kan øke deres ferdighetsnivå innen digital sikkerhet. Dette kan være et uttrykk for en indre motivasjon til å lære mer om digital sikkerhet.

Ca. en tredjedel oppgir at de i ganske stor eller svært stor grad selv oppsøker slik informasjon, mens også en tredjedel oppgir at de i ganske liten eller svært liten grad gjør dette. Her ligger et stort potensial i å finne ut hvorfor så mange ikke oppsøker informasjon som kan øke deres ferdighetsnivå, og å motivere flere til å gjøre dette.

I hvilken grad oppsøker du selv informasjon som kan øke ditt ferdighetsnivå innen digital sikkerhet? (Prosent)







SIKKERHETSATFERD

Gode holdninger og riktig kunnskap er viktig, men det må også komme til uttrykk gjennom sikker atferd. De fleste eksperter er enig om visse ting alle må gjøre for å unngå digitale trusler. Man skal velge sikre passord, holde de digitale enhetene oppdaterte, ta sikkerhetskopi av viktige data, unngå å åpne lenker man ikke stoler på, ikke la seg lure av kriminelle og mye mer.

I sum utgjør dette et atferdsmønster som kan avgjøre om man er sikker i møtet med digitale trusler. Det er ønskelig at så mange som mulig har en sikker atferd på nett, og spesielt at de gjør de tingene som har størst effekt. For eksempel å bruke 2-trinns verifikasjon der det er mulig.

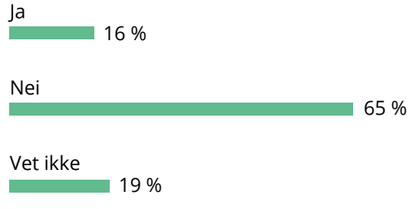
Disse atferdsmønstrene er ikke hugget i sten. De endrer seg over tid fordi vi lærer mer om hva som fører til god sikkerhet og fordi teknologien, eller bruken av den, endrer seg. Bruk av passord er et slikt eksempel. Tidligere fikk man råd om å bruke kompliserte passord (For eksempel 43yHH!q), bytte dem ofte og absolutt ikke skrive dem ned. I dag sier ekspertene at passordene skal være lange, at man ikke skal bytte dem før det er nødvendig og at man gjerne kan skrive dem ned (og oppbevare dem på en sikker plass) dersom det hjelper en å huske dem.

Rådet om å holde de digitale enhetene oppdatert har ikke endret seg, men hvordan man utfører det på har kanskje endret seg for mange. Tidligere måtte man selv holde programvare og operativsystemene oppdaterte. Nye versjoner måtte lastes ned, og installeres av den enkelte. Nå blir mange programmer og operativsystemer oppdatert automatisk. I stedet har vi fått svært mange nye ting som kobles på nett (alt fra lyspærer til kjøleskap) som ikke har den samme graden av automatisering når det kommer til det å holde systemene oppdaterte. Rådet om å oppdatere enhetene har derfor fått en ny betydning for mange.

Undersøkelsen ser på atferdsmønstrene for å finne ut hva nordmenn gjør for å holde seg trygge på nett, og for å finne ut om atferden i befolkningen endrer seg i tråd med de rådene som gis om sikker digital atferd.

De fleste respondentene oppgir at de ikke bevisst bryter reglene for digital sikkerhet, mens 16 % sier at de gjør dette. Det er også verdt å merke seg at 19 % sier at de ikke vet om de bryter reglene bevisst.

Det hender at jeg bevisst bryter regler for digital sikkerhet



Reglene for digital sikkerhet er en del av normene, altså de forventningene fellesskapet har til at den enkelte skal handle i tråd med det vi mener er sikkert. Slike normer kan være skrevet ned, for eksempel i en instruks fra arbeidsgiver eller i en brukeravtale til en spesifikk digital

tjeneste. De kan også være mer uuttalte regler, ting «man bare ikke skal gjøre».

Slike regler vil naturligvis variere fra en arbeidsplass til en annen, eller fra miljø til miljø. Det som kan være «strengt forbudt» noen steder, er kanskje ikke så farlig et annet sted. Når man i denne undersøkelsen spør om folk bevisst bryter reglene, er det med andre ord ikke for å kontrollere om spesifikke normer og regler blir overholdt, men om respondentene er klar over om de bryter reglene eller ikke.

Regler for digital sikkerhet kan være kompliserte å forholde seg til, og det er ikke alltid så godt å vite hvorfor en regel er slik den er. Hvilken digital fare er det man egentlig unngår ved å følge akkurat denne regelen? Vil man bli rammet selv dersom regelen ikke følges, eller vil det kunne gå ut over noen andre? Dersom regelen er hemmende for det man ønsker å oppnå ved å bruke digitale tjenester, hvem kan og bør sette reglene til side?

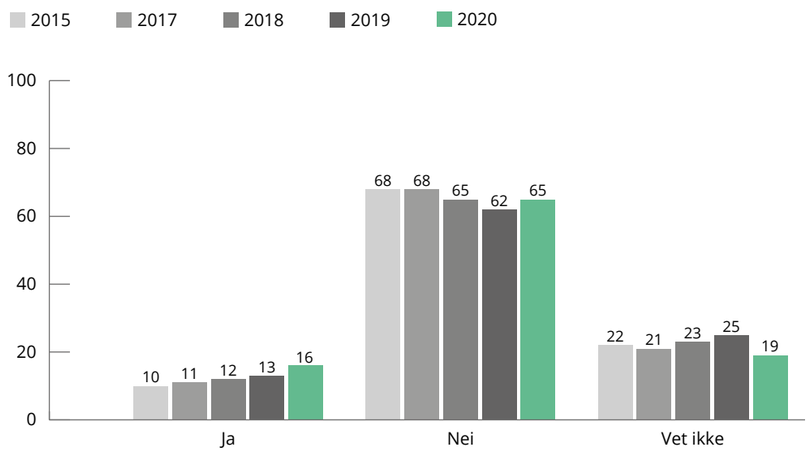
Noen regler kan være svært vanskelige å følge, og bør endres eller oppdateres. Et slik eksempel kan være at man blir avkrevd å bruke unike passord på enhver brukerkonto. Grunnlaget for regelen er at dersom et passord skulle komme på avveie, så vil man ikke kunne bruke det til å logge seg på noen andre steder. Denne regelen var kanskje mulig å følge da vi bare hadde noen få brukerkontoer på nett, men i dag er den svært vanskelig å følge fordi de fleste av oss har svært mange digitale brukerkontoer. Å lage sterke passord for alle disse, uten å gjenbruke noen passord, er svært krevende. Spesielt dersom man fra tjenesteleverandøren blir bedt om å skifte passordene regelmessig.

En løsning for mange er å velge unike passord på de viktigste tjenestene, og å skrive dem ned på et trygt sted selv om det sistnevnte også er imot reglene mange steder. For mange vil et passordverktøy være til nytte for å holde styr på mange passord.

Arbeidsgivere og leverandører av digitale tjenester bør kartlegge i hvilken grad brukerne bryter reglene, og bruke dette som en indikasjon på om de bør jobbe med å kommunisere behovet for reglene bedre, eller å revidere om reglene i seg selv er mulige å følge.

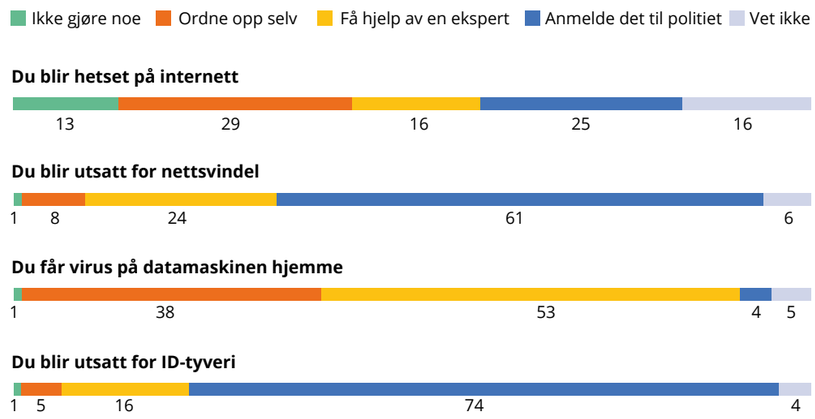
Undersøkelsen viser at det er en økende tendens at folk bryter reglene bevisst.

Det hender at jeg bevisst bryter regler for informasjonssikkerhet. (Prosent)



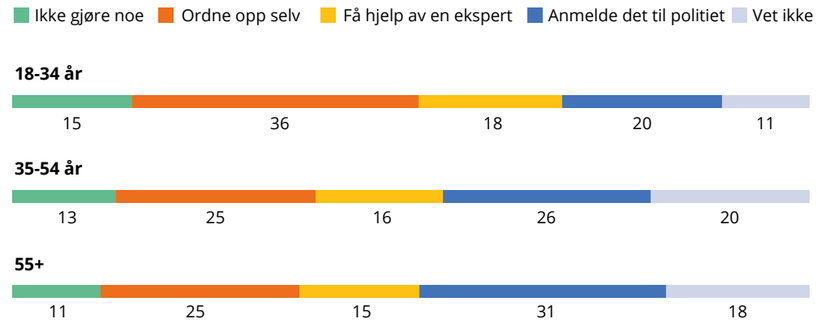
Hvordan folk reagerer på hendelser er også en del av sikkerhetsatferden. Respondentene blir spurt om hva de mest sannsynlig vil gjøre dersom de blir utsatt for noen av de mest vanlige hendelsene nordmenn opplever på nett.

Hva vil du mest sannsynlig gjøre dersom du blir utsatt for følgende? (Prosent)



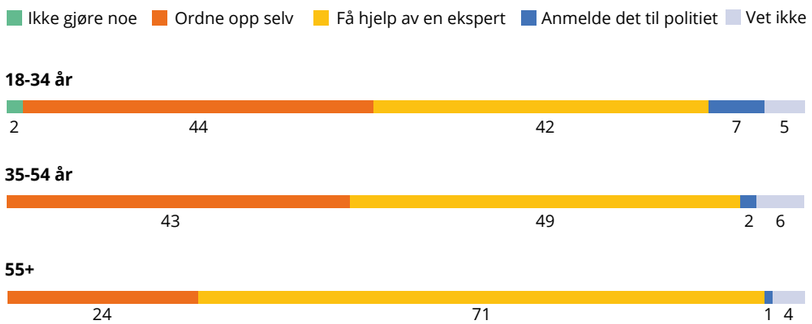
Når en betrakter respondentenes alder ser man at de yngre (18-34) er mer tilbøyelig til å ville ordne opp selv dersom de blir hetset på nett, mens de eldre (55+) er mer tilbøyelig til å ville anmelde det til politiet.

Hva vil du mest sannsynlig gjøre dersom du blir hetset på internett? Aldersforskjeller. (Prosent)



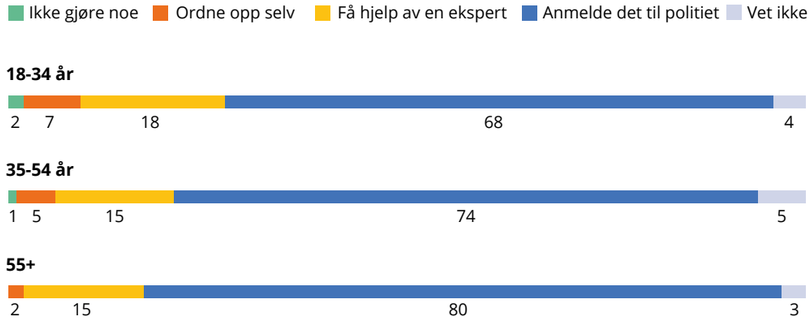
For det tilfellet at respondentene får virus på datamaskinen hjemme vil de enten ordne opp i dette selv, eller be om hjelp av en ekspert. Den eldste gruppen vil i hovedsak be om hjelp, heller enn å ordne opp selv.

Hva vil du mest sannsynlig gjøre dersom du får virus på datamaskinen hjemme? Aldersforskjeller. (Prosent)



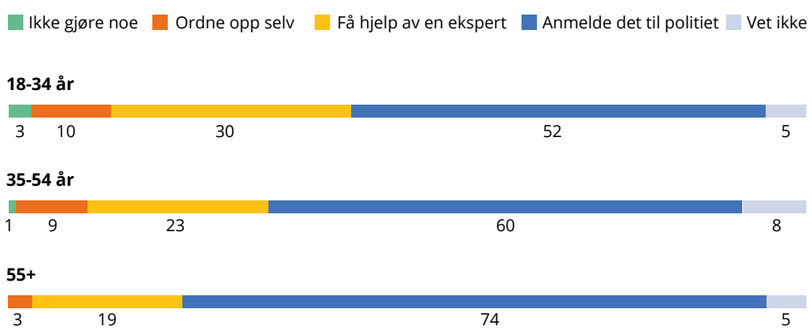
Mange nordmenn blir utsatt for ID-tyveri, og ved en slik hendelse oppgir de fleste respondentene at de vil anmelde det til politiet.

Hva vil du mest sannsynlig gjøre dersom du blir utsatt for ID-tyveri? Aldersforskjeller. (Prosent)



Det er også aldersforskjeller når det gjelder spørsmålet om hva man vil gjøre dersom man blir utsatt for nettsvindel. Svært få eldre sier at de vil ordne opp i dette selv, men sier derimot at de vil anmelde dette til politiet. Den yngste gruppen sier derimot i større grad enn de andre at de vil be om hjelp fra en ekspert. Det er også tre ganger så mange i den yngste gruppen som sier at de vil ordne opp selv, enn blant de eldste.

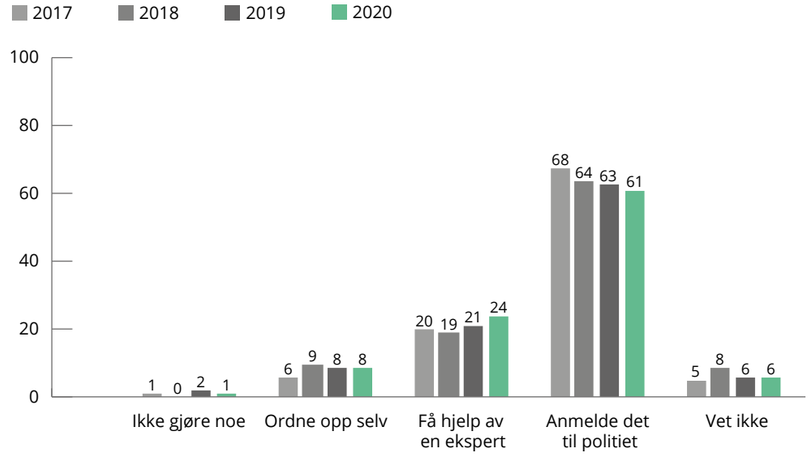
Hva vil du mest sannsynlig gjøre dersom du blir utsatt for nettsvindel? Aldersforskjeller. (Prosent)



Dersom en observerer dette spørsmålet over tid ser man en synkende tendens til at nordmenn vil anmelde nettsvindel til politiet. Undersøkelsen gir ikke svar på hva som er årsaken til denne tendensen, men en forklaring kan være at tilliten til at politiet skal kunne hjelpe dem synker. At hele 30 % av den yngste gruppen heller vil få hjelp av en ekspert, kan tyde på at de ønsker å gjøre noe med det, men at det ikke er politiets oppgave å hjelpe dem.

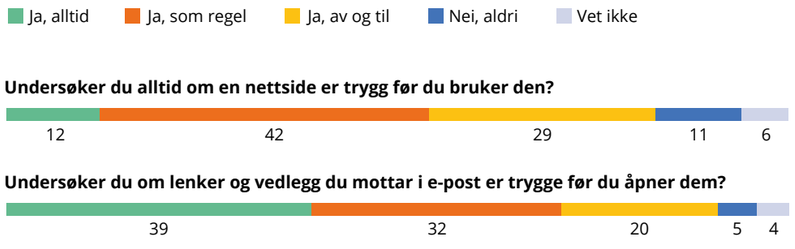
En forklaring kan være at nordmenn ikke anser nettsvindel for å være så alvorlig at en anmeldelse er nødvendig.

Hva vil du mest sannsynlig gjøre dersom du blir utsatt for nettsvindel? (Prosent)



Det vil alltid hvile et stort ansvar på den enkelte, når det kommer til deres digitale sikkerhet. En del av forebyggingen mot digitale trusler er å unngå å bli lurt når man bruker nettsider eller epost. Dette er de mest brukte angrepsvektorene, og er gjerne der man bør være mest på vakt.

Undersøker du alltid om nettsider, lenker og vedlegg er trygge? (Prosent)

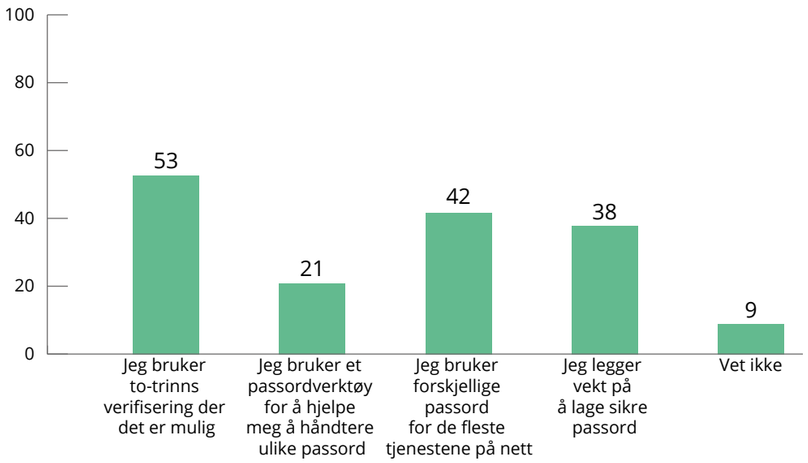


Respondentene blir spurt om de alltid undersøker om en nettside er trygg før de bruker den. De fleste gjør dette, mens 11 % sier at de aldri gjør det. Det er ingen vesentlige forskjeller basert på kjønn eller alder.

Respondentene blir også bedt om å angi om de undersøker lenker og vedlegg som de mottar i e-post. Her er det kun 5 % som sier at de aldri undersøker om de er trygge før de åpner dem.

I undersøkelsen ser man på passord, og hvordan respondentene forholder seg til de rådene som gis for bruk av passord.

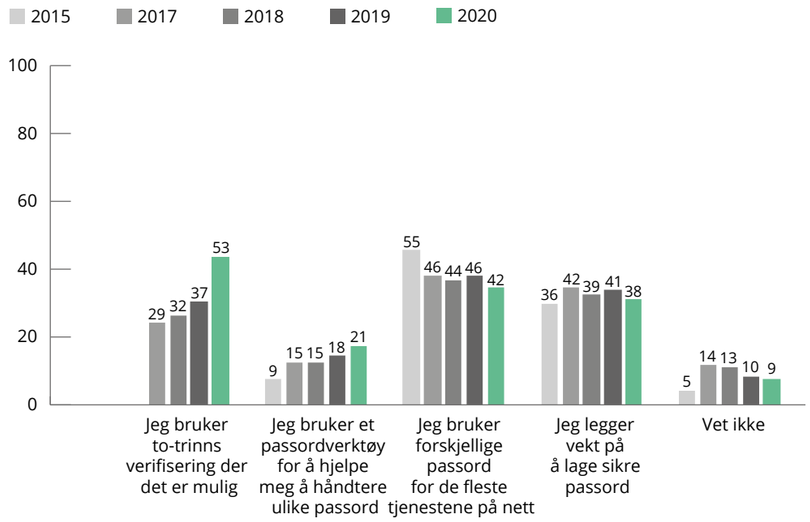
Hvordan bruker du passord i privat sammenheng?
Respondenten kunne her krysse av for flere alternativer. (Prosent)



Når en observerer dette over tid, ser man visse tendenser. Det er for det første en klar økning i bruk av to-trinns verifisering i befolkningen. Dette er en svært positiv utvikling fordi bruk av to-trinns verifisering er en av de mest effektfulle tiltakene for å beskytte digitale brukerkontoer. Undersøkelsen gir ikke svar på om økningen skyldes at respondentene har blitt mer klar over betydningen av tiltaket, eller om leverandørene av digitale tjenester nå i større grad krever eller anbefaler at brukerne aktiverer sikkerhetstiltaket.

Det er også en økning i bruk av passordverktøy, og en svak nedadgående tendens om at folk bruker forskjellige passord for de fleste tjenestene på nett. Disse to tingene kan ha en sammenheng. Økt bruk av passordverktøy muliggjør at man kan velge forskjellige passord fordi man ikke lenger trenger å huske på passordene selv.

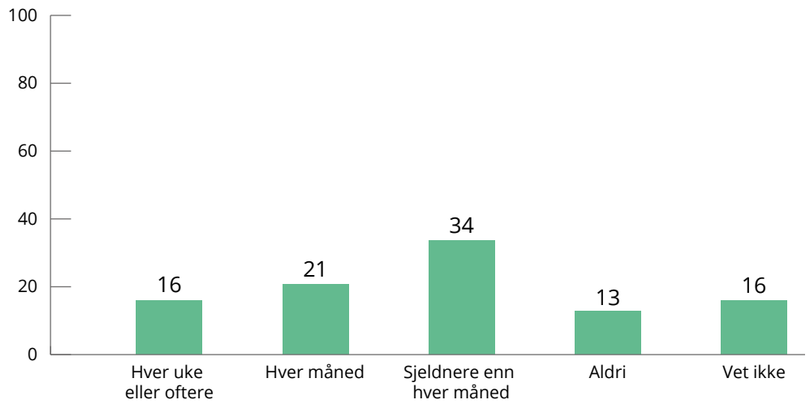
Hvordan bruker du passord i privat sammenheng?
Respondenten kunne her krysse av for flere alternativer. (Prosent)



Det er enkelte forskjeller mellom aldersgruppene. I den yngre aldersgruppen (18-34) oppgir 29 % at de bruker passordverktøy, mens i den eldste gruppen (55+) oppgir 12 % det samme. Den eldste gruppen er imidlertid flinkere til å bruke forskjellige passord enn de to andre gruppene. 49 % av de over 55 svarer at de bruker forskjellige passord for de fleste tjenestene på nett, mens 38 % av de i gruppen 35-54 og 40 % av de i gruppen 18-34 svarer det samme.

Sikkerhetskopiering er et tiltak som kan forhindre at konsekvensene ved egne feil, eller ved noen typer datakriminalitet, blir store for den som blir utsatt for tap av data. Alle bør sikkerhetskopiere data som er viktige, og den enkelte må vurdere hvor ofte det er nødvendig å ta slike kopier.

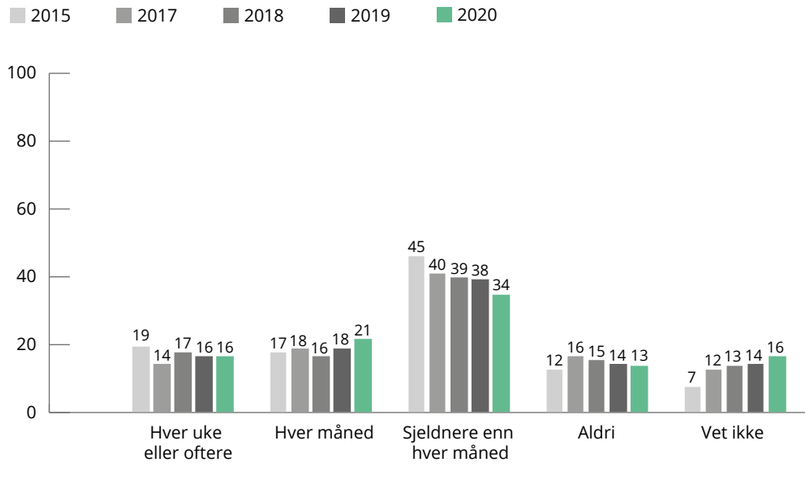
Hvor ofte sikkerhetskopierer du data som er viktige for deg i privat sammenheng? (Prosent)



Det er først og fremst andelen som svarer «Vet ikke» som er økende. En mulig forklaring på dette er at vi i mindre grad enn før tar en aktiv rolle i sikkerhetskopiering.

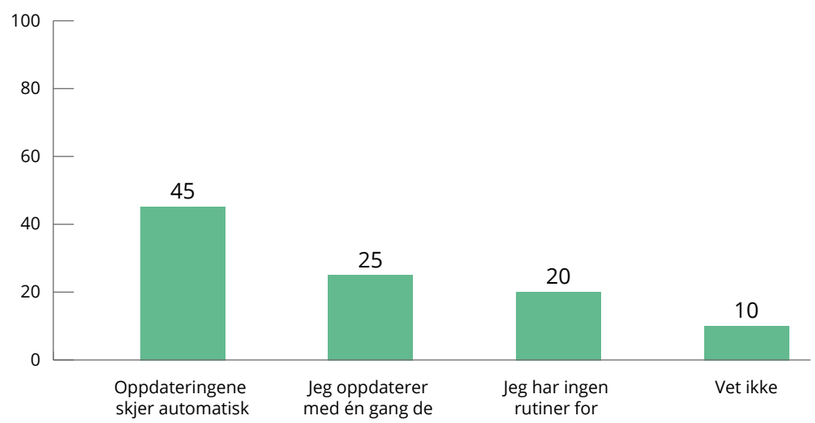
Mye skjer nå automatisert i operativsystemer, programmer og apper, og det er derfor ikke nødvendigvis slik at man vet hvor ofte sikkerhetskopieringen skjer.

Hvor ofte sikkerhetskopierer du data som er viktige for deg i privat sammenheng? (Prosent)

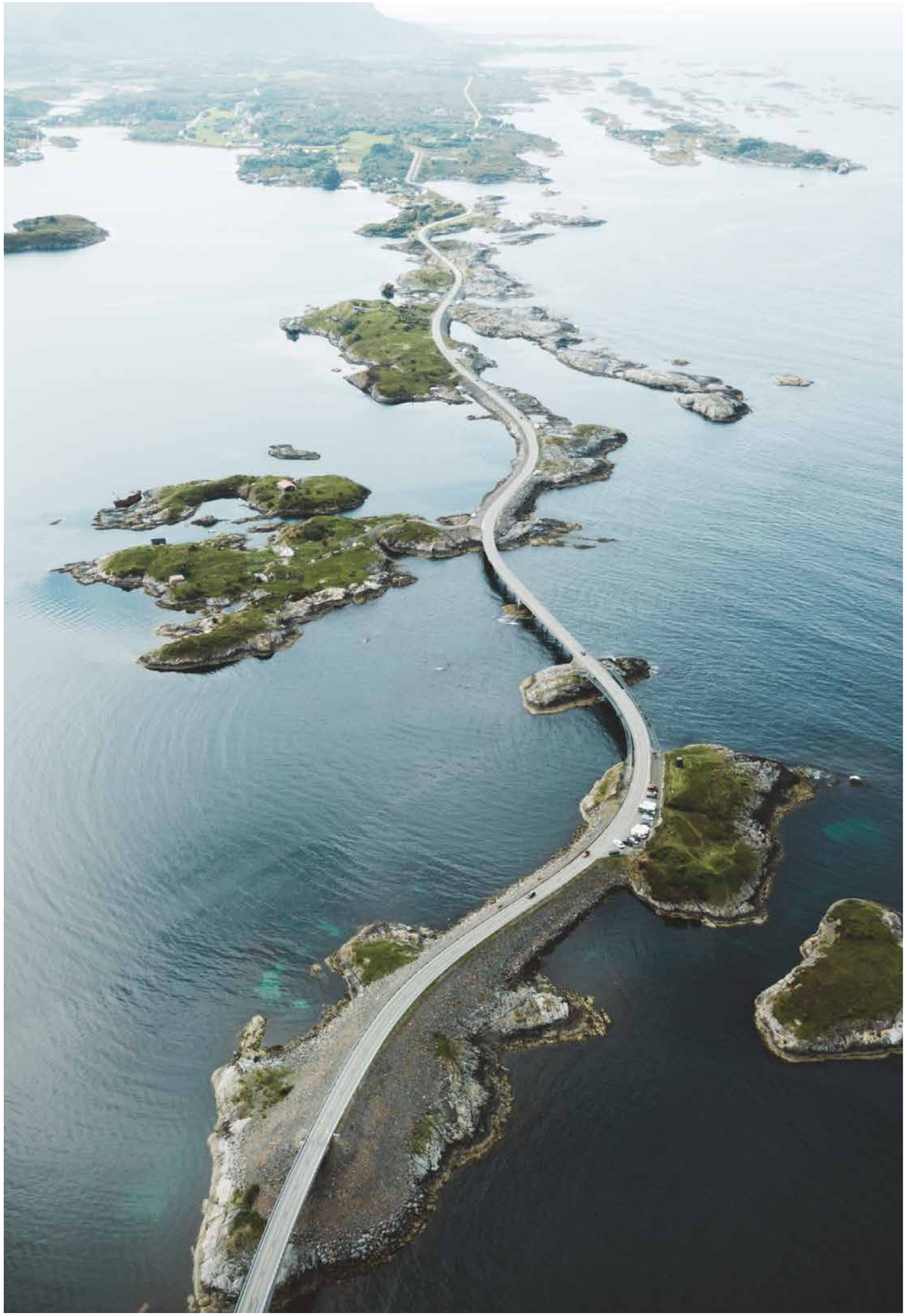


Nesten halvparten oppgir at oppdateringer av operativsystemer og programmer skjer automatisk, og en fjerdedel oppgir at de selv gjør dette så snart oppdateringene er tilgjengelig.

Har du rutiner for å oppdatere operativsystemene og programmene på din private datamaskin? (Prosent)



Dersom en betrakter respondentenes alder ser man at blant den eldste gruppen (55+) sier 55 % at oppdateringene skjer automatisk, mens kun 32 % av den yngste gruppen (18-34) sier det samme. Resultatene er omvendt for alternativet «Jeg oppdaterer med én gang de er tilgjengelige», der 33 % av den yngste gruppen svarer dette, mens kun 19 % av den eldste gruppen svarer det samme. Dette kan skyldes at det i noen grad krever teknisk kompetanse å sikkerhetskopiere data, og at de som er eldre i mindre grad har nødvendig kompetanse til dette.



NORDMENNS OPPFATNING AV DIGITAL RISIKO KNYTTET TIL COVID-19

Samfunnsutviklingen påvirker, og blir påvirket av, den digitale sikkerhetskulturen. I særdeleshet det som handler om hvordan vi bruker og sikrer det digitale. I NorSIS rapport fra 2019 så man nærmere på hvorvidt regjeringens lovforslag om tilrettelagt innhenting (digitalt grenseforsvar) påvirket våre holdninger omkring spørsmål om overvåking og kontroll. Det er av betydning å følge med på samfunnsutviklingen, og forsøke å relatere dette til det nasjonale digitale sikkerhetskulturen. Slik kan vi bedre forstå mekanismene i kulturutviklingen og vi kan som samfunn være bedre forberedt når endringer skjer.

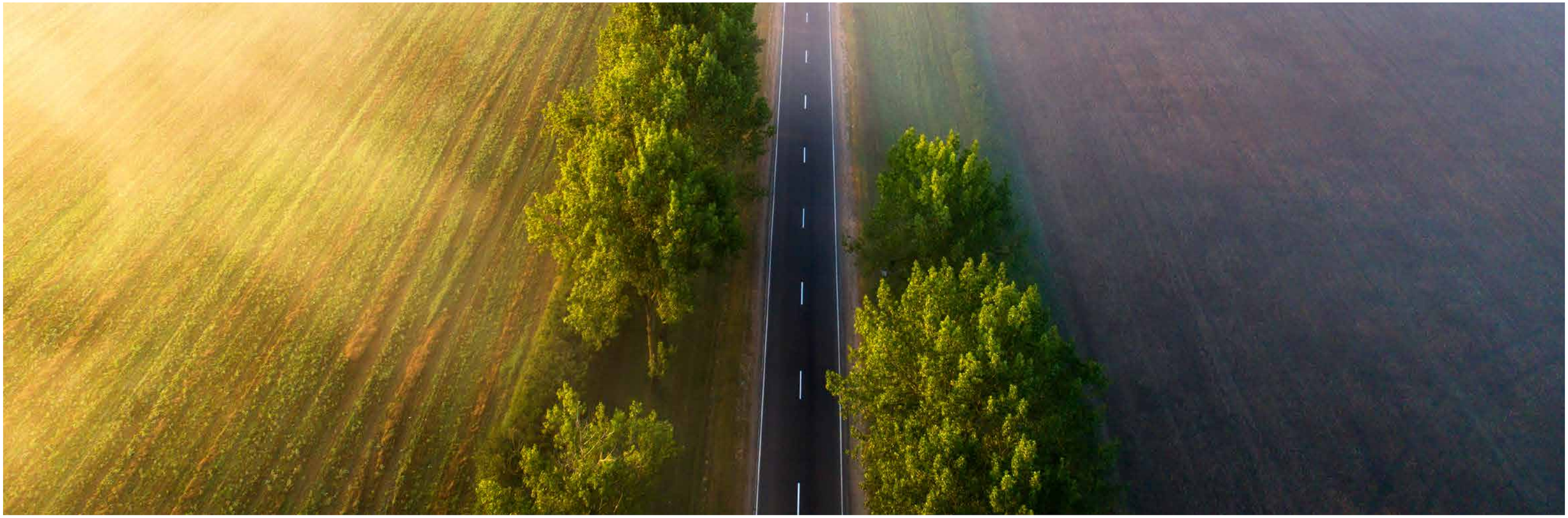
Den store hendelsen i 2020 er utvilsomt utbruddet av Covid-19, og det som fulgte da Regjeringen innførte en rekke omfattende tiltak og restriksjoner den 12. mars. Blant disse var restriksjoner på reiser og at folk ikke lenger kunne samles i større grupper. Norske bedrifter svarte hurtig med å enten pålegge eller oppfordre de ansatte å arbeide hjemmefra.

Både sikkerhetsmyndigheter, andre aktører innen digital sikkerhet og mediene har advart mot risikoen denne nye situasjonen kan føre til[8, 9, 10]. For mange ansatte i norske virksomheter har situasjonen endret seg på den måten at de ikke lenger er like godt beskyttet mot digitale trusler gjennom arbeidsgivers sikkerhetssystemer.

Mens det er vanlig at datanettverkene på jobb er sikret med brannmurer, overvåking og andre beskyttelsesmekanismer, er det ikke like vanlig at hjemmenettverkene er sikret på samme måte.

Noen arbeidsgivere tilbyr VPN-løsninger slik at de ansatte kan koble seg til datanettverket som om de var fysisk til stede på kontoret. For noen viser det seg imidlertid at VPN-løsningene, som i utgangspunktet var ment å være et tiltak for ansatte på reise, ikke er dimensjonert for at alle ansatte skal bruke det hele tiden. For noen blir resultatet at sikkerhetsløsningene ikke virker som planlagt, og at man av den grunn blir mer sårbar fordi man blir tvunget til å la være å bruke dem.

Sårbarhetene rundt bruk av hjemmekontor kan også øke ved at noen bruker privat utstyr til å utføre arbeidsoppgaver. Slikt utstyr er ofte ikke forvaltet og sikret på samme måte som utstyret som er levert fra arbeidsgiver, og det er da en fare for at programvare og operativsystemene ikke er oppdaterte. Dersom utstyret, enten det er privat eller levert fra arbeidsgiver, brukes til private formål (for eksempel av barn eller andre) kan det også medføre en økt sårbarhet fordi det kan bli installert ondsinnet kode som følger med spill, programvare eller nettsteder.



Kort tid etter at utbruddet av Covid-19 ble erklært som en pandemi, ble det registrert at kriminelle utnyttet situasjonen til å spre ondsinnet kode og til å gjennomføre ulike typer informasjonstyverier og bedragerier.[11, 12, 13, 14, 15, 16, 17]

Som mennesker er vi kanskje ekstra sårbare for å bli manipulert i en situasjon som denne. Vi kan alle føle på utrygghet og en trang til informasjon om hva som skjer i samfunnet. En velutformet epost eller melding i sosiale medier kan trigge vårt informasjonsbehov, og en klikker, åpner eller aksepterer det en vanligvis ikke ville ha gjort. Resultatet er at betalingsinformasjon eller brukernavn/passord blir stjålet, at det blir installert ondsinnet kode på våre datamaskiner som setter både vår egen og arbeidsgivers informasjon i fare, eller at våre datamaskiner blir brukt som verktøy i angrep på andre.

Metode

NorSIS har undersøkt hva befolkningen tenker om hvordan det digitale risikobildet har endret seg som en følge av korona-utbruddet og de påfølgende tiltakene.

Undersøkelsen ble gjennomført av YouGov Norway AS i uke 14 og 15, altså 4-5 uker etter at de første tiltakene ble innført av Regjeringen.

NorSIS ønsket å vite mer om hvordan den norske befolkningen ser på risiko knyttet til sin egen situasjon, og til situasjonen for fellesskapet, og stilte følgende spørsmål:

1. Tror du at korona-utbruddet medfører en endring i det digitale risikobildet for samfunnet?
2. Tror du at korona-utbruddet medfører en endring i det digitale risikobildet for deg selv?

Respondentene er ikke bedt om å angi et tidspunkt eller tidsperiode for sin vurdering. Det legges derfor til grunn at respondentene har svart med bakgrunn i en vurdering i det øyeblikket spørsmålet ble stilt. Det er heller ikke gitt noen orientering om eventuelle sikkerhetstiltak som myndighetene eller andre har iverksatt som en konsekvens av den nye situasjonen. Det legges derfor til grunn at respondentene har svart med bakgrunn i den kunnskapen de allerede hadde på tidspunktet spørsmålet ble stilt. Det er med andre ord respondentens oppfatning av risiko som er i fokus her, ikke en vurdering av risiko der alle forhold er tatt i betraktning.

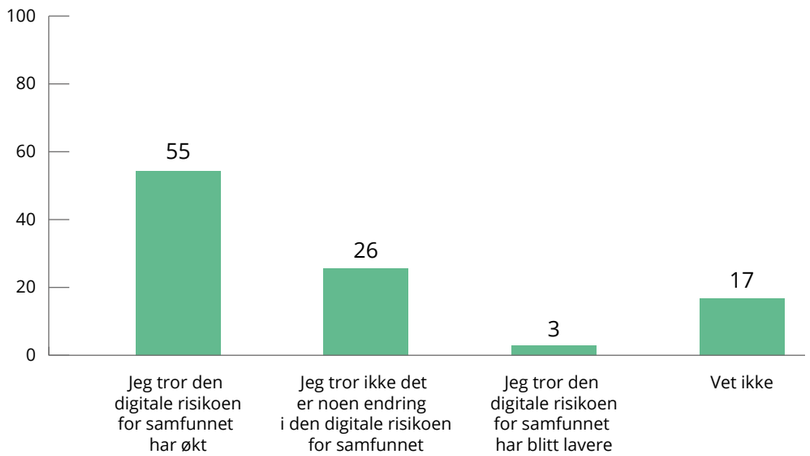
I NorSIS årlige undersøkelser av befolkningens digitale sikkerhetskultur legges det vekt på å undersøke respondentenes syn på fellesskapet, i et sikkerhetsperspektiv. I et digitalisert samfunn henger alt sammen med alt, og sikkerhet for fellesskapet innebærer at den enkelte må ta et ansvar for sikkerhet for både seg selv og andre.

I denne undersøkelsen spørres det om respondenten tror at korona-utbruddet medfører en endring i det digitale risikobildet for samfunnet, eller for seg selv. Hensikten med spørsmålet er å avdekke om respondentene er oppmerksom på hvorvidt risikobildet har endret seg, dernest hvordan de tror at risikoen har endret seg. Før en kan forvente at noen skal handle sikkert, må en være oppmerksom på at det er behov for en slik handling. Vi omtaler gjerne dette som at man må være «bevisst». En bør imidlertid merke seg at en slik bevissthet ikke i seg selv nødvendigvis fører til en handling som ivaretar ens egen eller andres sikkerhet. Å være oppmerksom på en endring i risiko er imidlertid en av forutsetningene for at den enkelte skal endre sin sikkerhetsatferd.

Risiko for samfunnet

På spørsmålet *Tror du at korona-utbruddet medfører en endring i det digitale risikobildet for samfunnet?* svarer respondentene slik:

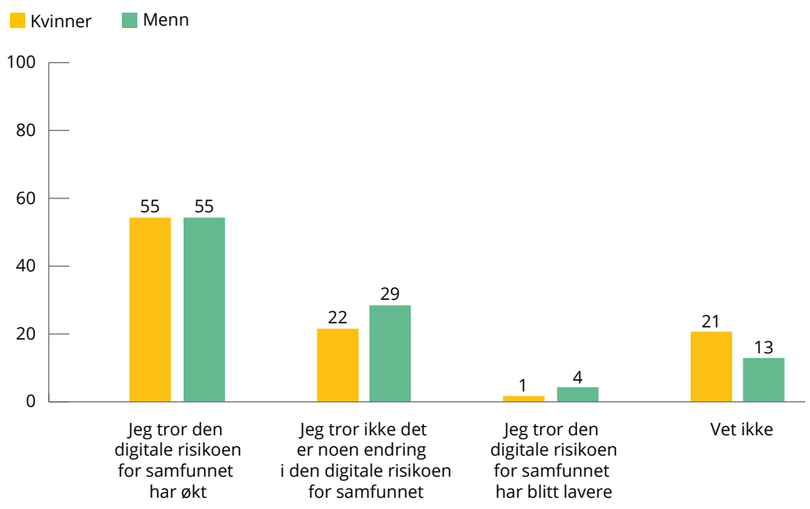
Tror du at korona-utbruddet medfører en endring i det digitale risikobildet for samfunnet? (Totalt. Prosent)



Over halvparten av befolkningen mener at den digitale risikoen for samfunnet har økt som en følge av korona-utbruddet, mens omtrent en fjerdedel mener at det ikke er noen endring i den digitale risikoen.

Dersom en ser på kjønnsfordelingen ser man følgende:

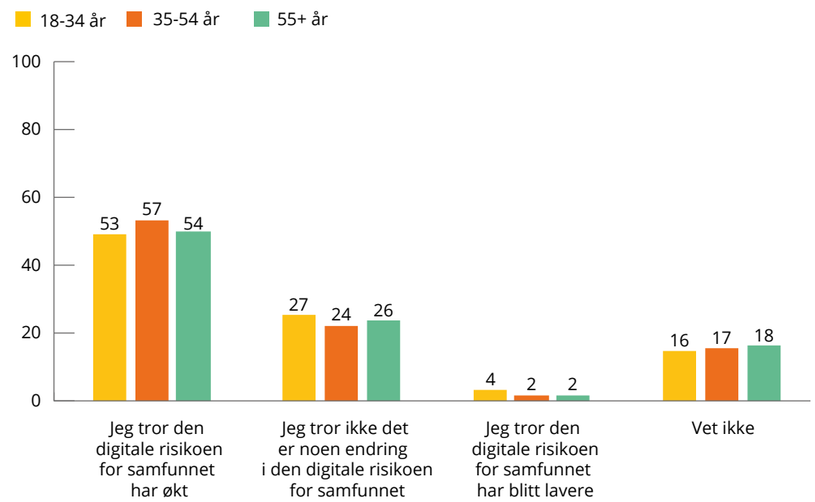
Tror du at korona-utbruddet medfører en endring i det digitale risikobildet for samfunnet? (Kjønnsforskjeller. Prosent)



Det er ingen forskjell mellom kvinner og menn på synet om at den digitale risikoen har økt. Det er imidlertid en signifikant forskjell mellom kvinner og menn på synet om at det ikke er noen endring i digital risiko. Mens 22 % av kvinner mener at det ikke er noen endring, mener 29 % av menn det samme. Vi ser en tilsvarende, men motsatt, forskjell mellom kvinner og menn som har svart «Vet ikke» på spørsmålet.

Dersom en betrakter alder ser man følgende:

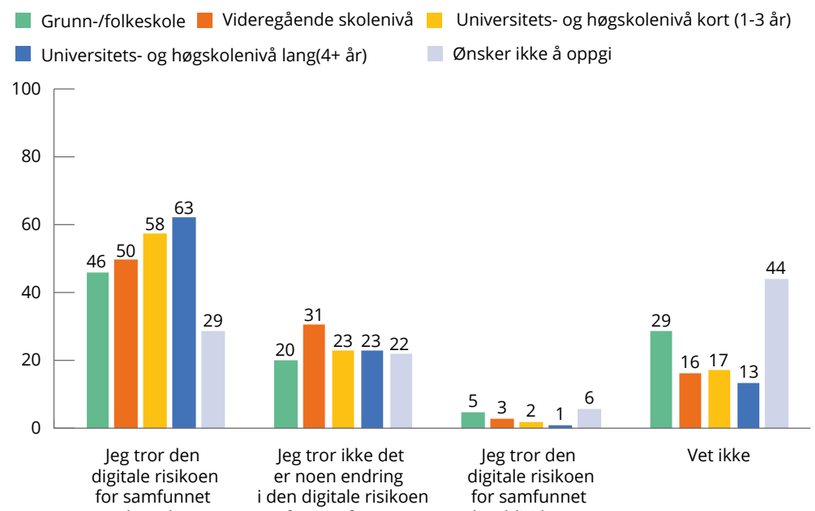
Tror du at korona-utbruddet medfører en endring i det digitale risikobildet for samfunnet? (Alder. Prosent)



Det er ingen signifikante forskjeller mellom aldersgruppene i dette spørsmålet.

Dersom en betrakter utdanningsnivå ser man følgende:

Tror du at korona-utbruddet medfører en endring i det digitale risikobildet for samfunnet? (Utdanningsnivå. Prosent)



Med utdanningsnivå menes her høyeste fullførte utdannelse. Det er en signifikant forskjell blant de som har svart at de tror at den digitale risikoen for samfunnet har økt, der de med universitetsutdannelse (kort og lang) i større grad mener at risikoen har økt. 63 % av de med lang universitetsutdannelse svarer dette, mens 58 % av de med kort universitetsutdannelse har svart det samme. Til sammenligning har 46 % av de mer grunn- eller folkeskole svart det samme. Kun 29 % av de som ikke vil oppgi utdanningsnivå mener at samfunnets risiko har økt. Sistnevnte kategori er også sterkt representert blant de som angir «Vet ikke».

Vurdering

Med tanke på at digital risiko har fått stor oppmerksomhet i media etter at Regjeringen innførte tiltakene i midten av mai, er det som forventet at mange mener at den digitale risikoen i samfunnet har økt. Det er interessant å merke seg at svært få mener at risikoen har blitt lavere, og at omlag en fjerdedel av befolkningen mener at det ikke er noen endring. Undersøkelsen gir ikke svar på hvorfor respondentene svarer som de gjør. Det trekkes derfor ikke slutninger omkring dette.

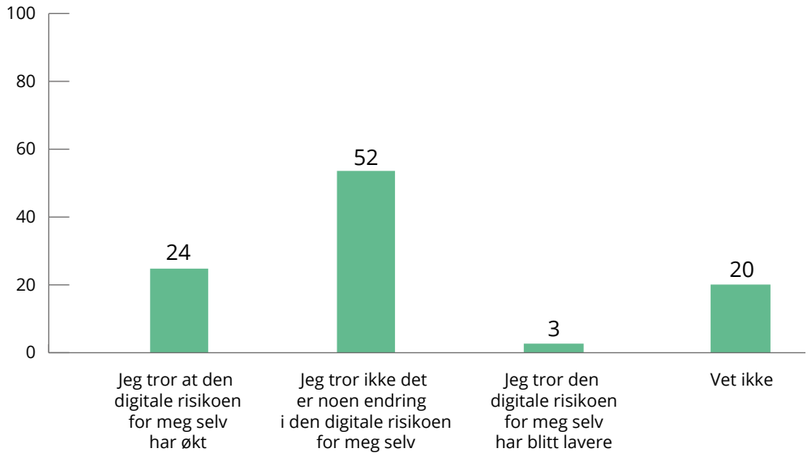
Det er imidlertid interessant å merke seg at det også for dette spørsmålet er visse kjønnsforskjeller i svarene. Dette samsvarer med NorSIS tidligere undersøkelser, som har vist at det er visse forskjeller mellom kjønnene når det kommer til interesse for teknologi og IT og hvordan kvinner og menn ser på digital risiko. At flere kvinner enn menn i denne undersøkelsen utrykker en usikkerhet omkring spørsmålet, samsvarer med funn i tidligere rapporter.

Det er også forskjeller i svarene, basert på utdanningsnivå. Jo høyere utdanning, jo fler svarer at den digitale risikoen i samfunnet har økt. En mulig forklaring på dette kan være at man gjennom å ta høyere utdanning får en bedre forståelse for hvordan ting påvirker hverandre i et samfunn. Andre forklaringer kan være at utdanningsnivået henger sammen med det å holde seg orientert om samfunnshendelser[18], eller at høyere utdanning i større grad inneholder digital sikkerhet som tematikk.

Risiko for den enkelte

På spørsmålet *Tror du at korona-utbruddet medfører en endring i det digitale risikobildet for deg selv?* svarer respondentene slik:

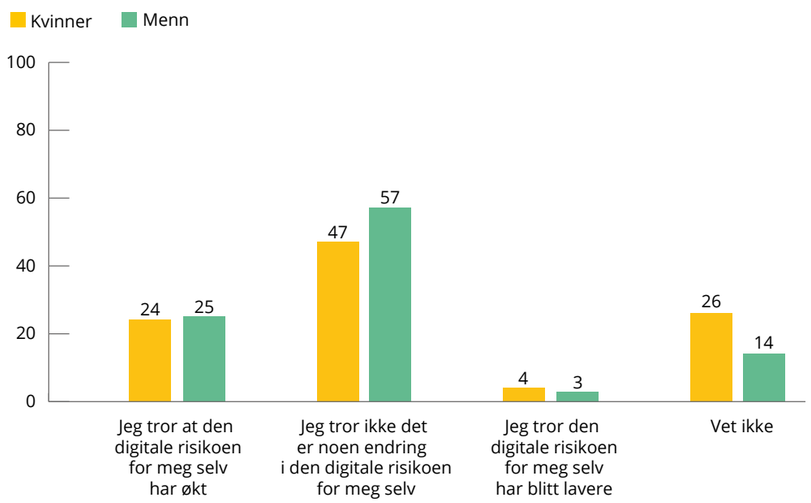
Tror du at korona-utbruddet medfører en endring i det digitale risikobildet for deg selv? (Totalt. Prosent)



Omtrent en fjerdedel av befolkningen tror at den digitale risikoen for dem selv har økt som en følge av korona-utbruddet, mens 52 % mener at det ikke er noen endring i risikobildet for dem selv. Kun 3 % mener at risikoen har blitt lavere, og 20 % oppgir at de ikke vet.

Dersom en betrakter kjønnsfordelingen ser man følgende:

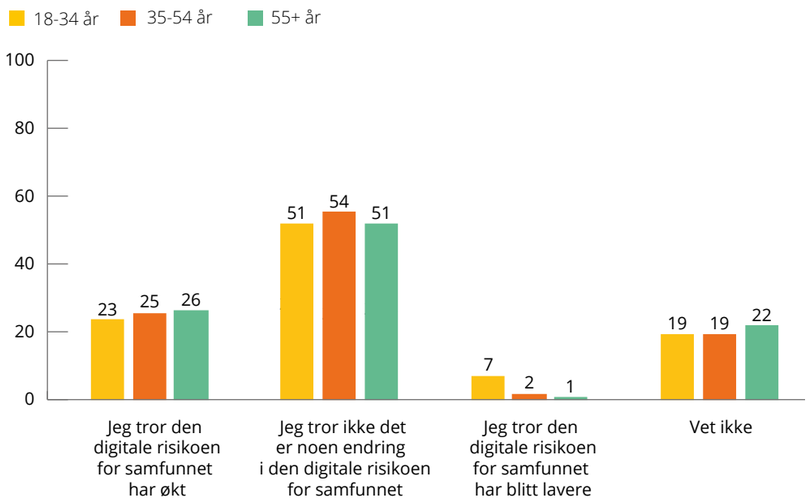
Tror du at korona-utbruddet medfører en endring i det digitale risikobildet for deg selv? (Kjønn. Prosent)



Det er en signifikant forskjell mellom kvinner og menn blant de som tror at det ikke er noen endring i risikobildet, og blant de som oppgir at de ikke vet. 57 % av menn og 47 % av kvinnene tror at korona-utbruddet ikke har ført til noen endring i risikobildet for dem selv, mens 26 % av kvinnene og 14 % av mennene oppgir at de ikke vet.

Dersom en betrakter alder ser man følgende:

Tror du at korona-utbruddet medfører en endring i det digitale risikobildet for deg selv? (Alder. Prosent)

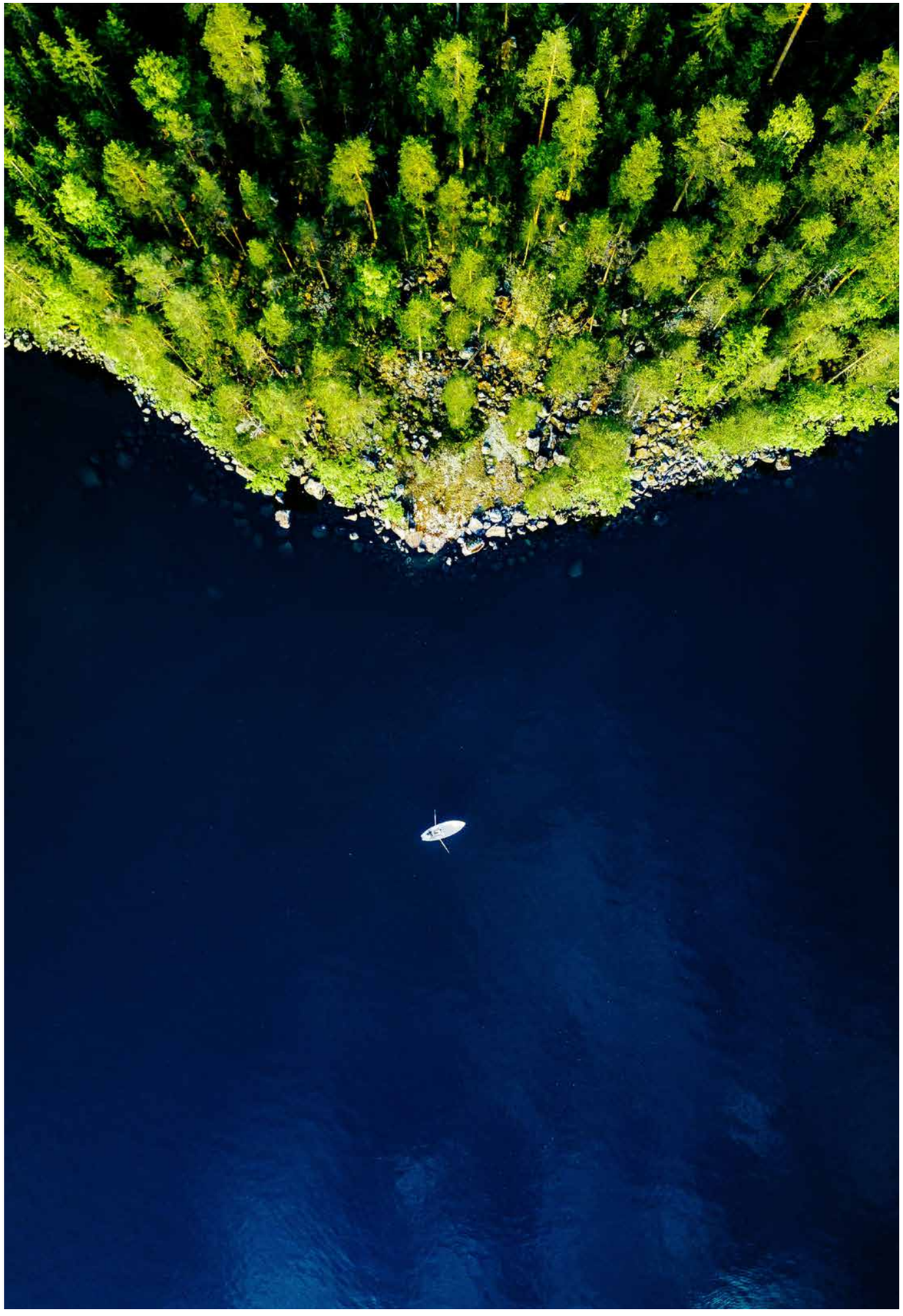


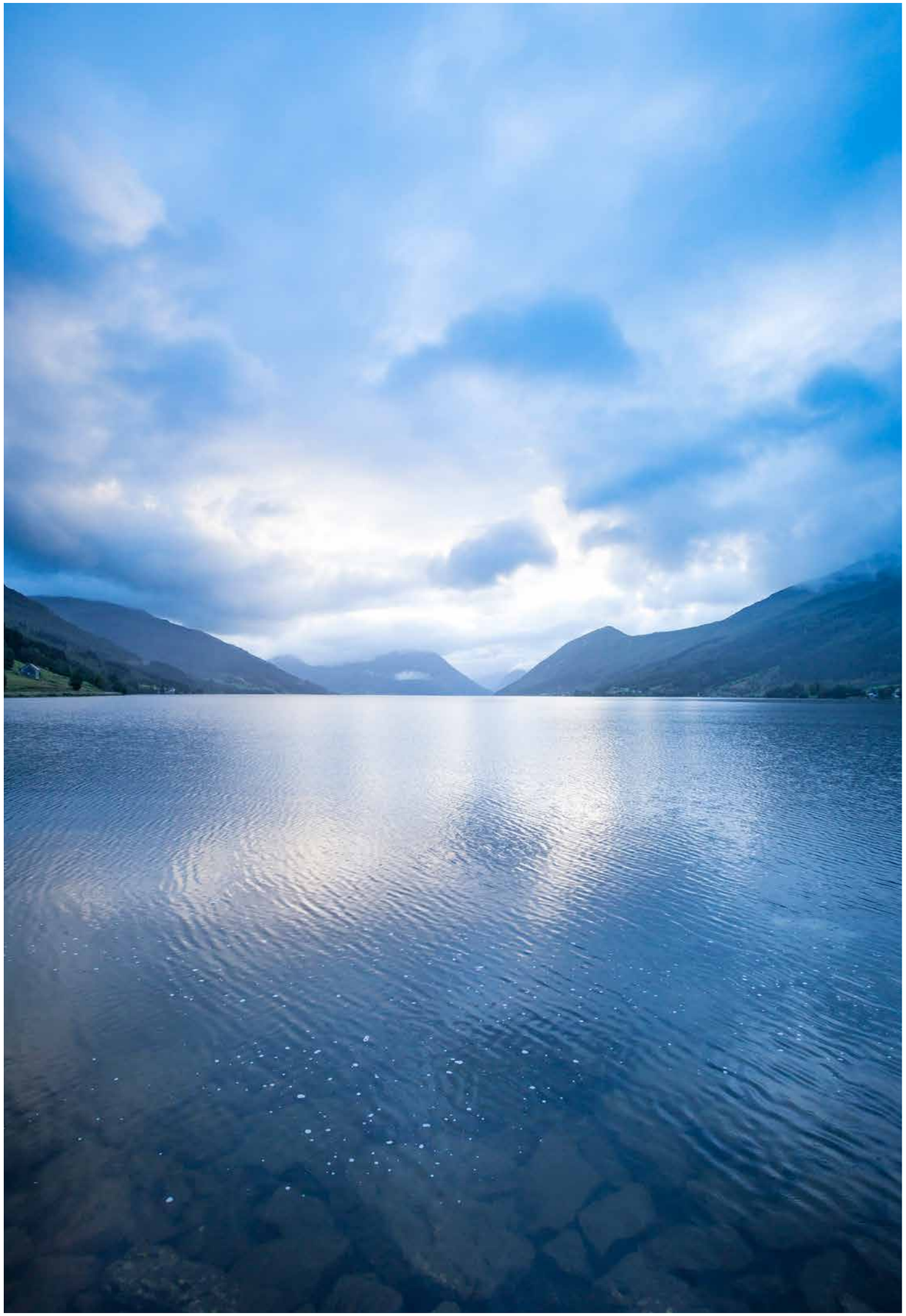
Det er en signifikant forskjell mellom aldersgruppene som kan svart at de tror den digitale risikoen for dem selv har blitt lavere etter korona-utbruddet. 7 % av de mellom 18-34 år mener at risikoen har blitt lavere, mens henholdsvis 2 % og 1 % i gruppene 35-54 år og 55+ år mener det samme.

Vurdering

Det fremstår som paradoksalt at 55 % av respondentene mener at risikoen for samfunnet har økt, mens kun 24 % mener at dette gjelder dem selv. Undersøkelsen går ikke inn i mulige forklaringsmodeller, men det et gjenkjennbart mønster fra tidligere undersøkelser om digital sikkerhetskultur. Når det kommer til synet på risiko på nett, mener nordmenn at det er mye større risiko for at noen andre skal gjøre noe mot dem (f.eks. hacke en nettside der de har personlig informasjon) enn at de selv skal gjøre noe feil.

Mange kan kjenne seg igjen i tankemønstre om at «dette kommer ikke til å hende meg», når det er snakk om ulykker eller andre uønskede hendelser. Innen psykologien definerer man dette som «Optimism bias»[19], altså at farlige eller uønskede ting muligens kan komme til å hende andre, men ikke med en selv. Den enkelte føler gjerne at de har en kontroll over de tingene som medfører digital risiko, selv om den reelle kontrollen kan være mye lavere enn en tror. En positiv side ved «Optimism bias» er at den virker inn på motivasjon. Selv om man har opplevd å bli utsatt for datakriminalitet, gir man ikke bare opp å bruke digitale tjenester. Man prøver igjen, og tenker «det kommer ikke til å skje med meg igjen». En av de negative sidene er at man gjerne undervurderer risiko.





MESTRINGSFORVENTNING (SELF-EFFICACY) INNEN DIGITAL SIKKERHET

NorSIS har kartlagt digital sikkerhetsatferd i en årrekke, både i befolkningen, i mindre grupper og blant ansatte i virksomheter. Disse kartleggingene viser at det er grunnlag for å hevde at mange har det man anser for å være god sikkerhetsatferd. For eksempel: flertallet undersøker om en nettside er trygg før de bruker den og stadig fler bruker 2-trinns verifikasjon der det er mulig.

Det er likevel en viss bekymring for at ikke atferdsmønstrene endrer seg like raskt som en skulle ønske. På noen områder skjer utviklingen sakte, og på andre områder står den på stedet hvil. NorSIS har i tidligere rapporter om digital sikkerhetskultur uttrykt en bekymring for at forbedringene uteblir, på tross av at oppmerksomheten og opplæringstilbudene innen digital sikkerhet øker.

Opplæring i digital sikkerhet

Fokuset på digital sikkerhet i samfunnet har utvilsomt økt de senere årene. Det er mange aktører som tilbyr et bredt spekter av opplæringstilbud innen digital sikkerhet, men på tross av dette uteblir mye av den ønskede atferdsendringen. Det er derfor på sin plass å stille spørsmål ved måten vi tilnærmer oss sikkerhetsopplæring, i alle fall dersom det er varig atferdsendring vi ønsker.

Undersøkelsene til NorSIS viser at opplæring i digital sikkerhet i hovedsak blir gitt til arbeidstakere, gjennom opplæringstilbud på arbeidsplassen. Det faglige innholdet i slik opplæring holder stort sett en god kvalitet. Undervisningsmålene handler i hovedsak om å overføre faktakunnskap om digital sikkerhet til mottakeren. Kunnskap om digital sikkerhet er åpenbart en nødvendig forutsetning for at den enkelte skal kunne gjøre de riktige tingene, og på den måten beskytte seg mot digitale trusler. For å lage et sikkert passord, må man vite hva det er. For å kunne undersøke om et nettsted er trygt, må man vite hvordan man gjør det.

På tross av et omfattende tilbud av opplæring i digital sikkerhet, viser kartleggingene at forventede endringer i holdninger og handlinger uteblir. Konsekvensen er at både den enkelte og samfunnet er mer utsatt for risiko. Det er vanskelig å være tilfreds med dette, og en bør undersøke hvorfor det er slik at nordmenn ikke gjør mer av de tingene som skal til for at de skal være trygge på nett.

I denne undersøkelsen svarer 88 % at de er enten helt eller delvis enig i at de vet

hva digital sikkerhet er. 73 % mener at det er viktig å tenke på digital sikkerhet både hjemme og på jobb, og 70 % mener at de utsetter seg for risiko på nett. Dette tyder på at det ikke er den såkalte bevissthetenomkring digital sikkerhet som er mangelfull. Det må være noe annet som fører til at folk ikke gjør det de bør gjøre.

En mulighet er at selve tilnærmingen til opplæring i digital sikkerhet ikke er optimalt tilpasset utfordringen, altså å få mennesker til å tenke og handle mer sikkert. Opplæringsmetoder som har som mål å overføre faktakunnskap er basert på premisset «Bare folk vet hva de skal gjøre, så kommer de til å gjøre det.» Samtidig hører man ofte at det er *den menneskelige faktoren* som er årsak til at ting har gått galt. Spørsmålet vi da må stille er om kunnskapsoverføring som metode er riktig og tilstrekkelig for å møte utfordringene som *den menneskelige faktoren* representerer.

Utfordringen ligger trolig i at kunnskapsoverføring i seg selv ikke er nok. Mennesker fungerer ikke slik at de vil gjøre alle de riktige tingene, bare de vet hva de riktige tingene er. Trolig har vi alle kjent dette på kroppen selv. Alle som har sertifikat vet at man ikke skal kjøre fortere enn fartsgrensen, og de vet hva konsekvensene av å gjøre det kan være. Likevel kjører mange for fort. Alle vet at det er skadelig for helsen å røyke. Likevel er det mange som røyker.

I disse eksemplene er det rimelig å anta at folk har nødvendig faktakunnskap, og at det derfor må være noe annet som virker inn og som forhindrer at kunnskapen blir utnyttet. Som nevnt oppgir 88 % at de vet hva digital sikkerhet er, men likevel er det langt færre som gjør alle de riktige og viktige tingene som skal til for å ivareta den digitale sikkerheten på en god måte.

Atferdsendring

Målet med sikkerhetsopplæring er ikke som regel ikke kunnskapen i seg selv. Målet er at den enkelte skal være i stand til å gjøre bedre vurderinger omkring digital risiko, og at de har en atferd som beskytter dem bedre mot digitale trusler. Når atferdsendringene uteblir må en spørre: Hva gjør vi feil, og hva kan være en bedre tilnærming?

Mange som har ansvar for å gi opplæring i digital sikkerhet er opptatt av å *bruke et språk som mottakeren forstår*. Med andre ord, bare en kommuniserer på en forståelig måte, så skal opplæringen ha ønsket effekt. Det er imidlertid lite trolig at det er uforståelig språk som er hovedårsaken til at effekten uteblir. Dersom en ser på læreplaner og undervisningsopplegg i skolen, eller på undervisningsmateriellet som tilbys av myndighetene og private aktører som leverer opplæring i digital sikkerhet, så er dette stort sett utformet på en forståelig måte.

En annen bekymring som er vanlig i sikkerhetsbransjen, er at opplæringen gis på feil tidspunkt eller med feil frekvens. Ved inngangen til Sikkerhetsmåneden 2019 ble det hevdet[20, 21] at bedrifter og virksomheter ikke burde gi opplæring til ansatte etter *skippertaksmetoden*, altså kun en gang i året. I stedet burde man gi opplæring oftere for å unngå at de ansatte slurver og glemmer hva de skal gjøre. Med andre ord: Hvis man repeterer budskapet ofte nok vil man oppnå at mottakeren utvikler en sikrere atferd.

Det er imidlertid noe dypt problematisk med begge disse synspunktene på sikkerhetsopplæring, og hva som skal til for at opplæringen skal være effektiv. Den såkalte *menneskelige faktoren* er åpenbart mye mer kompleks enn det disse tilnærmingene ser ut til å ta inn over seg. Å tenke at mennesker «vil ta til fornuft» bare en gjentar budskapet mange nok ganger, er en overforenkling på grensen til det naive. Man kan hevde at dette er en «ovenfra og ned» holdning fra vårt fagmiljø, der man antar at problemet er ukunne hos mottakeren og at det ikke er noe galt med opplæringen i seg selv. Det er det imidlertid ingen holdepunkter for. Riktignok er det mange som henviser til det menneskelige faktoren, dog uten å gjøre noen videre analyse av hva denne egentlig består i. Løsningene som foreskrives er gjerne mer av det samme: kurs – bare oftere.

Dersom hyppigere formaninger og påminnelser hadde hatt en effekt, ville vi enkelt kunne få en slutt på at mennesker spiser for mye, nyter skadelige rusmidler eller gjør andre ting som er skadelige for dem selv og andre. Årsaken til at vi ikke ser repeterende formaninger av typen «Husk å ikke spise for mye» er selvsagt fordi det ikke fungerer.

Motivasjon

Dersom målet er å bedre forstå og å påvirke den menneskelige faktoren, kan det være en mer effektiv strategi å se til motivasjonspsykologi[22].

Professor i psykologididaktikk Åge Diseth slår fast at det ikke er noen klar sammenheng mellom det vi gjør, og det som motiverer atferden: En person som velger å gjennomføre en treningsøkt på 5km kan både være motivert av et indre ønske om å forbedre tiden sin, eller av en ytre forventning fra sin lege som mener at dette må til for at han skal forbedre helsen. Kanskje treningen bare er en velkommen avkobling fra noe annet? Samtidig kan en person som har en sterk disposisjon til å prestere være tiltrukket av utfordrende situasjoner der hun får mulighet til å demonstrere sine ferdigheter. En slik motivasjon kan lede til mange ulike typer atferd, for eksempel at hun velger å løpe 5km, gjøre en ekstra innsats på jobb, utvikle ferdigheter i en fritidsaktivitet og mye annet[23]. Det er derfor liten grunn til å tro at tilnærminger til sikkerhetsopplæring som er basert på et nærmest mekanisk forhold mellom stimuli og atferd vil ha en særlig effekt, fordi den *menneskelige faktoren* er mer kompleks enn som så.

Diseth forklarer videre at det er en grunnleggende forskjell på å sette seg et mål om å oppnå et positivt resultat, og det å unngå et negativt resultat. Vi kan for eksempel ønske å oppnå en positiv anerkjennelse (approach) for å ha fulgt sikkerhetsreglene, eller å unngå en negativ kritikk (avoidance) for å ha brutt dem. Forskning innen motivasjonspsykologi viser at mennesker presterer bedre når vi er motivert av positive resultater, enn når vi har unngåelsesmotivasjon knyttet til negative utfall. Alle mennesker har motstridende tendenser til positiv anerkjennelse og negativ kritikk, men det er individuelle forskjeller som avgjør om en person lener seg mer i den ene eller den andre retningen. Dette har åpenbart en betydning for hvilken effekt ulike typer sikkerhetsopplæring har for ulike personer. Noen kan bli positivt motivert av for eksempel *spillifiseringteknikker*[24], mens andre kan bli negativt motivert av å unngå å bli «straffet» for sikkerhetsbrudd.

Det er mange ulike typer av motivasjon som kan spille en rolle for hvilken sikkerhetsatferd vi utviser, for eksempel implisitte motiver (prestasjon og tilhørighet), ytre motiver (ros og kritikk) eller indre motiver (interesse). Denne rapporten går ikke nærmere inn på disse, og det henvises til faglitteratur innen psykologi, pedagogikk og sosiologi.

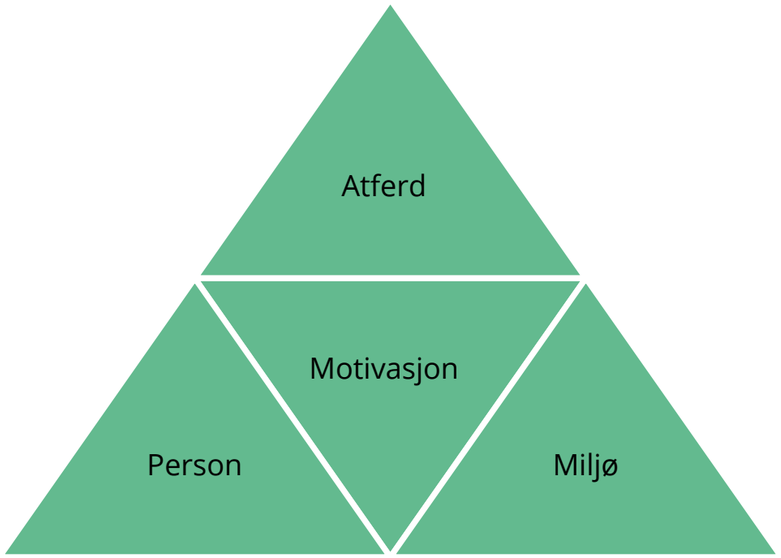
Vi vil derimot gå nærmere inn på den kognitive motivasjonsfaktoren mestringsforventning, fordi denne er en sterkt prediktor for atferd.

Mestringsforventning

Albert Bandura[25], professor i psykologi ved Stanford University, har gjennom 50 år forsket på sosial-kognitiv teori. Et av hans sentrale begreper er mestringsforventning (eng: self-efficacy) som knyttes til spesifikke kompetanser og ferdigheter. Ifølge hans forskning vil mestringsforventning påvirke prestasjon, ambisjoner og motivasjon.

Mestringsforventning er troen på at man er i stand til å kontrollere ens egen utførelse av bestemte oppgaver. Den grunnleggende forutsetningen i mestringsforventning er at atferd ikke bare er et samspill mellom stimuli (miljø) og respons (atferd), men at også de kognitive faktorene (person) samspiller med de to andre. Motivasjon er altså et samspill mellom atferd, person og miljø[26].

Atferd som resultat av et samspill mellom person og miljø i gjensidig påvirkning



Mestringsforventning handler om at man tror på at man er i stand til å organisere og utføre de handlinger som kreves for at man skal oppnå et ønsket resultat med de forutsetninger og evner man har. Vi forutsetter at den enkelte har som et mål å være trygg på nett. I dette målet ligger det at man skal unngå å bli utsatt for datakriminalitet, ID-tyveri, krenkelser, miste verdifulle data, ødeleggelse av digitalt utstyr, at digitale tjenester blir utilgjengelige og mye mer. Dette er langsiktige og generelle mål, som egentlig bare kan nås gjennom å sette seg kortere og mer konkrete mål. Mestringsforventningen til disse konkrete målene, eller oppgavene, vil da være avgjørende for om det langsiktige målet nås eller ikke.

Man snakker om to typer forventninger som har betydning for motivasjonen: *effektivitetsforventning og resultatforventning*. Effektivitetsforventning handler om troen på at man er i stand til å utføre en spesifikk handling (for eksempel å undersøke om en epost er trygg), mens resultatforventning handler om troen på at slike handlinger fører til ønsket resultat (at man gjennom å undersøke epostene blir tryggere i møtet med digitale farer).

Selv om det gjerne er en sammenheng mellom de to typene forventninger, trenger det ikke å være det:

Høy effektivitetsforventning og høy resultatforventning: Sterk motivasjon og høy produktivitet. Eksempel: Man er sikker på hvordan en tar backup av viktige dokumenter, og tror at det fører til at dokumentene ikke vil gå tapt ved et eventuelt løsepengevirus.

Høy effektivitetsforventning og lav resultatforventning: Typisk for en protestholdning. Eksempel: Men vet hvordan man skal holde datamaskinen oppdatert, men man tror ikke at det vil føre til at en selv eller andre blir mer sikker.

Lav effektivitetsforventning og høy resultatforventning: Selv-devaluering. Eksempel: Man tror at dersom man bare hadde gjort de riktige tingene så ville en vært trygge på nett, men en tror ikke at en får til å gjøre de spesifikke tingene som skal til.

Lav effektivitetsforventning og lav resultatforventning: Resignasjon. En vet ikke hva en skal gjøre, eller har noen tro på at det ville hjelpe uansett.

Personer med høy mestringsforventning, altså høy effektivitetsforventning og høy resultatforventning, har generelt et bedre utgangspunkt for å lykkes med digital sikkerhet, enn de som har en lav mestringsforventning. De som tilhører de to siste kategoriene har et dårlig utgangspunkt for å lykkes med digital sikkerhet. Sikkerhetsopplæring som ikke spesifikt adresserer deres lave mestringsforventning vil trolig ikke lykkes med å hjelpe denne gruppen til å utvikle en sikrere atferd i møte med det digitale.

For de som tilhører de to siste kategoriene er det mulig at feil sikkerhetsopplæring snarere kan redusere mestringsforventningen. Repeterende formaninger om aktiviteter man ikke vet hvordan man skal utføre, eller som man ikke tror har noen effekt, kan i verste fall føre til at mottakeren blir enda mindre motivert. Resultatet er paradoksalt: Mer sikkerhetsopplæring fører til mindre sikkerhet for noen.

Metode for kartlegging av mestringsforventning innen digital sikkerhet

Det finnes forslag til hvordan en kan bygge opp et datasett for mestringsforventning innen digital sikkerhet. Et av dem er *The Cybersecurity Engagement* and *Self-Efficacy Scale*[27], laget for å kartlegge slik mestringsforventning hos unge voksne.

Ettersom mestringsforventning knyttes til spesifikke aktiviteter, bør de som skal kartlegge dette tilpasse spørsmålssettene slik at de passer til aktivitetene. Det er publisert mye forskning omkring slike kartlegginger, som man kan bruke til inspirasjon og veiledning[28].

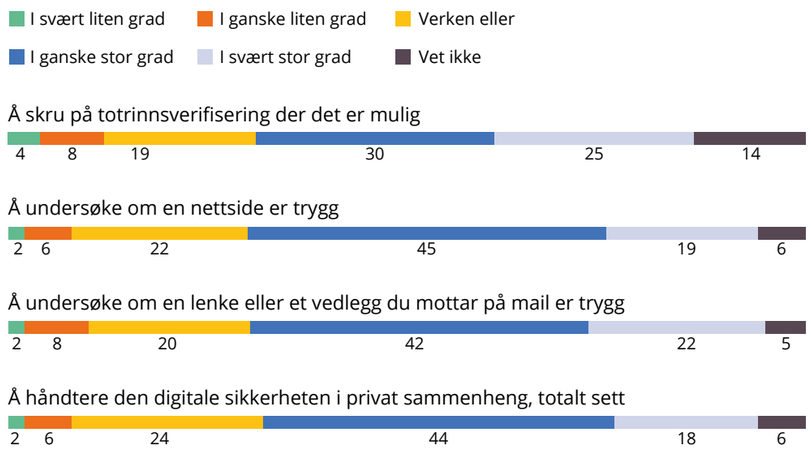
I årets undersøkelse har man økt fokuset på mestringsforventning i datainnsamlingen. Det er lagt til noen nye spørsmål, i tillegg til at deler av det eksisterende spørsmålssettet også kan brukes til å beskrive nordmenns mestringsforventning innen digital sikkerhet.

Metoden som er valgt har visse svakheter som man bør være oppmerksom på. For det første er spørsmålssettet ikke utelukkende innrettet med tanke på mestringsforventning, men på digital sikkerhetskultur som helhet. For å unngå at spørsmålssettet blir for omfattende, har man vært nødt til å inngå kompromisser der spørsmål som kunne vært stilt har blitt utelatt. For det andre har man ikke hatt fokus på å lage et spørsmålssett som kan avdekke *biaset sosial* ønskverdighet, altså at respondentene svarer det de tror at vi ønsker å høre.

Mestringsforventning innen digital sikkerhet i den norske befolkningen

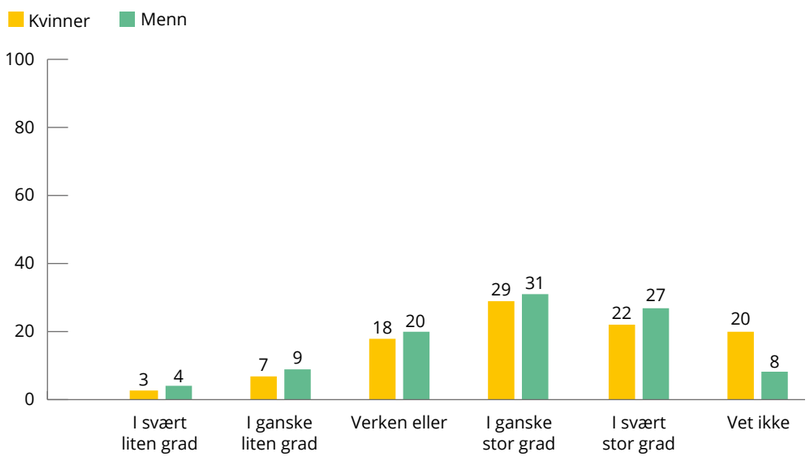
Respondentene er bedt om å ta stilling til i hvilken grad de mener at de vil klare å utføre noen av de mest sentrale aktivitetene som motvirker digitale trusler. Flertallet (64 %) av de spurte mener at de i svært stor eller ganske stor grad vil klare å utføre disse aktivitetene, og å håndtere den digitale sikkerheten privat, totalt sett. 8-12 % av respondentene mener at de i svært liten eller ganske liten grad vil klare å gjøre det.

I hvilken grad mener du at du vil klare å utføre sentrale aktiviteter innen digital sikkerhet? (Prosent)



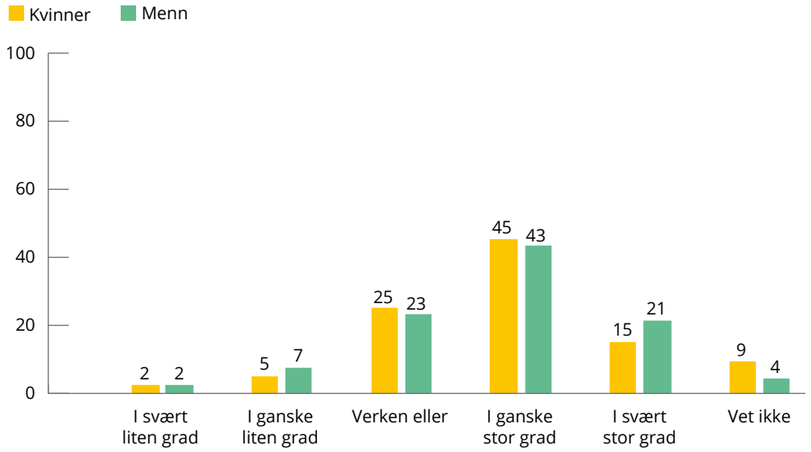
Det er enkelte kjønnsforskjeller. På spørsmålet om å skru på totrinnsverifisering oppgir flere menn at de i svært stor grad mener at de vil klare å gjøre dette. Samtidig oppgir flere kvinner at de ikke vet om de vil klare å gjøre det.

I hvilken grad mener du at du vil klare å skru på totrinnsverifisering der det er mulig? Kjønnsforskjeller. (Prosent)



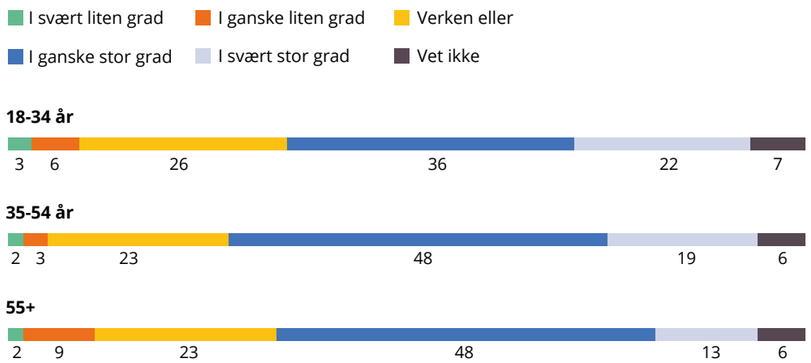
Det er videre en forskjell mellom kvinner og menn på spørsmålet om de vil klare å håndtere den digitale sikkerheten i privat sammenheng, totalt sett. Igjen oppgir flere menn at de i svært stor grad mener at de vil klare å gjøre dette, mens flere kvinner oppgir at de ikke vet om de vil klare det.

I hvilken grad mener du at du vil klare å håndtere den digitale sikkerheten i privat sammenheng, totalt sett? Kjønnsforskjeller. (Prosent)



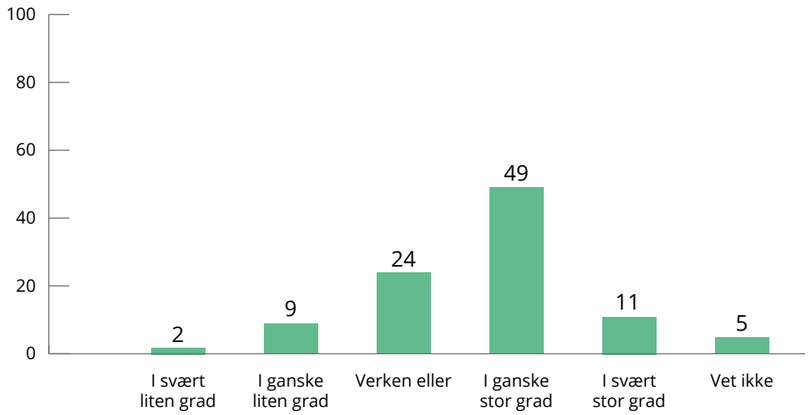
Det er også noen forskjeller mellom aldersgruppene, generelt at de yngre aldersgruppene i større grad oppgir at de mener at de vil klare å utføre aktivitetene.

I hvilken grad mener du at du vil klare å håndtere den digitale sikkerheten i privat sammenheng, totalt sett? Aldersforskjeller. (Prosent)



Å kunne vurdere hva som er trygt eller utrygt å gjøre på nett ligger i selve kjernen i det man omtaler som sikker atferd på nett. Dette omfatter både det å kunne vurdere om en lenke eller vedlegg er trygge å åpne, hvorvidt man skal dele andres innlegg, legge igjen betalingsinformasjon, laste ned apper, hvem man skal stole på og mye mer. I dette spørsmålet ligger det med andre ord omfattende og komplekse handlingsmønstre som i sum gjør den enkelte tryggere på nett. Forutsetningene for å kunne si at man er i stand til å vurdere dette omfatter både kunnskap om hvordan truslene kan arte seg, og kunnskap om de aktivitetene man må utføre for å undersøke de potensielle truslene.

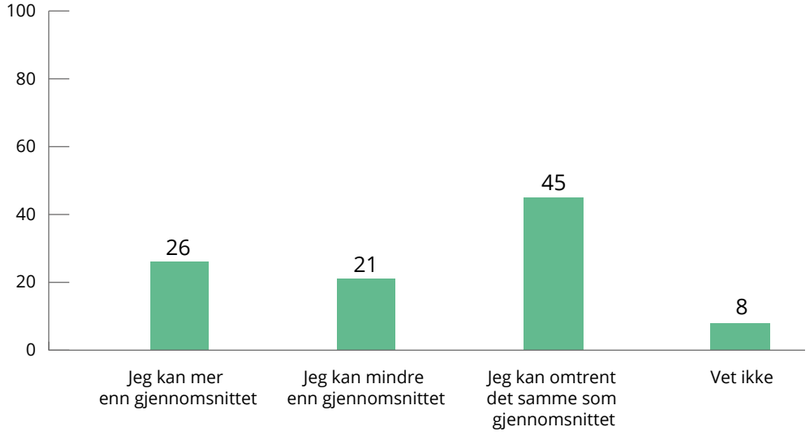
I hvilken grad er du i stand til å vurdere hva som er trygt eller utrygt å gjøre på nett? (Prosent)



60 % mener at de i ganske stor eller svært stor grad er i stand til å vurdere dette, mens 11 % mener at de i ganske liten eller svært liten grad er det.

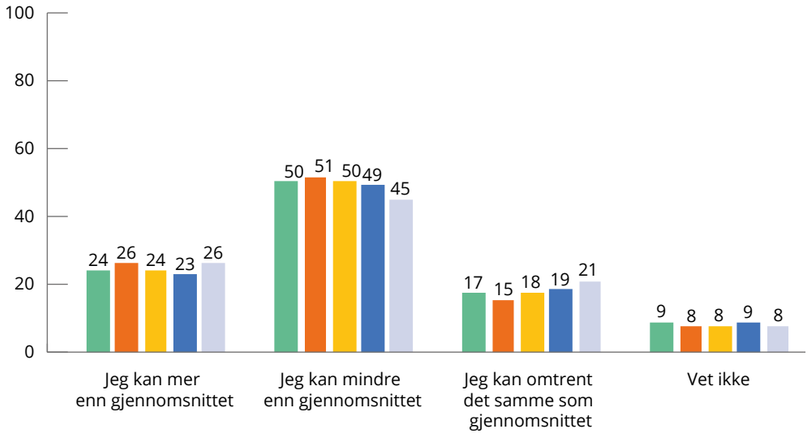
Respondentene bes om å vurdere egen kunnskap innen digital sikkerhet, relatert til befolkningen forøvrig. Det er lite trolig at den enkelte kan vite med sikkerhet om de kan mer eller mindre enn folk flest, men hensikten er å få frem hvordan de opplever sin egen kunnskap. Dersom man tror at de kan mer eller mindre om digital sikkerhet enn folk flest, kan dette påvirke deres mestringsforventning i henholdsvis positiv eller negativ retning.

Tror du at du kan mer eller mindre om informasjonssikkerhet i forhold til resten av befolkningen? (Prosent)



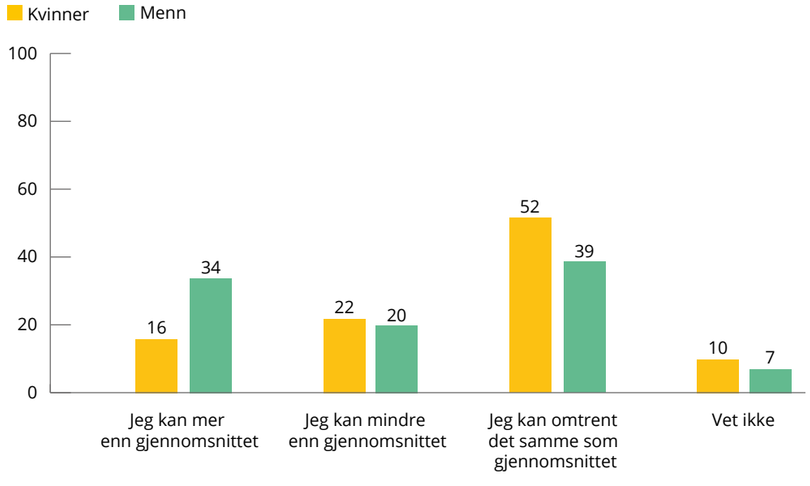
Nær halvparten av de spurte oppgir at de kan omtrent det samme som gjennomsnittet i befolkningen, mens 26 % mener at de kan mer enn gjennomsnittet. 21 % mener at de kan mindre enn folk flest.

Tror du at du kan mer eller mindre om informasjonssikkerhet i forhold til resten av befolkningen? (Prosent)



Dersom en betrakter dette spørsmålet over tid ser man at det ikke er signifikante endringer fra undersøkelsen i 2019, men det er en svakt stigende tendens til at flere uttrykker at de kan mindre enn folk flest.

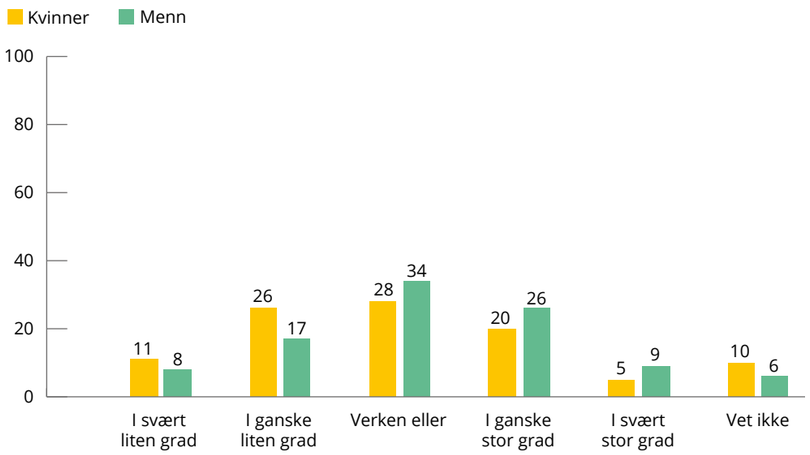
Tror du at du kan mer eller mindre om informasjonssikkerhet i forhold til resten av befolkningen? Kjønnsforskjeller. (Prosent)



Det er signifikante forskjeller mellom kvinner og menn i synet på dette. Langt fler menn oppgir at de kan mer om digital sikkerhet enn det kvinner gjør, og langt flere kvinner oppgir at de kan omtrent det samme som gjennomsnittet i befolkningen.

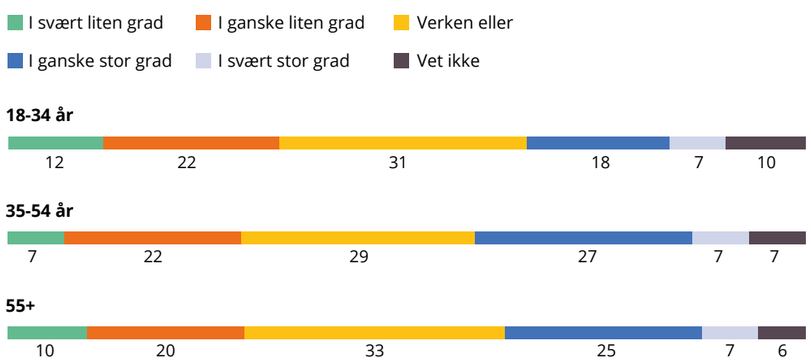
Hvorvidt man oppsøker informasjon som kan øke ferdighetsnivået innen digital sikkerhet kan sees på som en indikator for motivasjon og interesse. Også her observerer vi forskjeller mellom kvinner og menn. Flere kvinner oppgir at de i ganske liten eller svært liten grad oppsøker slik informasjon, mens flere menn oppgir at de i ganske stor eller svært stor grad gjør dette.

I hvilken grad oppsøker du selv informasjon som kan øke ditt ferdighetsnivå innen digital sikkerhet? Kjønnsforskjeller. (Prosent)



Det er noen aldersforskjeller her, primært at personer i aldersgruppen 35-54 i større grad oppsøker slik informasjon enn det personer i gruppen 18-34 gjør.

I hvilken grad oppsøker du selv informasjon som kan øke ditt ferdighetsnivå innen digital sikkerhet? Aldersforskjeller. (Prosent)



Vurdering og anbefaling

Det finnes en stor forskningskropp relatert til mestringsforventning, men langt mindre forskning på mestringsforventning innen digital sikkerhet. At tilbydere av opplæring innen digital sikkerhet foreløpig ikke har basert sin opplæring på forskning og teori omkring dette er derfor noe en må forvente. Den økende betydningen av det digitale og av digital sikkerhet i samfunnet, og det faktum at for mange nordmenn fremdeles utviser en usikker atferd på nett, krever imidlertid at tiden nå er inne for å evaluere opplæringsinnholdet og metodene. Norske sikkerhetsmyndigheter, sikkerhetsbransjen og sikkerhetsaktører bør i mye større grad ha fokus på mestringsforventning i sikkerhetsopplæringen. De som tilbyr sikkerhetsopplæring innen digital sikkerhet bør videre kartlegge den digitale mestringsforventningen for å dokumentere at deres opplæring har en positiv effekt på denne.

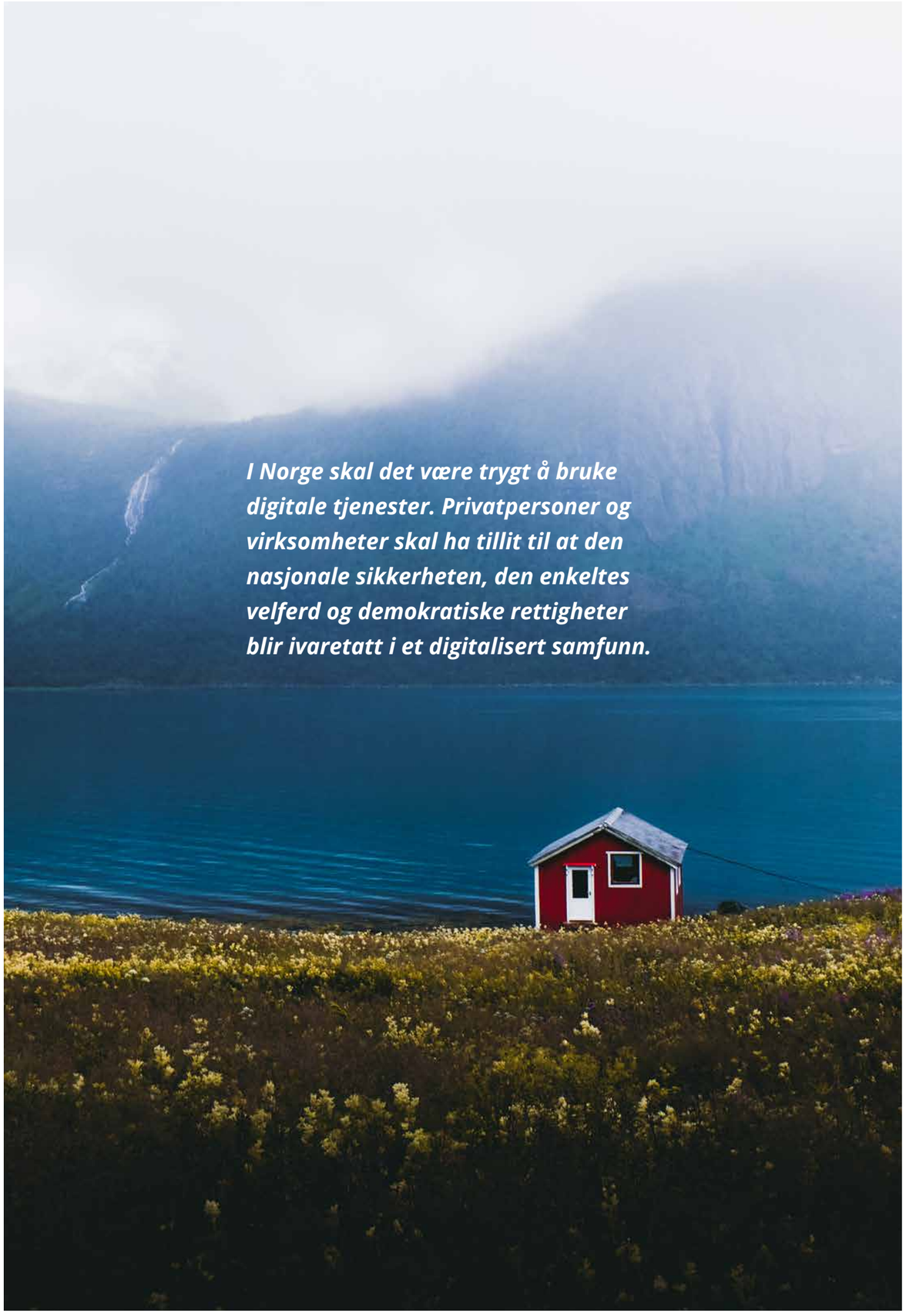
God sikkerhetsopplæring, det vil si sikkerhetsopplæring som også øker mottakerens mestringsforventning, kan basere seg på følgende[29]:

Egen tidligere erfaring med å mestre aktiviteten. Å huske tidligere forsøk på å mestre aktiviteten er en god indikator på å mestre fremtidige oppgaver. Tidligere mestringsforsøk kan bestå av varierende grad av suksess, og den viktigste faktoren som bestemmer mestringsforventningen er den erfaringen man har med å lykkes. Opplæringen kan derfor med fordel være lagt opp med en viss progresjon i vanskelighetsgrad, og slik at nye aktiviteter og ferdigheter bygger på det som deltakeren allerede har vist at de behersker og at undervisningen minner om dette.

Vikarierende erfaring i form av modellæring (observere andre som utfører aktiviteten). Når en ikke selv har erfaring med aktiviteten, kan det å observere andre som utfører den øke mestringsforventningen. Spesielt dersom en identifiserer seg med den som observeres. Opplæring kan for eksempel inneholde video og animasjonsmateriale som viser hvordan aktivitetene skal utføres, eller at noen i samme «gruppe» som deltakeren demonstrerer det.

Verbal overtalelse (Peptalk som formidler at «dette kan du utføre»). Å bli fortalt at dette er noe en vil klare å gjennomføre, kan endre oppmerksomheten fra hjelpeløshet til mestring. I stedet for å bare gi opp, gjør et forsøk på å mestre. Dette vil derimot ikke fungere dersom de personlige mestringserfaringene står i motstrid til overtalelsen. Hvis man selv har erfart at man ikke klarer å utføre aktiviteten, hjelper det ikke at andre sier «dette klarer du».

Fysiologisk aktivering (for eksempel økt hjerterate). Kroppslige spenninger, økt hjerterate og skjelvende hender kan forsterke en opplevelse av manglende mestring. Dette kan gjerne få en betydning når man skal testes i digital sikkerhet ved endt undervisning. Opplæring og tester bør gjennomføres i omgivelser som ikke stresser deltakeren.



OPPSUMMERING

Årets undersøkelse bekrefter konklusjonen fra tidligere års undersøkelser: den positive utviklingen for flere av de sentrale indikatorene på sikker digital adferd enten uteblir eller er veldig svak.

Digital sikkerhetskultur dannes ofte innen rammen av sikkerhetsopplæring, og det er helt nødvendig å være tydelig på hva en ønsker å oppnå med slik opplæring. Det er ofte ikke kunnskapen i seg selv som er det viktige, men at de som får opplæring settes i stand til å utvikle normer, holdninger og atferd som fører til at de er tryggere i møtet med digitale trusler. Det er selvsagt ikke slik at all sikkerhetsopplæring er uegnet til å nå disse målene, men når den ønskede effekten uteblir bør man evaluere om tilnærmingen er hensiktsmessig eller om det finnes andre tilnærminger som kan bidra til at målene nås. Denne rapporten har derfor sett til motivasjonspsykologi og hvordan mestringsforventning er en helt sentral kognitiv faktor når det kommer til atferd og atferdsendring, også innen digital sikkerhet.

De som tilbyr opplæring i digital sikkerhet bør arbeide målrettet med mestringsforventning og på den måten øke mulighetene for at de som mottar opplæringen utvikler en sikrere atferd. Det oppfordres også til at man i større grad kartlegger mestringsforventning, enten det er snakk om sikkerhetsmyndighetene, aktører som tilbyr opplæring i digital sikkerhet eller virksomheter som benytter seg av slik opplæring. Resultatene bør publiseres fritt slik at vi alle kan utvikle mer kunnskap om hvordan vi effektivt kan arbeide med mestringsforventning innen digital sikkerhet, og slik at vi kan strekke oss mot visjonen i Nasjonal strategi for digital sikkerhet:

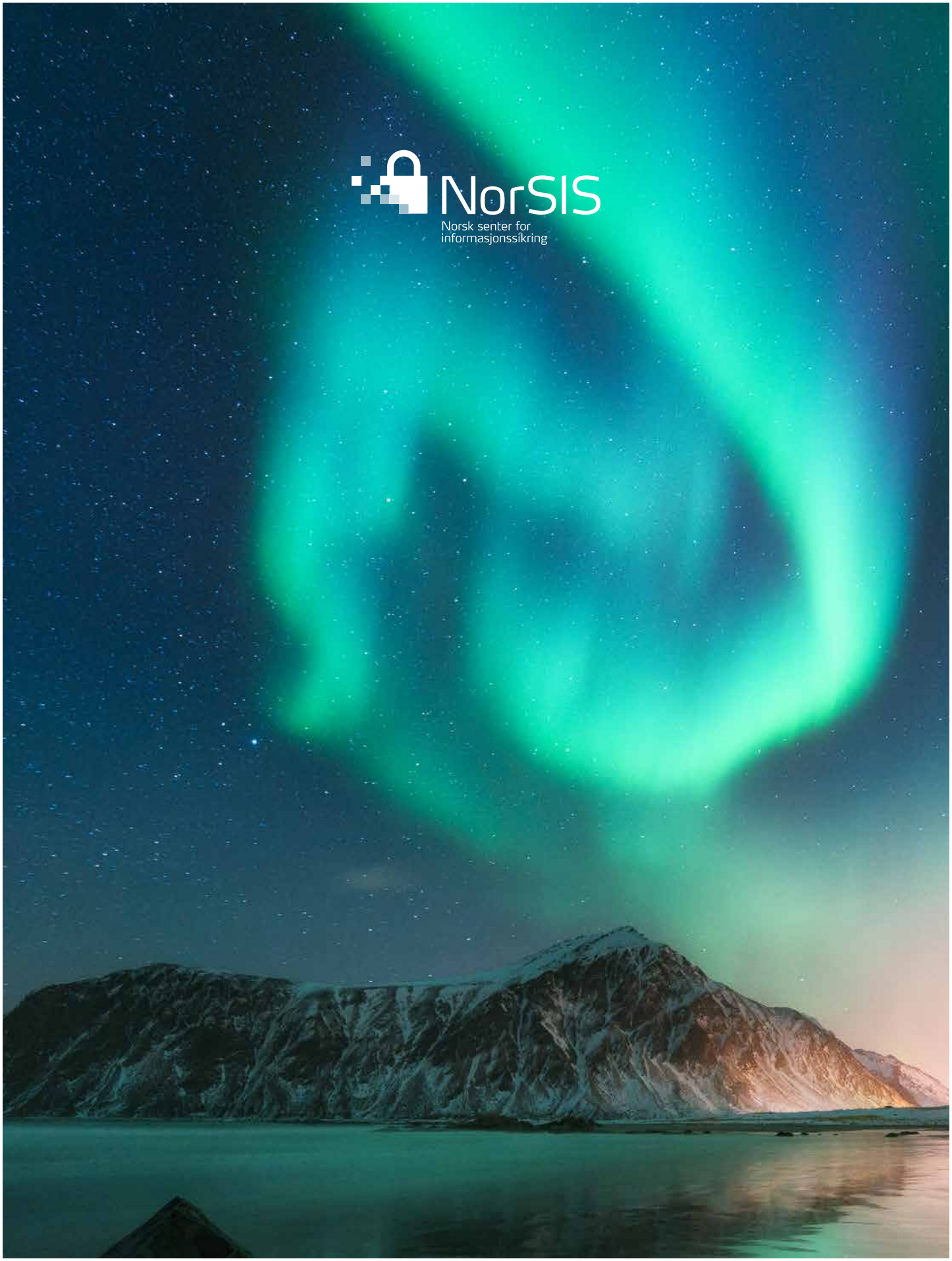
I Norge skal det være trygt å bruke digitale tjenester. Privatpersoner og virksomheter skal ha tillit til at den nasjonale sikkerheten, den enkeltes velferd og demokratiske rettigheter blir ivaretatt i et digitalisert samfunn.

Årets undersøkelse er den første der NorSIS aktivt samler inn data om mestringsforventning, og det er behov for å bygge opp et datagrunnlag over tid før man kan vurdere om utviklingen går i riktig retning. Det konkluderes derfor ikke om mestringsforventningen er lav eller høy i befolkningen, siden man ikke har etablert en referanse for slike vurderinger.

Denne rapporten går også inn på noen av effektene som Covid-19 har hatt på befolkningens holdninger til digital risiko. Det er interessant at de fleste mener at den digitale risikoen i samfunnet har økt, bare ikke for dem selv. Spørreundersøkelsen ble gjennomført ganske tidlig etter at myndighetene innførte de strenge tiltakene, så en bør kartlegge igjen om noe tid for å avdekke hva langtidseffektene er. Det er likevel både nyttig og interessant å se hvordan store samfunnshendelser påvirker våre holdninger og syn på digital sikkerhetskultur. Denne kunnskapen må vi bruke til å bedre forstå hva som påvirker samfunnets normer og holdninger innen digital sikkerhet, og til å utvikle bedre metoder for å påvirke disse i den retningen vi ønsker.

FOTNOTER

[1] Computer Assisted Web Interview
[2] https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf
[3] Gelfand, M. (2018). Rule Makers, Rule Breakers: How tight and loose cultures wire our world. Scribner. ISBN 978-1-5011-5293-1
[4] https://en.wikipedia.org/wiki/Social_desirability_bias
[5] https://www.nrk.no/norge/kripos-sokte-med-bilder-fra-norske-etterforskninger-i-omstridt-app-1.14935430
[6] Chauvin B, Hermand D, Mullet E. Risk perception and personality facets. Risk Anal. 2007;27(1):171-185. doi:10.1111/j.1539-6924.2006.00867.x
[7] Regjeringens digitaliseringsstrategi: https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/digitaliseringsstrategi-for-offentlig-sektor/id2612415/
[8] https://nsm.no/aktuelt/mer-hjemmekontor-store-muligheter-men-ogsa-risikoer
[9] https://nettvett.no/korona/
[10] https://www.telenor.no/bedrift/sikkerhet/hjemmekontor/
[11] https://www.interpol.int/News-and-Events/News/2020/Unmasked-International-COVID-19-fraud-exposed
[12] https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know
[13] https://www.who.int/about/communications/cyber-security
[14] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains
[15] https://www.computerweekly.com/news/252480238/Coronavirus-now-possibly-largest-ever-cyber-security-threat
[16] https://www.wired.com/story/coronavirus-cyberattacks-ransomware-phishing/
[17] https://economictimes.indiatimes.com/tech/internet/dont-use-these-websites-for-any-coronavirus-related-updates/articleshow/74827689.cms?from=mdr
[18] https://press.nordicopenaccess.no/index.php/noasp/catalog/view/45/213/1920-1
[19] https://en.wikipedia.org/wiki/Optimism_bias
[20] https://www.digi.no/artikler/kommentar-nar-norske-sikkerhetsmyndigheter-foreskriver-skippertak-som-metode-i-2019/475347
[21] https://www.digi.no/artikler/kommentar-en-sikkerhetsmaned-til-besvaer/474854
[22] Diseth, Åge. (2019). Motivasjonspsykologi – Hvordan behov, tanker og emosjoner fremmer prestasjoner og mestring. Gyldendal Norsk Forlag. ISBN 987-82-05-51711-0
[23] Ibid. S.18
[24] https://no.wikipedia.org/wiki/Spillifisering
[25] https://snl.no/Albert_Bandura
[26] Diseth, Åge. (2019). Motivasjonspsykologi – Hvordan behov, tanker og emosjoner fremmer prestasjoner og mestring. s.143
[27] Amo, L.C., Zhuo, M., Wilde, S., Murray, D., Cleary, K., Amo, C., Upadhyaya, S., Rao, H.R. (2015). Cybersecurity Engagement and Self-Efficacy Scale. Ikke publisert.
[28] https://positivepsychology.com/self-efficacy-scales/
[29] Ibid s.146



Teknologiveien 22
2815 Gjøvik
Org.nr. 995195003

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