NorSIS
Norsk senter for informasjonssikring

Ungdom og digital sikkerhetskultur

Ungdom og digital sikkerhetskultur

Ansvarlig: Peggy Heie Sandbekken
Forfattere: Bjarte Malmedal og Hanne Eggen Røislien
Layout og foto: Maria Nyheim

Rapporten er støttet av Senter for IKT i utdanningen

Innhold

Innledning

NorSIS publiserte i 2016 en rapport om den norske informasjonssikkerhetskulturen. Forut for dette tildelte Justis- og beredskapsdepartementet midler til å utvikle en metode for kartlegging av sikkerhetskultur på et nasjonalt nivå. I vår datainnsamling la vi vekt på å samle inn data fra ulike sektorer og grupper i samfunnet, for å lære mest mulig om hvordan disse forholder seg til informasjonssikkerhet i en digital hverdag. En slik gruppe er ungdom, og i denne studien omfatter det de som er under 20 år.

Ungdom er en gruppe som opptar NorSIS. Erfaringene våre fra tjenesten Slettmeg.no viser at ungdom ofte havner i situasjoner som god praksis innen informasjonssikkerhet, eller bevissthet omkring risiko og konsekvenser, kunne forhindret. Det er også en gruppe vi mener har dårlige forutsetninger for å utvikle

gode sikkerhetsvaner. Vi gjorde funn i vår studie fra 2016 som antydet at alder er en signifikant faktor for store deler av det vi beskriver som informasjonssikkerhetskultur. Merk at vi behandler begrepene informasjonssikkerhetskultur og digital sikkerhetskultur som synonymer i denne studien.

Vi er derfor svært tilfreds med at Senter for IKT i utdanningen deler vår interesse for å utvikle mer kunnskap om nettopp denne gruppen, og for deres støtte til denne rapporten.

Direktør NorSIS

Digitale medier og plattformer er en stor og naturlig del av de unges liv. Ungdom er vokst opp som digitale innbyggere og benytter internett og digitale verktøy og hjelpemidler. De er vant med og kjent med digitale flater. Digitale medier er med å påvirke de unges holdninger, syn på samfunnet og verden i sin helhet.

Ungdom skiller ikke i dag mellom digital og fysisk verden, slik eldre generasjoner har en tendens til å gjøre. Historisk sett er digital teknologi umodent for oss mennesker. Datakraften i smarttelefonen er formidabel, den første romfergen hadde mindre datakraft enn smarttelefonene som har blitt allemannseie. De færreste av foreldregenerasjonen til dagens unge har vokst opp i en digital tidsalder. Foreldre og skole har imidlertid et ansvar for å lære de unge etikk og sikker bruk av digital teknologi. For å kunne gjøre dette må foreldre, skole og samfunnet generelt ha kompetanse til å overføre digitale verdier til den oppvoksende generasjonen. Vi er forskjellige som

individer, dette gjelder også de unge, noen er forsiktige, andre tester grenser. For oss foreldre er det en kjent sak at ungdom vil teste grenser, de skal frigjøre seg fra oss voksne og bli selvstendige og trygge mennesker. Vi voksne har et ansvar for å skape trygge rammer for de unge på nett. For å kunne være gode rollemodeller må man vite hvordan og hvilke verdier og normer man overfører til den oppvoksende generasjonen.

Tidligere forskning har vist at barn og unge sitter mye alene med digitale medier, uten en voksen til å veilede seg. Det er imidlertid mye antagelser om de unges bruk av digitale medier. Det er viktig med innsikt og derfor har vi utarbeidet en rapport i samarbeid med Senter for IKT i utdanningen slik at fakta og kunnskap kan benyttes i arbeidet med å trygge de unges digitale hverdag.

Peggy Sandbekken Heie
Administrerende direktør
NorSIS

Behovet for å kartlegge informasjonssikkerhets-kultur blant ungdom

Det norske samfunnet går gjennom en omfattende og hurtig digitalisering i både privat og offentlig sektor. Produksjon, produkter og tjenester blir digitalisert, og dette fører til at digitaliseringen knyttes enda sterkere til vekst i den nasjonale økonomien. I følge World Economic Forum sin rapport *Global Information Technology Report* (2013)[1], vil nasjoner som allerede er høyt digitalisert oppleve en større effekt av ytterligere digitalisering. En økning i digitaliseringsgrad på 10 % kan medføre en 0.75 % økning i BNP per innbygger. I følge rapporten er Norge den femte mest digitaliserte nasjonen i verden, og har dermed et potensiale til å oppleve en økning på 24 milliarder kroner[2] per år som en følge av en slik økning i digitaliseringsgrad. På samme tid koster datakriminalitet det norske samfunnet enorme summer hvert år. I følge *Mørketallsundersøkelsen 2014*[3], kan disse tapene beløpe seg til hele 19 milliarder kroner per år.

1: http://www3.weforum.org/docs/WEF_GITR_Report_2013.pdf

2: Estimat 2014

3: *Mørketallsundersøkelsen*, The Norwegian Business and Industry Security Council (NSR)

Dette tegner et dystert bilde. Digitaliseringen har et potensiale til å skape økonomisk vekst, og velferd, gjennom nasjonal og internasjonal handel, og mer effektive offentlige tjenester. Dette potensialet blir imidlertid nærmest spist opp av tapene datakriminalitet fører til. Når vi også tar i betraktning at fremmede stater stjeler norsk teknologi, forskning og utvikling betyr det at våre fremtidige inntektskilder står i fare for å bli kraftig redusert.

Dette er imidlertid ikke bare et spørsmål om økonomi. Teknologi, IT og digitale tjenester er en uatskillelig del av alle nordmenns liv. Vi er avhengige av at både enkeltpersoner, og samfunnet som helhet, er motstandsdyktige mot de nye farene som truer på nettet. Det er også slik at vi ikke kan skape et trygt digitalt rom kun ved hjelp av teknologi. Alle nordmenn, voksne som barn, må forholde seg til et samfunn som er drevet av en rask teknologisk utvikling, med et trussel-landskap som er i konstant endring. Hvordan hver enkelt oppfatter risiko, og våre holdninger og kunnskaper om hvordan vi kan beskytte oss selv, vil påvirke hvordan digitaliseringen skjer. I verste fall kan vi få en utvikling der vi, som samfunn, er lite villig til å ta i bruk mulighetene som digitaliseringen gir. En befolkning som frykter digitale handelsløsninger, vil unngå dem[4]. Hvis vi ikke stoler på at myndighetene vil behandle vår informasjon på en sikker måte, vil vi motsette oss digitalisering i det offentlige. Hvis vi ikke stoler på hverandre, kan det bety at vi legger bånd på oss i måten vi bruker digitale tjenester i våre sosiale liv.

4: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

Vi blir bombardert med historier om at alt har, kan og vil gå galt, men er vi egentlig i stand til å forstå hva som er den faktiske risikoen til enhver tid, eller for enhver digital tjeneste? Vi frykter at vi som nasjon skal trå feil. At vi, med bakgrunn i frykt, skal overkompensere med sikkerhetstiltak som fører til en nedkjølingseffekt for digitaliseringen, eller at vi lar være å innføre sikkerhetstiltak fordi vi ikke forstår hvor stor risikoen er.

Med andre ord; Vi har behov for å lære mer om informasjonssikkerhetskulturen i samfunnet vårt. NorSIS gjennomførte et prosjekt i 2016 der det ble utviklet en ny metode for å kartlegge informasjonssikkerhetskultur på et nasjonalt nivå. Resultatene ble publisert i rapporten[5] *«The Norwegian Cybersecurity Culture»* i 2016. Rapporten beskriver informasjonssikkerhetskulturen for nasjonen som helhet, men det er åpenbart at ulike grupper i samfunnet har ulike utfordringer og muligheter. En slik gruppe er barn og unge. I motsetning til mange av dagens voksne, har denne gruppen vokst opp omgitt av IT og digitale tjenester. Men; de har også vokst opp med en foreldregenerasjon som trolig ikke har hatt mulighet til å bidra nok med det vi kan kalle «digital oppdragelse». Mye er derfor overlatt til skolen, og ikke minst til de unge selv.

5: https://norsis.no/den-norske-informasjonssikkerhetskulturen/

Hvilken informasjonssikkerhetskultur som er fremtredende blant ungdom er av særlig stor interesse, fordi vi antar at store deler av menneskers holdnings- og verdigrunnlag dannes i ung alder. Disse følger enkeltmennesket videre, og tas med inn i arbeidslivet etterhvert.

Norske myndigheter arbeider kontinuerlig med å utvikle sine strategier for informasjonssikkerhet, og et av de strategiske målene er å styrke utdanning innen dette området. Å forstå mest mulig om informasjonssikkerhetskulturen for ungdom er derfor en forutsetning for å utvikle en god utdanningspolitikk og en digital trygghet for de unge i samfunnet.

Kartlegging av informasjons-sikkerhetskultur

Å lage en metode for å kartlegge informasjons-sikkerhetskultur er utfordrende. I dette kapitlet ser vi nærmere på hvilke utfordringer som ligger i det å kartlegge kultur, og vi presenterer vår tilnærming til det å lage en metrikk for informasjonssikkerhetskultur på et nasjonalt nivå.

Utfordringene med å måle kultur

Hovedutfordringen med å måle informasjons-sikkerhetskultur er i selve konseptet. Hvordan konseptet har oppstått, og hvordan det blir anvendt i det daglige, har gjort det utfordrende å betrakte det i ulike deler av samfunnet. Årsaken er tilsynelatende enkel. *Informasjonssikkerhetskultur* er et konsept som først og fremst er utviklet og brukt i deler av næringslivet, av personer som har dette som

sin fag-ekspertise. Med andre ord, informasjonssikkerhetskultur er et begrep som er utviklet av virksomheter som allerede vet mye om hva informasjonssikkerhet er. Dette gjenspeiler ikke næringslivet som helhet, og i særdeleshet ikke hele det norske samfunnet.

Når en skal lage en metrikk for informasjonssikkerhetskultur er det flere utfordringer som må adresseres. En utfordring er spørsmålet om terminologi, altså hva vi faktisk mener når vi refererer til *informasjonssikkerhetskultur*. En annen er hvilke nivåer vi skal anvende begrepet på, altså om konseptet informasjonssikkerhetskultur er gyldig både på bedriftsnivå og på et nasjonalt nivå. Selv om konseptet er utviklet i bedrifter, har vi også «nasjonale» informasjonssikkerhetskulturer. Imidlertid blir ikke disse uttrykt og diskutert på samme vis. For eksempel; Bedrifter, virksomheter og organisasjoner har en tydelig definert hensikt, mens vi sjelden snakker om «hensikten» til en nasjon. Bedrifter kan aktivt lære opp sine ansatte og sette krav til kunnskap og atferd. Spørsmålet er da om det er mulig å utvikle en generell forståelse for begrepet informasjonssikkerhetskultur, som er like anvendbart i bedrifter og for nasjoner?

Begrepet *informasjonssikkerhetskultur* er ikke nytt, og det mangler ikke på forsøk på å måle det. Selv om det ikke eksisterer en entydig forståelse av hva begrepet inneholder, brukes det vanligvis til å beskrive «noe som har med atferd å gjøre». Med andre ord, informasjonssikkerhetskultur er vanligvis knyttet til de sikkerhetsatferden til ansatte i norske bedrifter. Dette er relativt enkelt å måle, og det er vanlig at man måler enkelte atferds-trekk, og ekstrapolerer funnene. Spørsmålet er om dette egentlig sier noe om kultur. Er prosentandelen som trykker på en phishing-lenke en gyldig indikator for bevissthet og kunnskap omkring informasjonssikkerhet? Eller kan det like gjerne være et resultat av ressursene og kunnskapen til den som angriper? Enda viktigere; slike studier forklarer ikke hvordan bevissthet og holdninger utvikles, og hvordan våre verdigrunnlag påvirker det vi tenker om informasjonssikkerhet spesielt og teknologi generelt, eller hvilken rolle vår interesse for teknologi påvirker oss når vi må forholde oss til en utrygg digital hverdag.

Informasjonssikkerhetskultur som verktøy

Informasjonssikkerhetskultur er et konsept som får stadig større oppmerksomhet. Både fageksperter og virksomheter som spesialiserer seg innen informasjonssikkerhet er tydelige på at de tekniske fremskrittene alene ikke kan skape et trygt digitalt rom. Det virker åpenbart at tekniske sikkerhetsløsninger ikke vil kunne forhindre ethvert sikkerhetsbrudd. De menneskelige faktorene påvirker hvordan enkeltmennesket forholder seg til informasjonssikkerhetsteknologi, og dette forholdet er ofte i motstrid til sikkerhetsbehovene.

Virksomhetene har lenge vært klar over at deres interne kultur har innvirkning på resultatene. Det er kulturen i organisasjonen som får frem det beste i hver enkelt. Kultur utvikler vaner hos enkeltmennesket som gjør dem suksessfulle på arbeidsplassen. Når det kommer til informasjonssikkerhetskultur, og dens innvirkning på digital sikkerhet, er det imidlertid tydelig at modenheten i organisasjonen er lav. Informasjonssikkerhetskultur blir i hovedsak betraktet på to måter:

For det første blir det sett på som et verktøy innen mål- og resultatstyring. For det andre blir det sett på som en sum av handlinger, altså slik de ansatte oppfører seg. Dette betyr at informasjonssikkerhetskultur av mange blir sett på som normative atferdsmønstre som kan endres og forbedres for å oppnå bedre resultater i en organisasjon. Et tydelig tegn på dette er at mange diskuterer hvorvidt informasjonssikkerhetskulturen i en organisasjon er «god» eller «dårlig». Dette gir helt tydelige normative overtoner som indikerer at informasjonssikkerhetskultur er et verktøy, og at det er noe som kan testes, måles og forbedres. Denne tilnærmingen leder oss til et sentralt spørsmål: Er kultur reduserbart til handlinger? Er det kun et verktøy for mål- og resultatstyring i virksomheter? I så fall er det fristende å spørre om kultur-begrepet brukes feil, og at man heller burde omtale det som kjøreregler (Code of Conduct).

Kultur blir ikke redusert til et sett av handlinger i noen andre kontekster.

Innen humanistiske fag er kultur-begrepet langt mer komplekst enn som så, og det brukes sjeldent normativt. Kultur blir betraktet gjennom de underliggende idéene, verdiene og holdningene som fører til handlingene. Kultur er ikke et verktøy; Kultur plasserer den enkelte i samfunnet, og påvirker hvordan vi betrakter verden. Med andre ord, verdier og holdninger kommer til uttrykk gjennom handlinger og atferdsmønstre.

En helhetlig tilnærming til informasjonssikkerhetsultur

Det er tilsynelatende motstridende syn på hvordan vi skal forstå informasjonssikkerhetskultur mellom fag-ekspertise innen informasjonssikkerhet og innen humanistiske fag. Dette bør ikke kommer som en overraskelse, for til nå har informasjonssikkerhet og kultur vært adskilte disipliner. Den delen av akademia som har arbeidet med kultur, har i liten grad vært involvert i informasjonssikkerhet. Og omvendt. Vi tror at

en helhetlig og felles tilnærming bidrar til å utvikle et språk og en diskusjon som begge fagdisiplinene kan delta i.

Vi mener at en metode for kartlegging av informasjonssikkerhetskultur vil ha nytte av en mer helhetlig tilnærming der vi tar et steg tilbake fra enkel kartlegging av phishing-eposter, og heller fokuserer på holdninger og perspektiver knyttet til et sikkert digitalt rom, og hvordan disse henger sammen med ens verdigrunnlag, interesser, kunnskaper og adferd.

Metode

Informasjonssikkerhetskultur er et komplekst område, og mekanismene som påvirker den er drøftet i hovedstudien.

Å utvikle et sett med indikatorer som skal være robuste nok til å kunne brukes i ulike samfunnsgrupper, i alle generasjoner, i alle virksomheter og alle utdanningsnivåer er svært krevende. Indikatorene som ble utviklet i hovedstudien ble kvalitetssikret gjennom en omfattende pilotstudie og gjennom referansegruppens vurderinger.

Metoden er ytterligere beskrevet i hovedstudiens rapport.

Forskningsspørsmål

Hovedstudien fokuserer på informasjonssikkerhetskultur på et nasjonalt nivå. Enkeltfunn i hovedstudien tyder på at alder er en faktor som har betydning. Med bakgrunn i dette formuleres følgende forskningsspørsmål:

- Hvordan kan informasjonssikkerhetskulturen blant unge karakteriseres?
- I hvilken grad er det sammenheng mellom utdanning i informasjonssikkehet for unge og deres sikkerhetsatferd og bevissthet?
- Hvilke digitale trusler er unge mest bekymret for?
- I hvilken grad tar unge et ansvar for sikkerhet og trygghet for det digitale rom?

Indikatorer på informasjonssikkerhetskultur

Indikatorene for informasjonssikkerhetskultur er utviklet som en del av hovedstudien. De ble utformet som et elektronisk spørreskjema på norsk og engelsk. Noen av bakgrunnsvariablene er tilpasset deltakerne utenfor Norge.

Indikatorene er gjengitt i vedlegg A.

Demografi

Totalt er undersøkelsen sendt til ca. 150.000 personer, og det er samlet inn 14.000 svar inklusiv pilotundersøkelsen. I hovedundersøkelsen ble ca. 8.200 svar lagt til grunn for analysene.

Det ble samlet inn data fra ungdommer på tilsammen 5 skoler i hovedstudien. En skole i Østfold, og fire skoler i Oslo. Denne rapporten er basert på datagrunnlaget fra de fem skolene, i tillegg til et mindre antall ungdom fordelt på de øvrige undersøkelsene som ble gjennomført i hovedstudien. Deltakelse er 772 unge under 20 år. Svarprosent er ukjent.

Dette gir ikke nødvendigvis et representativt utvalg fra hele skole-norge, fordi det kan være forskjeller mellom skoler og geografiske forskjeller mellom kommuner og fylker.

Datagrunnlaget er egnet til å si noe om sikkerhetskultur blant ungdom, men det er viktig å samtidig være klar over at det ikke er metodisk grunnlag for å fastslå at resultatene er gyldige for norske ungdommer generelt. Når vi i denne rapporten bruker begreper som «ungdommene» henviser vi til de som har respondert på vår undersøkelse.

Kjønns- og aldersfordelingen er som følger:

Kjønn	#	%
Kvinner	407	52,7
Menn	365	47,3
n=	772	

Alder	#	%
Under 15	144	18,7
15–19	628	81,3
n=	772	

Utvalg	#	%
Skole	708	91,7
Andre virksomheter	64	8,3
n=	772	

Analyse

Det er gjennomgående benyttet gjennomsnitt som sentraltendens i analysene. Variablene er stort sett nominale eller ordinale med få responskategorier (færre enn fem). Signifikans i forskjeller mellom grupper er vurdert med chi-kvadrattesten ($\chi 2$). Det er oppgitt effektsstørrelser knyttet til figurene, her er Cramérs V benyttet. Vurdering av størrelsen av effektene er gjort slik: 0,10–0,30 (liten), 0,30–0,50 (moderat) og >0,50 (stor).

Informasjonssikkerhet og informasjonssikkerhets-kultur i skolen

I tillegg til at skolen er et sted elevene kan lære om informasjonssikkerhet som innhold i fag, er skolen også den organisasjonen barn og unge har mest erfaringer med. Slik sett er praksis ved skolene relevant for de unges dannelse av informasjonssikkerhetskultur. Man kan da spørre seg om hvordan skolen er som «rollemodell» for elevene.

I undersøkelsen *Monitor skole 2016* vurderer skoleledere forhold ved informasjonssikkerhet på sin skole. 40 % mener at utsagnet «Skolen har gode rutiner for registrering, bruk, tilgang, lagring og sletting av personopplysninger» passer helt. Ytterligere 40 % mener at utsagnet passer delvis for sin skole, men delvis oppfyllelse av disse rutinene er ikke tilfredsstillende. Det er også et betydelig antall skoler som ikke har informasjonssikkerhet med i sitt planmessige arbeid med IKT. 35 % av skolelederne i

undersøkelsen mener at utsagnet «Personvern, trygg bruk og sikring av data og informasjon er temaer i skolens planverk» ikke passer, eller passer litt.

Undersøkelsen om skolens digitale tilstand, *Monitor skole 2016*[6], fremhever to forhold ved elevers forhold til informasjonssikkerhet som problematiske. Omtrent 30 % av 7.-klassingene har benytter lærerens datamaskin, som medfører risiko for at sensitiv informasjon kan komme på avveie. Det er også slik at over 40 % av elevene i undersøkelsen oppgir at deres foresatte har tilgang til deres brukerkonto på læringsplattformen, mens 28 % oppgir at de ikke vet. Dette er ikke en ønskelig praksis.

Datatilsynet har undersøkt bruk og lagring av personopplysninger i skolen. Undersøkelsen[7], gjennomført i 2013 og 2014, konkluderer med at det er til dels store utfordringene for personvernet i skolen. Informasjonssikkerhet er en del av dette bildet. Datatilsynet avdekket at det lagres store mengder opplysninger om barnehagebarn og elever. Opplysninger om orden, oppførsel, adferd, karakterer og språkutvikling er noen eksempler. Det finnes også verktøy som gjør det mulig å logge hvilke nettsteder elevene har besøkt i skoletiden eller som logger når og hvor lenge elevene jobber med spesifikke oppgaver.

Datatilsynets undersøkelser viser at foresatte og elever ikke får god nok informasjon om hvilke opplysninger som lagres, hva de skal brukes til og hvor lenge de skal lagres. De mener at mye av årsaken til det, er at de ansvarlige ikke har god nok kunnskap og kompetanse om dette selv. De vet ikke engang alltid hvem som er ansvarlig for hva.

Medietilsynets undersøkelse *Barn og medier 2016*[8] viser at skolen er en viktig arena for å lære om trygg og sikker bruk av medier. I aldersgruppen 9–16 år svarer 78 % at de har lært om dette på skolen, fulgt av mamma (61 %) og pappa (54 %). Undersøkelsen viser også en tydelig økning i andelen barn som har lært om slik trygg og sikker bruk av nett, mobil og spill på skolen. Blant barn i alderen 9–11 år har 70 prosent av barna i 2016 lært om dette på skolen, mot 52 prosent av barn i samme alder i 2012. Blant barna i alderen 12–14 år har 85 prosent lært om trygg og sikker bruk på skolen, sammenlignet med 66 prosent i 2012 og 61 prosent i 2014.

Fra sårbarhetsutvalgets NOU, *Digital sårbarhet – sikkert samfunn*[9]: «Utvalget har sett at det eksisterer en utfordrende kompetansesituasjon innen IKT-sikkerhet på de fleste nivåer i samfunnet. Læreplanene for grunnskolen og den videregående skolen har målformuleringer knyttet til temaet, men det er uklart om det reelle læringsutbyttet dekker den kunnskapen om IKT-sikkerhet som hver enkelt av oss må ha for å kunne handtere en digitalisert hverdag på en trygg måte.» (s. 17).

6: Egeberg, G., Hultin, H., & Berge, O. (2016). *Monitor skole 2016: Skolens digitale tilstand.* Oslo, Norge: Senter for IKT i utdanningen. https://iktsenteret.no/sites/iktsenteret.no/files/attachments/monitor_2016_bm_-_2._utgave.pdf

7: https://www.datatilsynet.no/Om-Datatilsynet/rapporter-og-utredninger/Personvern-i-skole-og-barnehage---samlerapport/

8: Medietilsynet. (2016). *Barn & medier 2016.* 9–6-åringers bruk og opplevelser av medier. http://www.medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2016_barnogmedier.pdf

9: *Digital sårbarhet – sikkert samfunn:* https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/

Erfaringer fra Slettmeg.no

Slettmeg.no er en gratis råd- og veiledningstjeneste for personer som opplever krenkelser på nett. I 2016 håndterte tjenesten rundt 8000 henvendelser, og av disse sakene var ca. 14 % av de som søkte hjelp under 18 år. Våre veiledninger på slettmeg.no ble lest av 350.000 personer i 2016.

Om vi ser nærmere på hva voksne og eldre kontakter Slettmeg.no om, så trenger de i større grad brukerstøtte. Det vil si at de har havnet i problemer fordi de har vanskeligheter med å forstå hvordan teknologien fungerer, eller at de ikke vet hvordan informasjon kan spres.

Yngre mennesker er mer opptatt av personvern enn eldre. Selv om yngre kanskje ikke kjenner til personopplysningsloven i detalj har mange en klar formening om hva de ønsker å dele og ikke. Slettmeg.no sin erfaring er at

unge i større grad bruker lukkede grupper enn eldre. Dette kan selvfølgelig skyldes større teknisk kompetanse blant yngre og at unge i større grad kjenner til mulighetene for private grupper. Der eldre i større grad deler informasjon med alle, deler yngre oftere med en utvalgt gruppe.

Vår erfaring er at kunnskapsnivået blant yngre, om hva de bør og ikke bør gjøre på internett, er høy. Likevel ser vi at uønskede hendelser skjer. Dette skyldes trolig andre faktorer enn kunnskap. Det kan være tillitsforhold, gruppepress eller lignende som gjør at unge havner i problemer. Det ser også ut til at det er en oppfatning om at har du først delt noe innhold så må man regne med at det deles videre. Det kan også se ut til at det ikke er et bevisst forhold til i hvilken grad slik videre deling kan være et lovbrudd.

Påloggingsinformasjon ser ut til å være noe unge har utfordringer med. Tilliten til at venner ikke vil misbruke ens passord er høy, selv om det er mange eksempler på at venner har misbrukt påloggingsinformasjon som er blitt gitt til venner som man stoler på. Videre ser vi også at mange unge opplever problemer med at de mister påloggingsinformasjon til profiler de har på nett. Ofte bruker unge ikke epost, og eneste gangen de bruker epost er når de etablerer en konto. Deretter glemmes ofte både pålogging til epostkonto og til kontoene som har blitt opprettet på ulike nettsteder. I slike tilfeller opplever vi at det kan være vanskelig å for vedkommende å få slettet en konto.

61 % av de som kontakter Slettmeg.no er kvinner og 39 % er menn. Dette er en fordeling som har holdt seg stabil de siste årene. Vi har ingen entydige svar på hvorfor fordelingen er slik, men har trolig en sammensatt årsak og det er flere hypoteser for hvorfor det er slik. Jenter og kvinner kan være mer utsatt for krenkelser på nett og derfor øker mengden henvendelser fra kvinner. Den andre, som bør også bør utredes, kan være at gutter og menn vegrer seg for å søke hjelp. Tall fra andre lignende tjenester[10] viser at unge menn også er underrepresentert hos flere hjelpetjenester. Er det slik at unge menn har høyere toleranse grense for hva en krenkelse er, eller er de slik at menn er «opplært» til å tåle mer?

10: *Ung.no* rapporterer at flere kvinner som kontakter tjenesten enn men I sin årsrapport for 2016. *Kors på Halsen* rapporterer om 18% menn, 82% kvinner.

Tallene fra Slettmeg viser at i de tilfellene krenkeren er kjent, er det flest menn som står bak krenkelsen. Dette samsvarer med det man vet om mobbing blant unge[11], der det å være mobber er langt mer utbredt blant gutter enn jenter. Det å bli mobbet er derimot nesten like utbredt blant jenter som blant gutter. Vi vet for lite om årsakene til at gutter er så underrepresentert hos hjelpetjenestene. Vi antar at mange gutter opplever å bli krenket på nett, men at de ikke søker hjelp. Slettmeg mener at dette må undersøkes nærmere.

11: Folkehelseinstituttet. https://www.fhi.no/fp/barn-og-unge/oppvekst/fakta-om-mobbing-blant-barn-og-unge/

Informasjons-sikkerhetskultur – Teoretisk grunnlag

Beskrivelse av grunnleggende faktorer

Av alle egenskaper som skiller nasjoner fra hverandre, er kultur blant de mest dominerende. Alle nasjoner har kulturer. Nasjonale kulturer former oss, både hvordan vi er som gruppe og hvordan vi som individer plasserer oss i omgivelsene. Eller sagt på en annen måte: Nasjonale kulturer fungerer som et lim mellom innbyggerne og de er knyttet til våre underliggende verdier, som for eksempel hva vi anser å være normalt versus unormalt, trygt versus utrygt og rasjonelt versus irrasjonelt. Våre nasjonale kulturer gir oss et sett av verdier som hjelper oss å forstå omgivelsene. De utstyrer oss med et kompass som sier «hvordan vi gjør ting her». Resultatet er at de nasjonale kulturene blir til systemer av delte verdier, meninger og handlingsmønstre. Disse kan

variere stort fra nasjon til nasjon. De kulturelle verdiene og normene blir lært tidlig i livet, både gjennom formell utveksling (på skole, i fritidsaktiviteter, på arbeidsplassen etc.) og gjennom uformell sosial interaksjon med venner, foreldre, søsken og andre. Resultatet er at de nasjonale kulturene er dypt forankret i oss, og de varer gjennom generasjoner.

Nasjonale kulturer er selvsagt ikke helt klart definerte, og de kommer ikke som «one size fits all». De består av mange sub-kulturer, der faktorer som alder, geografi, interesser, kjønn mv. spiller inn. Digital kultur og Informasjonssikkerhetskultur er slike subkulturer, og vi observerer også forskjeller innad i disse, blant annet når en tar alder i betraktning.

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

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

Så langt har de fleste studier på informasjonssikkerhetskultur fokusert på adferdsdimensjonen. Mer spesifikt, de fokuserer på hvorvidt de folk vil trykke på en «phishing lenke», eller om de deler passordet sitt med fremmede. Resultatet har vært at, selv om det er en generell oppfatning om at informasjonssikkerhetskultur også omhandler verdier og holdninger, så settes disse til side til fordel for et fokus på adferd.

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

Dette fokuset leder oss til spørsmålet: Hva er nøkkelfaktorene som karakteriserer holdninger, verdier og følelser i en informasjonssikkerhetskultur? Hva er kjerneelementene i informasjonssikkerhetskultur?

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

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

Vi har pekt ut åtte kjerneområder, eller dimensjoner, som vi mener beskriver informasjonssikkerhetskultur på en helhetlig og relevant måte.

En kan ikke utelukke at det kan finnes andre dimensjoner som kan være nyttig å betrakte, men for vårt formål anses de utpekte kjerneområdene som tilstrekkelige.

Disse er:

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

I det følgende vil vi beskrive de åtte kjerneområdene, og våre funn for ungdommenes informasjonssikkerhetskultur.

Fellesskap

Kulturer er per definisjon kollektive. Kulturer består av individer: Kulturer utvikles av individer, og på same tid bidrar kulturer til å forme individene som er en del av kulturene. Kulturer beskriver det karakteristiske for en gruppe mennesker, herunder deres sosiale vaner, deres holdninger, verdier og prioriteringer. Kulturer krever en viss form for solidaritet blant sine medlemmer. For at en kultur skal være varig krever den lojalitet og solidaritet. Individene må identifisere seg som en del av gruppen, bidra til den og føye seg etter de uttalte og ikke-uttalte normene for adferd. Når vi peker ut fellesskap som et av kjerneområdene, ønsker vi primært å fokusere på hvordan individet forholder seg til fellesskapet. Ser den enkelte seg selv som en del av et større «cyber-fellesskap»? Blir den enkeltes adferd formet av et felles sett med normer og adferdsmønstre?

Styring og kontroll

Styring og kontroll relaterer seg til fellesskap: Hvordan skal fellesskapet reguleres, og av hvem? I denne sammenhengen fokuserer vi på hvordan ungdommer ser på styring og kontroll i et digitalisert samfunn. Et aktuelt spørsmål her er synet på overvåking. Hvem skal trekke opp linjene for hva som er akseptabel bruk av IKT og digitale tjenester, hvor skal linjene trekkes opp og hvordan skal den enkelte rette seg etter disse?

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

Tillit

Tillit er en grunnstein i ethvert fungerende demokrati. Et demokrati forutsetter en viss tillit mellom innbyggerne, mellom innbyggerne og myndighetene, mellom myndighetsorganer, mellom bedrifter, mellom ansatte og arbeidsgivere og så videre. Tillit er en forutsetning for velferd, stabilitet og økonomisk vekst i en nasjon. Når stadig mer av vår nasjonale vekst er knyttet til digitalisering av samfunnet, blir tillit på dette området stadig viktigere.

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

Som en konsekvens av dette er digitaliseringen både avhengig av, og sårbar for, tillit. Digitalisering er en ønsket utvikling for de fleste nasjoner, og gitt den teknologiske utviklingen vi observerer er det nærmest uunngåelig. For innbyggerne kan det imidlertid oppstå visse dilemma.

Folk blir ikke bare oppfordret til å ta i bruk teknologi, de blir i noen tilfeller tvunget til det. Å være bankkunde i dag betyr at du må forholde deg til nettbank. Prisene for bank-transaksjoner i tradisjonelle banker øker sterkt, og tilgjengeligheten til bank-filialene blir sterk redusert etterhvert som de legges ned. Kommunikasjonen mellom den enkelte og det offentlige skal primært foregå digitalt. Dersom den enkelte ikke føyer seg etter denne utviklingen, risikerer de både og å glipp av de positive gevinstene ved digitaliseringen, og i noen tilfeller store ulemper ved å ikke rette seg etter det samfunnet har lagt opp til.

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

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

Målrettet markedsføring er på et vis medaljens bakside, når det kommer til digitalisering og tillit. Mange anser målrettet markedsføring å være et brudd på tilliten, ettersom leverandørene av digitale tjenester bruker informasjon om den enkelte til sin egen vinning. Dersom dette leder til redusert tillit kan det potensielt skade digitaliseringen av samfunnet.

Risiko-oppfattelse

Kompetanse, læring og risiko-oppfattelse er knyttet til hverandre. Et eksempel: Studier viser at en kan finne økt «risiko-adferd» blant mennesker som mener at de har mye kompetanse eller ferdigheter. Med andre ord, mennesker som har mer kompetanse innen informasjonssikkerhet står i fare for å overvurdere sin egen evne til å kontrollere truslene, og de kan dermed være disponert til å ta mer risiko[12].

I en studie av Kathryn Parsons, Agata McCormac, Marcus Butavicius og Lael Ferguson fra *The Australian Defence Science and Technology Organisation*, risiko-oppfattelse er fremhevet som en nøkkelfaktor for utforming av adferdsmønstre. Studien sier at enkeltpersoner har «an unrealistic optimism for risks that they perceive to be under their personal control»[13 14]. De argumenterer videre at «an individual may view their actions on their personal computer to be under their control, threats may be seen as less risky. Hence, the chance that non-adherence to security policies will result in serious consequences may also be underestimated. This means that individuals might be more likely to engage in risky behavior».

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

13: Ibid

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

Optimisme for teknologi og digitalisering

Digitaliseringen hjelper ikke bare bedrifter å bruke informasjonsteknologi og data på en smart måte, den sørger også for at den enkelte kan utnytte gevinstene av et digitalisert samfunn. I tillegg er det en stadig viktigere forutsetning for nasjonal økonomisk vekst. Ved å fokusere på optimisme for teknologi og digitalisering forsøker vi å gå lenger enn å bare observere det faktum at digitalisering bidrar til å forme samfunnet. I stedet trekker vi oppmerksomheten mot innbyggernes holdninger til denne utviklingen. Med andre ord: Din holdning til digitaliseringen påvirker måten du forholder deg til teknologi. En trygg digital innbygger er en forutsetning for den nasjonale digitaliseringen. Mistillit til digitale tjenester og frykt for datakriminalitet er noen av utfordringene som folk må forholde seg til når samfunnet digitaliseres. Vi må derfor lære mer om hvordan informasjonssikkerhetskultur skapes og påvirkes, både i samfunnsgrupper, i bedrifter og på et nasjonalt nivå.

Kompetanse

Alt den enkelte foretar seg, enten det er kontakt med det offentlige, kommunikasjon med andre mennesker eller å dele feriebildene våre med andre på sosiale medier, så er vi nødt til å forholde oss til IKT og digitale tjenester. Enten vi liker det eller ei. Dette betyr at innbyggerne må sørge for å lære seg de ferdigheter som er nødvendig for at de kan ta del i et moderne samfunn. Alle nordmenn må ha et sett med grunnleggende digitale ferdigheter. Spørsmålet er: Hvor og hvordan får de disse ferdighetene? Det er et paradoks at myndigheter og bedrifter oppfordrer alle til å ta i bruk digitale tjenester, men slike ferdigheter i liten grad inngår i skolens læreplaner. Folk flest blir derfor tvunget til å lære disse ferdighetene på egenhånd og på uformelle arenaer.

I alle kulturer blir noen mennesker lyttet mer til enn andre. Enten det er kjendiser eller eksperter på sine områder, noen får mer taletid og gjennom det større mulighet til å påvirke oss andre. Disse menneskene har stor påvirkning på hvordan kulturen endres. De vi beundrer og lytter til

påvirker våre verdier og holdninger. Gjennom dette påvirker de hvordan vi forholder oss til andre mennesker og hvilken adferdsmønstre vi får. Gjennom å fokusere på dette vil vi undersøke hvem de sterke røstene er når det kommer til læring av informasjonssikkerhet. Lærer ulike grupper i samfunnet av forskjellige typer mennesker? Hvordan arter disse forskjellene seg?

Interesse for teknologi og IT

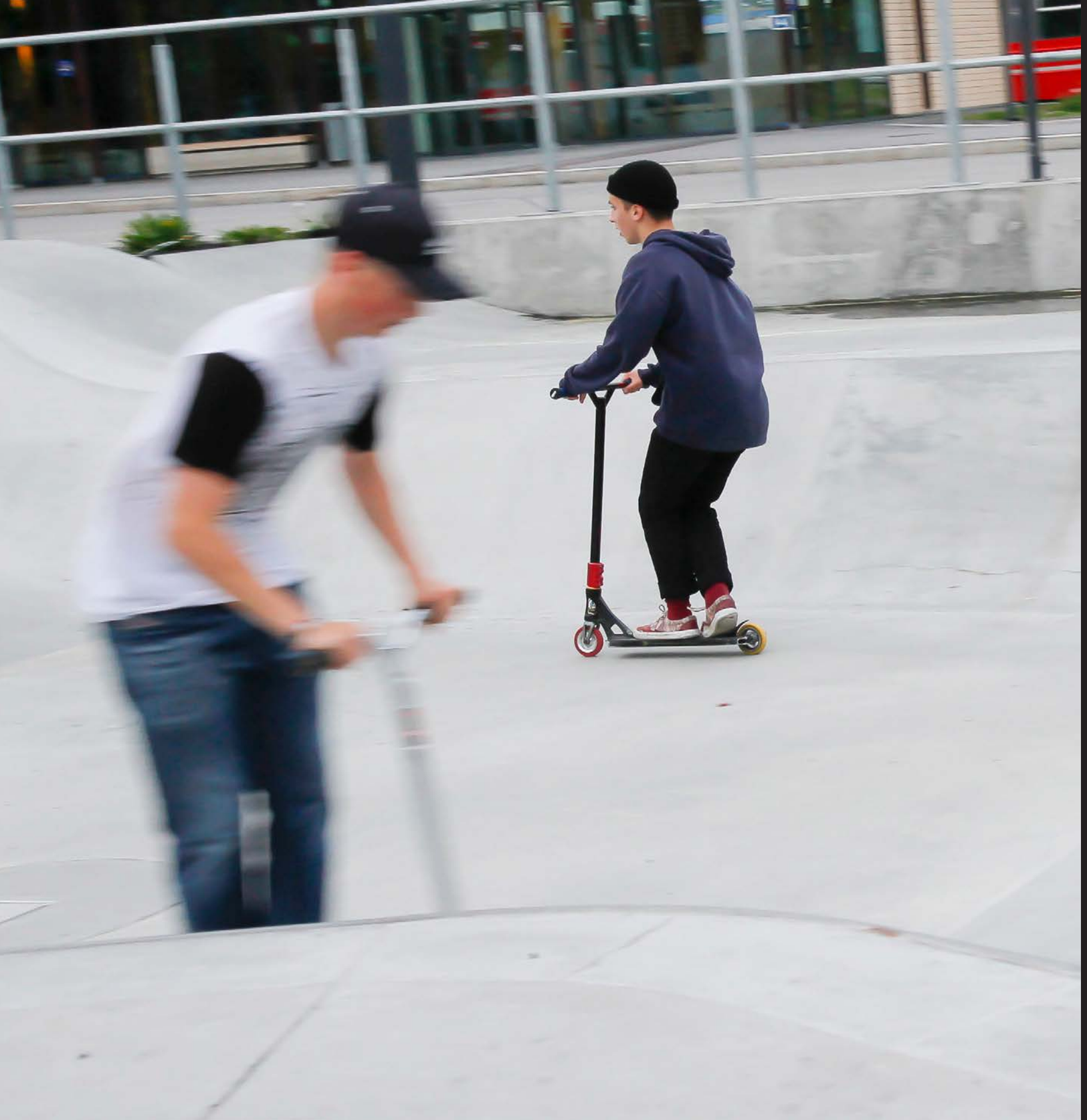
I et samfunn som blir stadig mer digitalisert, er det fristende å slå fast at de som har interesse for teknologi og IT har en fordel i forhold til de som ikke har slike interesser. Interesser former våre holdninger, ferdigheter og kunnskaper. Interesse påvirker også hvem vi vil assosiere oss med, og dermed hvem vi lærer fra. Med interesse følger det bevissthet, nysgjerrighet og tid. Dette er hjørnestener i all læring. Som en følge av dette kan en lure på om de som har slike interesser lærer raskere og «riktigere» enn de som ikke har det. Vi antar at interesse er en av nøkkelfaktorene for informasjonssikkerhetskultur og at det er viktig for deltakelsen i et digitalisert samfunn.

Adferdsmønstre

De fleste studier på informasjonssikkerhetskultur fokuserer på adferdstrekk eller adferdsmønstre. Dette er ikke uten grunn. Det er langt enklere å kun bry seg om adferd, og det er jo hva vi faktisk gjør som har en direkte og konkret påvirkning på informasjonssikkerhet.

I informasjonssikkerhet er det visse typer adferd som en oppfordrer til, mens en advarer mot andre. Myndighetene, ledende selskaper og eksperter gir råd som i sum kan sees på som en normativ standard for hvordan innbyggerne og ansatte skal oppføre seg på nett. Når det er sagt, ekspert-rådene og normene for «sikker adferd» har endret seg over tid. Dette er en naturlig konsekvens av den raske utviklingen i teknologien og hvordan vi tar teknologien i bruk. Dette betyr at det ikke er tilstrekkelig å få opplæring én gang. Opplæring må gjentas. Det du lærte for 10 år siden er ikke bare utdatert, det kan være direkte feil.
Når vi nå kartlegger informasjonssikkerhetskultur, så er det en rekke ting vi oppfordrer alle å gjøre. Man bør ikke dele passordet sitt med andre, man bør ta sikkerhetskopi av viktige data og man bør sikkerhetsoppdatere programmene sine jevnlig. Dette er en del av dagens normative beskrivelse av hva sikker digital adferd er, og vi oppfordrer til dette for å redusere faren for datakriminalitet, for tap av informasjon og for at du skal bli utsatt for manipulering og så videre.

Å måle adferdsmønstre som en del av den norske informasjonssikkerhetskulturen innebærer to ting: Først og fremst, vi vil beskrive det generelle adferdsmønsteret blant ungdommene. Dernest vil vi undersøke om de følger rådene som blir gitt dem.



Informasjonssikkerhet blant unge

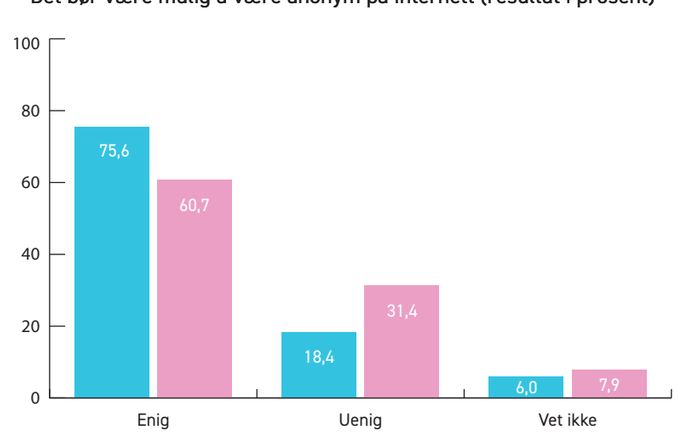
I det følgende beskriver vi hva som karakteriserer informasjonssikkerhetskulturen blant ungdom. I denne studien betyr det personer som er 19 år eller yngre. Vi viser til kapitlet om demografi for en ytterligere redegjørelse.

Fellesskap

Det interessant å undersøke i hvilken grad ungdommene mener at de er en del av et «digitalt fellesskap» eller en «informasjonssikkerhetskultur». En indikator kan være spørsmålet om anonymitet fordi begrensninger i anonymitet kan ha en positiv effekt på utfordringer som hets og mobbing på nett. 67,7 % av ungdommene svarer at de er enige i påstanden «Det bør være mulig å være anonym på internett.» Dette er en økning i forhold til befolkningen forøvrig, hvor 59 % svarer at de er enige i dette.

En annen indikator kan være hvorvidt ungdommene mener at sikkerhet for deres egen datamaskin har betydning for sikkerheten til fellesskapet. 71,6 % svarer at «Internett blir ikke tryggere selv om min datamaskin er sikker». Dette er omtrent det samme som for befolkningen forøvrig, der 73,9 % sier det samme.

Det kan virke som at ungdommene har en svakere fellesskapsfølelse når det kommer til det «digitale fellesskapet» enn det befolkningen forøvrig har, men vi kan ikke utelukke at det også kan skyldes manglende kunnskap om hva informasjonssikkerhet er i praksis. Det er også noen kjønnsforskjeller, der jenter ser ut til å ha en noe sterkere fellesskapsfølelse enn gutter når det kommer til synet på anonymitet på nettet. Effektstørrelsen er liten, men opp mot middels.



Figur 1: Kjønnsforskjeller i synet på overvåking. Tallene er signifikante p<0,001. Cramér's V er på 0,29

Det er ingen vesentlige forskjeller på gutter og jenter når det gjelder synet på om ens egen sikre datamaskin fører til at internett blir mer sikkert.

Styring og kontroll

Når det kommer til spørsmålet om overvåking av ens aktivitet på internett, stiller 38,9 % av ungdommene seg positive til dette dersom det fører til at de blir tryggere på nett. Dette er vesentlig færre enn det som gjelder for befolkningen forøvrig, hvor 59 % svarer at de er positive til slik overvåking.

Tilliten til politiet er imidlertid større blant ungdommene. 58,7 % sier at de tror at politiet vil hjelpe dem dersom de blir utsatt for datakriminalitet, og 20,9 % sier at de er uenige i dette. I befolkningen generelt svarer henholdsvis 45,8 % og 36,5 % det samme. I følge Politiets innbyggerundersøkelse fra 2016, svarer 6 % at de har et meget godt og 25 % at de har et ganske godt inntrykk av hvordan politiet håndterer identitetstyveri. For kategorien svindel på internett er tallene henholdsvis 4 % og 20 %.

Videre ser vi at 58,2 % av ungdommene mener at aktivistgrupper har en rolle i kampen mot datakriminalitet. Dette er vesentlig fler enn for befolkningen generelt, hvor 41.1 % svarer det samme. Dette kan selvsagt være et uttrykk for at ungdommene har lite kunnskap om hva etterforskning av kriminalitet faktisk innebærer, men i ytterste konsekvens kan det være et uttrykk for en forvitring av maktprinsippene i samfunnet. Altså, hvem skal utøve makt i det digitale rom, og hvordan skal de gjøre det? De fleste ungdommer mener samtidig at politiet skal beskytte dem når noe har gått galt. 61,8 % sier at de ville anmeldt nettsvindel, og 73,7 % sier at de ville anmeldt ID-tyveri. Igjen er dette færre enn det vi observerer for befolkningen generelt, der henholdsvis 85,6 % og 92,9 % sier det samme.

Ungdommene er mer opptatt av personvern enn befolkningen forøvrig når det kommer til overvåking: 54,4 % er uenige i at det er greit å bli overvåket på internett dersom det gjør det tryggere, og 67,7 % sier at det bør være mulig å være anonym på nett.

Når det gjelder det en selv gjør for å beskytte personlig informasjon, er det imidlertid færre som oppgir at de vil sørge for at slike data er slettet fra digitale enheter før de blir kastet eller solgt. 83,8 % sier at de vil gjøre dette, mot 90,6 % i befolkningen.

Tillit

En av grunnene til at det norske demokratiet er velfungerende, er fordi nordmenn har tillit til de rundt seg. Folk flest stoler på naboen, på sin arbeidsgiver og på myndighetene. Nordmenn forventer å ikke bli ranet av naboen, at arbeidsgiver betaler lønn og at myndighetene leverer den velferden en forventer uten noen form for korrupsjon.

Det er veldokumentert at det norske samfunnet er preget av en høy grad av tillit

Det er derfor ikke overraskende å se at 57,1 % av ungdommene oppgir at de stoler på at myndighetene skal beskytte informasjonen de har lagret om dem. Riktignok er dette en lavere andel enn for befolkningen forøvrig, hvor 65,4 % oppgir det samme.

64,4 % i aldersgruppen under 20 år mener at de ikke utsetter seg for risiko ved å bruke nettbank, og kun 9,5 % mener at risikoen ved bruk av nettbank er høy. 49 % sier at de ikke er bekymret for å bruke offentlige tjenester på nett, mens 11 % mener at de løper en risiko ved å bruke slike tjenester.

En interessant observasjon er at 18,6 % av ungdommene mener at norske nettsteder er tryggere enn utenlandske, og kun 1,3 % mener at utenlandske nettsteder er tryggere. 18,4 % mener at de er like trygge/utrygge, og 54 % mener at det avgjørende er om nettstedet er velkjent. Sammenlignet med befolkningen forøvrig er det like stor andel som mener at norske nettsteder er tryggere, mens det er flere unge som

mener at det er avgjørende at nettstedet er velkjent enn det man mener i befolkningen generelt (54 % vs. 39,6 %).

Risiko-oppfattelse

Risiko-oppfattelse er svært subjektivt, men er likevel en viktig faktor som påvirker hvordan vi tenker og handler når det kommer til digitale trusler. Det er en faktor som er vanskelig å tallfeste, beregne og forutse. Likevel vet vi at risiko-oppfattelsen vil bli påvirket av sikkerhetshendelser, hva vi tror at vi vet om digitale trusler, våre erfaringer osv.

50 % av ungdommene mener at de utsetter seg for risiko når de bruker internett. Dette er langt færre enn det som gjelder for befolkningen generelt, der 72 % sier det samme. Vi ser her ingen kjønnsforskjell mellom gutter og jenter. 61,3 % av ungdommene mener at de får tilstrekkelig informasjon om truslene som finnes på nett. 81,8 % svarer at de mener at de kan avgjøre hva som er trygt eller utrygt å gjøre på nett. Dette er vesentlig mer enn for befolkningen forøvrig, der 61 % svarer at de kan vurdere dette. Kun 7 % av ungdommene sier at de ikke kan vurdere dette, i motsetning til 23,5 % i befolkningen generelt.

59,4 % av ungdommene mener at det er størst risiko for at noen andre skal gjøre noe mot dem (for eksempel hacke en webside hvor de har lagt inn personlige data), mens 27,9 % mener at de selv skal gjøre noe som utsetter dem for risiko. Dette er tilsvarende som for befolkningen forøvrig, og kan bety at det er en generell positiv tro på egne ferdigheter når det kommer til informasjonssikkerhet. Eller sagt på en annen måte: Ungdommene har tro på egne ferdigheter, men uttrykker bekymring for andres intensjoner.

Vi undersøker også om kunnskap om digitale trusler har ført til at ungdommene har avstått fra å bruke tjenester på nett. 42,1 % sier at slik kunnskap har fått dem til å la være å bruke tjenester på nett, mens 36,4 % sier at de ikke har latt være å bruke dem.

Ungdommene er ikke veldig bekymret for å bruke digitale tjenester. Generelt finner vi en sammenheng mellom risiko-oppfattelse og alder. Det vil si: Jo eldre man er, jo større risikofylt oppleves aktiviteter på nett. Unntakene er hendelser som primært rammer de yngre aldersgruppene, for eksempel nettmobbing. Kun 9,5 % mener at det å bruke nettbank er risikofylt, og 11 % mener at det er risikofylt å bruke offentlige tjenester på nett. Dersom vi fokuserer på det vi mener er godt nettvett, ser vi at 72,9 % mener at det er risikofylt å dele passordet sitt med andre. I befolkningen generelt mener 85 % det samme. 38,1 % mener at det er risikofylt å bruke det samme passordet på flere nettsteder. Dette er langt færre enn i befolkningen generelt, hvor hele 61 % anser en slik praksis for å være risikofylt. Kun 30,2 % mener at det er risikofylt å ikke ta sikkerhetskopi av sine data, mot 63 % i befolkningen forøvrig.

Optimisme for teknologi og digitalisering

Ungdommene er generelt svært positive til å ta i bruk ny teknologi. 93,9 % er positive til dette, mens kun 2.7 % er negative. Samtidig sier 62,6 % at de vet hva informasjonssikkerhet er. Dette er noe lavere enn for befolkningen generelt, der 89,9 % sier at de vet hva det er.

Kompetanse

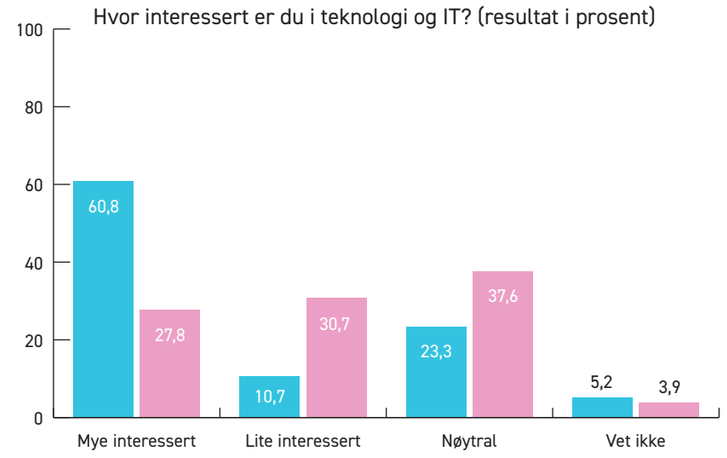
Nordmenn er generelt kunnskapsrike når det kommer til informasjonssikkerhet. De ser også seg selv som relativt kunnskapsrike, og mener at de kan gjøre riktige vurderinger for sin sikkerhet på nett. Generelt mener nordmenn at de kan like mye eller mer enn gjennomsnittet, når det kommer til informasjonssikkerhet. I befolkningen generelt mener 57,4 % at de kan omtrent det samme som folk flest, mens 33,4 % mener at de kan mer enn gjennomsnittet. Blant ungdommene mener 58,5 % at de kan like mye som folk flest, mens 26,9 % mener at de kan mer.

Hele 81,8 % av ungdommene mener at de er i stand til å vurdere hva som er trygt eller utrygt å gjøre på nett. I befolkningen forøvrig mener 61,1 % det samme. Kun 7 % av ungdommene sier at de ikke vet hvordan de skal vurdere dette, mens 11,2 % sier at de ikke vet. Ungdommene har altså større tro på egne ferdigheter enn det befolkningen generelt har.

Interesse

Nesten halve befolkningen (47,1 %) forteller at de har en interesse for teknologi og IT, mens 33,4 % forteller at de er nøytrale i forhold til det. Vi observerer at blant ungdommene sier 43,3 % at de er interessert i dette, mens 30,8 % sier at de er nøytrale. Dette fremstår som noe overraskende, da vi hadde forventet at de yngre aldersgruppene var mer interessert i teknologi og IT. Det er likevel slik at i sum er gruppene som er positive eller nøytrale i forhold til interesse er klar majoritet. Dette samsvarer med spørsmålet om ungdommene er positive til ny teknologi.

Det er imidlertid store kjønnsforskjeller når det gjelder interesse. Det er omlag dobbelt så vanlig at gutter er interessert i teknologi og IT som det jenter er. Dette er betydningsfullt fordi vi i hovedstudien koblet interesse til en rekke positive trekk ved informasjonssikkerhetskultur, herunder kompetanse, læring og sikker adferd. Effektstørrelsen er middels (Phi=0,454).



Figur 2: Kjønnsforskjeller for interesse for teknologi og IT. Tallene er signifikante p<0,001. Phi=0,454. N=772.

Adferdsmønstre

71,2 % av ungdommene sier at de undersøker om en nettside er trygg før de bruker den, men kun 6,5 % sier at det alltid gjør dette. 81,8 % sier at de vet hvordan de skal undersøke om noe er trygt eller utrygt på nett.

De fleste fageksperter er enige om hva som regnes å være sikker bruk av passord, men vi observerer likevel at hele 44 % sier at de bruker samme passord over alt. Dette er en signifikant økning i forhold til befolkningen generelt, der 18,5 % sier det samme. Blant ungdommene er det 42 % som sier at de bruker forskjellige passord på de fleste nettsteder. Passord-managere kan hjelpe oss å bruke sikrere og forskjellige passord på ulike nettsteder. Likevel er det kun 7 % som oppgir at de bruker slike verktøy. 29 % sier at de legger vekt på å lage sikre passord. I befolkningen forøvrig er det 7,8 % som sier det samme.

27,7 % sier at de ikke har noen rutiner for å oppdatere programvare, og 17,1 % sier at de ikke vet om de har slike rutiner. For befolkningen generelt svarer man henholdsvis 18 % og 6,6 % på dette spørsmålet.

Dette betyr at datamaskiner og andre digitale enheter som brukes av ungdom i større grad er sårbare for datakriminalitet, dersom ingen andre personer i deres nærmiljø tar ansvar for å oppdatere dem.

22,9 % sier at de aldri tar sikkerhetskopi av sine data, mot 14,7 % i befolkningen generelt. 20,3 % sier at de ikke vet om de gjør dette, mot 9,3 % i befolkningen generelt. De fleste av ungdommene som tar sikkerhetskopi (34,3 %), gjør det sjeldnere enn hver måned.

Sikkerhetsprogramvare som antivirus, brannmurer og VPN-løsninger kan gi beskyttelse mot datakriminalitet og andre uønskede sikkerhetshendelser. 5,4 % forteller at de ikke bruker noen former for sikkerhetsprogramvare, og hele 30,7 % sier at de ikke vet om de bruker slik programvare. 47,3 % oppgir at de bruker brannmur og 50,4 % oppgir at de bruker anti-virus. Det er oppsiktsvekkende at så mange ikke vet om de bruker noen former for sikkerhetsprogramvare. I befolkningen forøvrig er det 9,3 % som sier at de ikke vet. Vi kan videre anta at det høye antallet som bruker brannmur og anti-virus kan forklares ved at de fleste datamaskiner i dag blir levert med slike programmer. Det er derfor ikke sikkert at dette er et valg som ungdommene i realiteten tar selv.

17 % av ungdommene sier at de noen ganger bevisst bryter reglene for informasjonssikkerhet. I befolkningen forøvrig er det 9,5 % som sier det samme.

Kompetanse, kunnskap og læring

Introduksjon

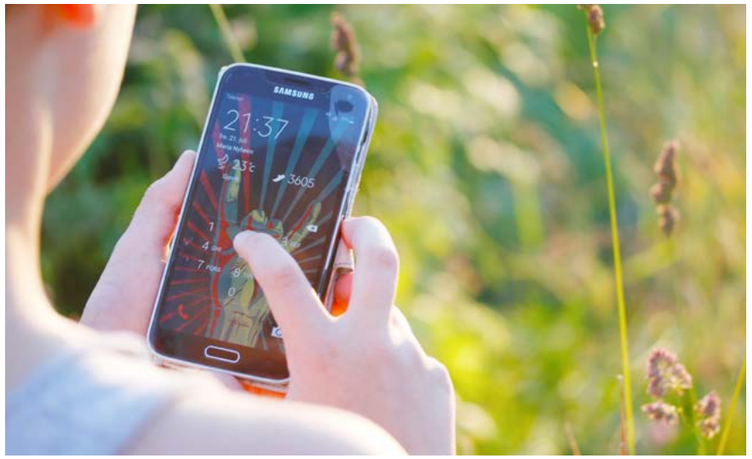
Det har vært svært mange teknologiske framskritt innen informasjonssikkerhet de senere årene, men utvikling innen teknologi alene kan ikke skape et trygt digitalt samfunn. Bruk av sterk kryptering og sikrere operativsystemer og programmer gjør det vanskeligere å utnytte datasystemer til kriminelle formål. Dette tvinger de kriminelle til å tilpasse seg. Vi observerer en klar økning i nettsvindel og annen type datakriminalitet som retter seg mot mennesker. Dette kan bety at de kriminelle er i ferd med å endre fokus og metode, fra å angripe datamaskiner, til å angripe menneskene som bruker dem.

Måten vi forholder oss til informasjonsteknologi og digital risiko forandres og blir mer kompleks

Etterhvert som samfunnets avhengighet av teknologi øker, legges det mer ansvar på den enkelte innbygger. Vi forventer at alle skal forstå hvilken risiko de tar ved å bruke digitale tjenester. Dette betyr at den enkelte må har oppdatert kunnskap om en trussel som er i konstant endring, og om den teknologiske utviklingen og dens sårbarheter. Vi forventer at alle skal fremvise en trygg og sikker adferd på nett, selv om hva det faktisk er også endrer seg over tid. (Bytter du passordene dine ofte, og passer på at du ikke har skrevet dem ned noe sted? Vel, nå anbefaler vi at du skal skrive dem ned[15], og at du ikke skal bytte passordet før du tror at det har kommet på avveie[16]).

15: https://nsm.stat.no/blogg/er-sommerferie-2014-et-bra-passord/

16: https://www.cesg.gov.uk/articles/problems-forcing-regular-password-expiry

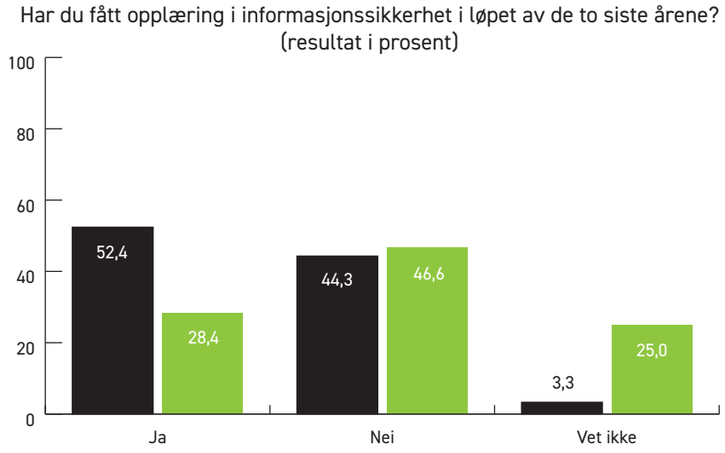


Dette plasserer et enormt ansvar på den enkelte. Vi forventer at alle skal oppføre seg etter både uttalte og ikke-uttalte normer. Bedrifter tilnærmer seg dette gjennom opplæring og bevisstgjøringskampanjer, men gjør lite for å vurdere effekten av disse tiltakene. De som ikke er i arbeid, eller som er ansatte i bedrifter som ikke gir opplæring i informasjonssikkerhet til sine ansatte, er i hovedsak overlatt til det de lærer på skolen eller til uformell kompetanseoverføring.

Ungdommene er i hovedsak fremdeles under utdanning, og er derfor normalt ikke en del av den utdanning som gis i bedriftene. Samtidig er de morgendagens ansatte, og de er i en fase i livet der verdigrunnlag og holdninger dannes. Vi må derfor vite mer om hvordan kompetanse og kunnskap om informasjonssikkerhet dannes hos denne gruppen. Lærer denne gruppen på en annen måte enn det som er vanlig i befolkningen generelt, og hvilken effekt har deres læring på forming av adferdsmønstre?

Våre funn

Vi finner at 28,4 % av ungdommene har fått opplæring i informasjonssikkerhet i løpet av de to siste årene. 44,5 % sier at de ikke har fått slik opplæring, mens hele 25 % ikke vet om de har fått opplæring.



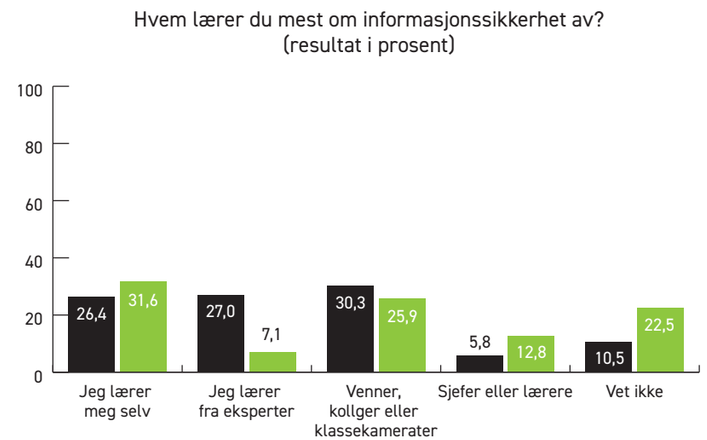
Figur 3: Opplæring i informasjonssikkerhet blant ungdommene. Forskjellene mellom unge og voksne er signifikant, p<0,001. Phi er 0,291. N=8227

Vi observerer en nær halvering av andelen ungdommer som sier at de har fått opplæring i informasjonssikkerhet de to siste årene, sammenlig-

net med befolkningen forøvrig. Det er interessant at det er liten forskjell på de som svarer «nei» på dette spørsmålet, og samtidig er svært stor økning for de som svarer «vet ikke». Effektstørrelsen er liten, opp mot middels (Phi=0,291).

Vi er opptatt av om slik opplæring har en effekt, og i hvilken grad vi kan beskrive effekten. Når vi spør ungdommene om de synes at opplæringen har gitt dem bedre ferdigheter innen informasjonssikkerhet, så svarer 54,1 % av de som har fått opplæring at de mener at de har fått bedre ferdigheter. I befolkningen generelt er det 77,1 % som mener dette. Det er også en høyere andel som mener at de ikke har fått bedre ferdigheter (20,6 % versus 10,2 % i befolkningen generelt), og en høyere andel av de som ikke vet om de har fått bedre ferdigheter (25,2 % versus 12,7 % i befolkningen generelt).

Spørsmålet er imidlertid ikke bare hvorvidt ungdommene har fått opplæring, men også hvordan de lærer og av hvem. Når vi ser på hvem ungdommene lærer av, sammenlignet med befolkningen forøvrig, observerer vi noen interessante funn. Mest fremtredende er det at ungdommene i langt mindre grad lærer om informasjonssikkerhet av eksperter og fagfolk enn det som er tilfellet for befolkningen generelt.



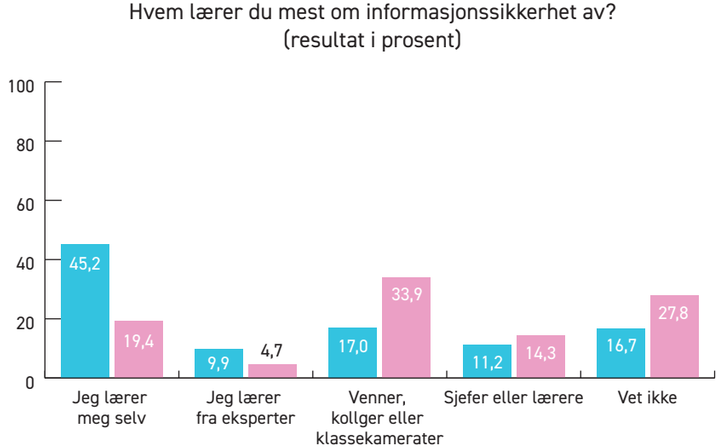
Figur 4: Hvem ungdommer lærer informasjonssikkerhet av. Forskjeller mellom unge og voksne er signifikante, p<0,001. Phi er 0,200. N=8227.

Det er videre flere som lærer av sjefer eller lærere, altså av autoritetspersoner. Det er også oppsiktsvekkende at så mange som 22,5 % forteller at de ikke vet av hvem de lærer om informasjonssikkerhet.

De under 20 år lærer i hovedsak ikke fra eksperter, kun 7 % sammenlignet med 27 % i befolkningen generelt

Når vi ser på kjønnsforskjellene ved hvem ungdom lærer om informasjonssikkerhet av, observerer vi at gutter oftere lærer av seg selv, mens jenter lærer mer i en sosial setting, altså av venner.

Det er også mer vanlig at jenter ikke vet hvem de lærer om informasjonssikkerhet av.



Figur 5: Kjønnsforskjeller i henhold til hvem ungdom lærer av. Forskjellene mellom kjønn er signifikante, p<0,001. Phi er 0,324. N=772.

Hvilken læringsmetode som er vanlig blant ungdommene er også av interesse. Det er en vesentlig forskjell på om læringen skjer formelt og strukturert, eller på en mer uformell måte.

Vi observerer at ungdommene i noe større grad lærer gjennom egen prøving og feiling, og at langt færre lærer på kurs eller utdanning, altså på en formell og strukturert måte. Igjen er det oppsiktsvekkende å se at så mange sier at de ikke vet hvordan de vanligvis lærer om informasjonssikkerhet.

Figur 6: Hvordan ungdommene lærer om informasjonssikkerhet. Tallene er signifikante, p<0,001. Phi er 0,198. N=8169.

Vi har videre undersøkt visse sider ved deres selv-innsikt når det kommer til opplæring i informasjonssikkerhet og synet på egne evner og ferdigheter. En slik side er hvor ungdommene plasserer seg selv, kunnskapsmessig, i forhold til de rundt seg.

Medietilsynets rapport fra 2016 undersøker hvem som lærer barn i aldersgruppen 9-16 om trygg og sikker bruk av medier.

Rapporten viser at de aller fleste barn i alderen 9–16 år har lært om trygg og sikker bruk av nett, mobil og spill. Kun tre prosent svarer nei på dette spørsmålet, og seks prosent har svart «vet ikke». 78 % har lært om dette på skolen, 61 % har lært om dette av mamma og 54 % av pappa. Det er også en del som oppgir å ha lært nettvett fra tv (39 %) og internett (32 %) og av venner (26 %).

Det er små forskjeller mellom jenter og gutter og mellom ulike aldersgrupper når det gjelder om man har lært om trygg og sikker bruk av nett, mobil og spill. Det er imidlertid noen forskjeller mellom kjønnene når det gjelder fra hvem man har lært om dette.

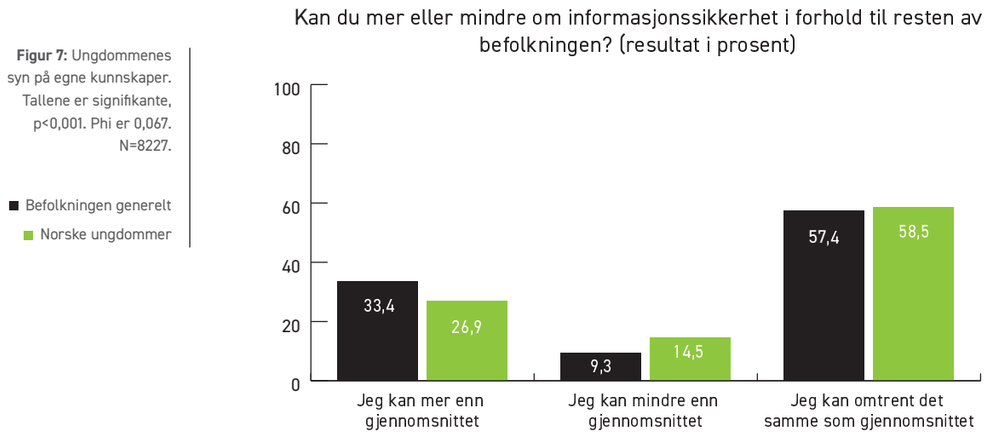
De samme kildene er viktigst, uavhengig av kjønn og alder, men medietilsynet finner at en høyere andel jenter enn gutter har lært om nettvett av foreldrene. Foreldre blir en mindre viktig kilde med alderen, mens internett som kilde blir viktigere, både for jenter og gutter. 50 % av guttene og 47 % av jentene i alderen 15–16 år har lært om trygg og sikker bruk av nett, mobil og spill på internett.

Det er også en litt høyere andel av jenter (28 %) enn gutter (24 %) som har lært om trygg og sikker bruk av venner, mens en høyere andel av gutter (13 %) enn jenter (5 %) har lært av data- og spillbutikker. Det er spesielt de eldste guttene (i alderen 15–16 år) som oppgir data- og spillbutikker som en kilde til kunnskap om nettvett (16 %).

I vår hovedstudie fra 2016 avdekket vi flere andre forhold som har relevans for kunnskap og læring.

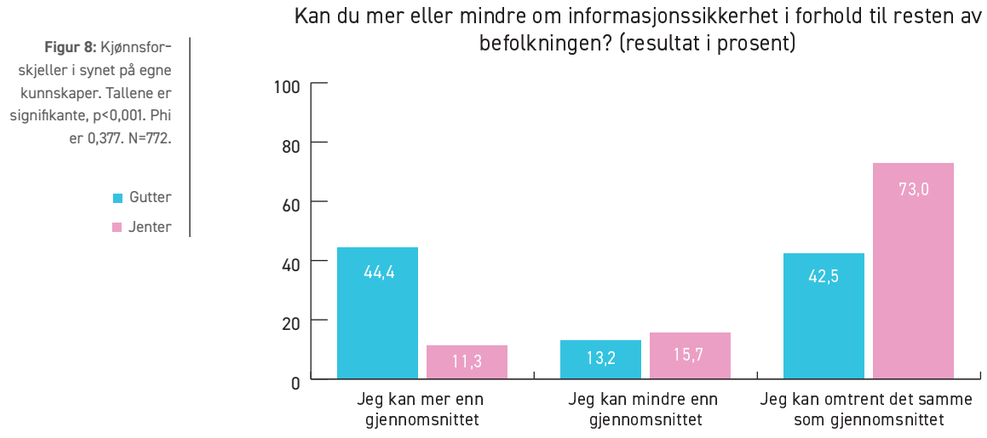
Vi vurderer også hvordan ungdommene bedømmer egne ferdigheter i forhold til de rundt seg. Når vi spør befolkningen forøvrig om den enkelte vurderer at de kan mer, like mye som eller mindre enn andre når det kommer til informasjonssikkerhet, så svarer 33 % at de kan mer enn folk flest, og 57,4 % sier at de kan omtrent like mye. Ungdommene har ikke like stor tro på egne ferdigheter, og vi finner at 26,9 % sier at de kan mer og 58,5 % sier at de kan like mye som andre.

Figur 7: Ungdommenes syn på egne kunnskaper. Tallene er signifikante, p<0,001. Phi er 0,067. N=8227.



Vår undersøkelse viser at det er noen kjønnsforskjeller for dette spørsmålet. Det er mer vanlig at gutter vurderer sin egen kompetanse høyere enn det jenter gjør.

Figur 8: Kjønnsforskjeller i synet på egne kunnskaper. Tallene er signifikante, p<0,001. Phi er 0,377. N=772.



Når det gjelder synet på om en selv er i stand til å vurdere hva som er trygt, viser studien at ungdommene vurderer egne ferdigheter høyere enn det som er vanlig i befolkningen generelt. 61 % av folk flest mener at de kan vurdere dette, mens hele 81,8 % av ungdommene mener at de har slike ferdigheter.

Et sentralt spørsmål innen kompetanse og kunnskap er hvorvidt den enkelte mener at de selv har mulighet til å påvirke sikkerheten til sine omgivelser. Vi omtaler gjerne dette som netthygiene, og beskriver dette som alle tiltak en gjør for at både en selv og de rundt en skal være tryggere på nett. Tankene dras i retning av tradisjonell hygienetenkning, der håndvask og vaksineringsprogrammer ikke bare skal beskytte den enkelte mot infeksjon og smitte, men også de som er i miljøet rundt en selv. På tross av at 62,6 % sier at de vet hva informasjonssikkerhet er, mener hele 71,6 % at internett ikke blir tryggere selv om deres egen datamaskin er sikker. Dette er ikke i tråd med den faglige oppfatningen av hva informasjonssikkerhet er. Å sikre egne datamaskiner, mobiltelefoner og andre enheter som er på nett vil forstyrre de kriminelle «verdi-kjedene», og vi anser derfor dette som en del av den helhetlige beskyttelsen av det digitale rom. En mulig forklaring på at så mange ikke er enige i en slik påstand kan skyldes at det ikke legges mye vekt på dette i den opplæringen som gis i dag.

På et nasjonalt nivå er det ikke sikkerheten til den enkelte datamaskin som er viktig, men at mange nok av dem er det.

Et annet forhold er hvordan interesse for teknologi og IT spiller inn på læring om informasjonssikkerhet. Hovedstudien viste at selv om nærmest hele befolkningen er positiv til ny teknologi, så er det kun 47 % som sier at de har en interesse for teknologi og IT. Blant ungdommene er det 43,4 % som sier at de har interesse for dette. Interesse er et av våre kjerneområder når vi skal beskrive informasjonssikkerhetskultur, blant annet fordi det påvirker selve læringsprosessen. Generelt lærer de som er interessert i teknologi og IT oftere av en fagekspert og gjennom egen prøving og feiling. Vi antar at dette har betydning for selve innholdet i

kunnskapsoverføringen, der de som er interessert mottar mer korrekt kunnskap om informasjonssikkerhet.

Vurdering

Når resultatene skal tolkes må en ta i betraktning at opplæring, slik det er formulert i vår undersøkelse, trolig ikke vil bli forstått likt av alle respondenter. Noen kan se på opplæring som noe som kun skjer i formelle rammer, mens andre kan se på den uformelle samtalen med sine venner som en del av opplæringen i informasjonssikkerhet. Det gis ingen enhetlig opplæring til ungdommene og vi har derfor valgt å tillate dem å tolke dette spørsmålet selv, til en viss grad.

En av de mer karakteristiske trekkene ved ungdommene er at det rår mye usikkerhet omkring opplæring i informasjonssikkerhet. Det er mange som ikke vet hvordan og av hvem de lærer om informasjonssikkerhet, på tross av at mer enn 6 av 10 sier at de vet hva det er. 25 % vet ikke om de har fått opplæring. 46 % vet ikke om de bryter reglene for informasjonssikkerhet. Dette tyder på at opplæringen som gis ungdommene er for lite strukturert og tydelig, både i form og innhold.

Studien viser at opplæring i informasjonssikkerhet er noe som primært skjer i voksen alder, og da i regi av en arbeidsgiver. Kun 28,4 % av ungdommene mener at de har fått opplæring i løpet av de to siste årene. De lærer i hovedsak av venner eller av seg selv. Det er få som lærer av fageksperter. Det er også slik at de fleste enten prøver og feiler selv, eller lærer i en uformell situasjon. Det er urovekkende at det ikke legges et større fokus på opplæring for denne aldersgruppen ettersom det er nettopp på dette stadiet i livet av verdier og holdninger formes. Det er også av stor betydning at ungdommene får tilgang til korrekt og tidsriktig informasjon om hvordan de skal beskytte seg selv, og de rundt seg, på internett. Å overlate læring om informasjonssikkerhet til tilfeldighetene og til den enkelte gir et dårlig utgangspunkt for at dagens ungdommer skal bli trygge digitale innbyggere og ansatte i norske bedrifter.

En rapport[17] (2014) fra Medietilsynet viser at 88 % av alle barn mellom 1 og 12 år bruker internett hver uke eller oftere. 55 % bruker internett daglig. Studien konkluderer med at barn bruker internett mer enn før, og at det er en størst økning i aldersgruppen 1–4 år. Når vi tar i betraktning at kun halvparten av befolkningen har fått opplæring i informasjonssikkerhet i løpet av de to siste årene må vi forvente at ungdommene ikke får tilstrekkelig veiledning og oppdragelse fra foreldre eller andre voksne, på dette området. En kan gjerne mene at barn og unge i dag har et naturlig talent for å navigere i det digitale landskapet, men det er ingenting som tyder på at de har en medfødt evne til å forstå et komplekst og dynamisk digitalt trusselbilde. Statistikk (2015) fra Slettmeg.no viser at 7826 personer kontaktet dem for å få hjelp med alt fra nettmobbing, å få fjernet personlige bilder fra nettet eller til å håndtere ulike former for datakriminalitet. Mange av disse er i aldersgruppen under 20 år.

Vi mener at interesse former våre holdninger, meninger, ferdigheter og kunnskaper

17: www.medietilsynet.no/globalassets/publikasjoner/2015/rapport_foreldre_smabarns_medie-bruk_2014.pdf

I vår hovedstudie slo vi fast at interesse er en driver for kunnskap og læring. Det påvirker hvordan og av hvem folk lærer om informasjonssikkerhet av, og vi ser interesse som en positiv og selv-forsterkende læringsmetode som både utvikler og drar nytte av fokus, nysgjerrighet og kunnskap. De med interesse for teknologi og IT lærer av fageksperter, og som en følge av det er læringsinnholdet trolig mer korrekt. Vi finner også en sammenheng mellom interesse og det vi anser å være sikker adferd på nett. De som har interesse kan mer og gjør mer av de riktige tingene.

For en bedrift kan det være nyttig å vite om de ansatte er interessert, fordi en da kan legge til rette for at opplæring skjer mest mulig på de ansattes premisser. Dersom de ansatte helst lærer fra fageksperter i formelle settinger, så vil trolig kurs og liknende utdanning være mest effektivt. Om de ansatte helst lærer av kolleger, i en uformell setting, så er det kanskje å foretrekke såkalt dilemmatrening der en bedre utnytter slike sosiale settinger. For en bedrift, og deres ansatte, er dette trolig helt greit. Ikke alle bedrifter eller bransjer har behov for ansatte som er interessert i teknologi og IT.

For barn og ungdom bør en trolig tenke noe annerledes, og det er det flere grunner til. Vi legger til grunn at det er samfunnsnyttig at alle innbyggere i Norge har et sett med basiskunnskaper og -ferdigheter som setter dem i stand til å delta i et digitalisert samfunn på en trygg måte. Vi ønsker at de yngre generasjonene skal ha tillit, men ikke være naive. Vi ønsker at de skal ha gode holdninger og en god netthygiene. Vi ønsker at de skal avstå fra å delta i nettmobbing og vi vil at de skal ta ansvar for at deres datamaskiner ikke blir brukt til kriminalitet mot andre. De må ha kunnskap om hva som er rett og galt, og de må ta til seg holdninger og adferdsmønstre som bidrar til et trygt digitalt samfunn.

Å basere seg på at den enkelte skal ha interesse for dette, representerer en passiv holdning til vår samfunnsutvikling. I stedet bør myndighetene, og spesielt utdanningssektoren, sørge for at dette er basiskunnskaper for alle ungdommene. Da tror vi at vi vil kunne se en markant forbedring i vår nasjonale motstandsdyktighet mot datakriminalitet og andre sikkerhetshendelser.

Risiko-oppfattelse

Introduksjon

Med risiko-oppfattelse[18] mener vi hvordan mennesker vurderer kjennetegn og alvorlighetsgrad for risiko. Vi er opptatt av risiko-oppfattelse fordi vi blir møtt med sikkerhetsdilemmaer hver gang vi bruker internett. Digitale trusler kan manifestere seg på mange forskjellige måter, og vi har problemer med å se de komplekse digitale hendelsesforløpene som til slutt gjør oss sårbare. Skal jeg åpne e-post vedlegget? Vil mine holdninger til myndighetenes overvåking av internett gjør at jeg blir mer eller mindre trygg på nettet i det lange løp? Klarer jeg å gjøre en korrekt vurdering av risikoen knyttet til mine nett-aktiviteter?

Mange hevder ofte at folk mangler kunnskap[19] [20] om digital risiko, eller at folk er naive[21] [22] og lite bevisste[23]. Etter at større sikkerhetshendelser har funnet sted er det ikke

uvanlig å se at «den menneskelige faktor» får skylden for det som har skjedd. Folk blir klandret for å ta feil valg fordi de har mistolket risikoen knyttet til deres handlinger. Mennesker omtales som «det svakeste ledd» i sikkerhetslenken. Etter slike hendelser ser vi gjerne at det innføres opplæring og bevisstgjøringsprogram for å forhindre at slike hendelser skal skje igjen.

Risiko, spesielt komplekse risiko-kjeder som inneholder såkalte «menneskelige faktorer», er mer basert på personlige vurderinger enn på objektive beregninger. Hvordan den enkelte vurderer risiko kan bli påvirket av en rekke faktorer som kan endre seg fra dag til dag, eller situasjon til situasjon. Fakta og kunnskap spiller en stor rolle i risikovurderingene, men det gjør også erfaring, hvor risikovillige vi føler oss den dagen og hvorvidt du er en person som høy eller lav aksept for risiko.

I vår hovedstudie fra 2016 undersøkte vi hvilke faktorer som har sammenheng med og betydning for hvordan den enkelte vurderer risiko. Vi fant blant annet at alder er en slik faktor, og at yngre generelt vurderer digital risiko som lavere enn det eldre gjør.

Våre funn

Ungdommene har en generelt lavere oppfatning om at de utsetter seg for risiko når de bruker internett, enn det som er tilfellet for befolkningen generelt. 50 % mener at de utsetter seg for risiko, mens 44,3 % mener at de ikke utsetter seg for risiko. I befolkningen forøvrig svarer 72,1 % at de utsetter seg for risiko, mens 25,3 % mener at de ikke utsetter seg for risiko.

Ungdommene mener også at trusselen hovedsakelig er ekstern, altså at noen skal gjøre noe mot dem, ikke at de selv gjør noe som utsetter dem for risiko.

18: http://heatherlench.com/wp-content/uploads/2008/07/slovic.pdf

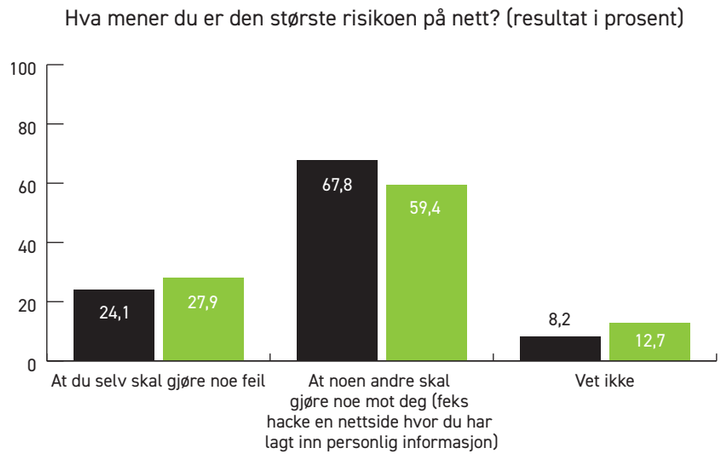
19: http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf

20: http://blog.trendmicro.com/trend-micro-lack-security-awareness-reason-high-number-cybercrime-victims/

21: http://www.welivesecurity.com/2016/01/29/businesses-still-naive-risks-cybercrime/

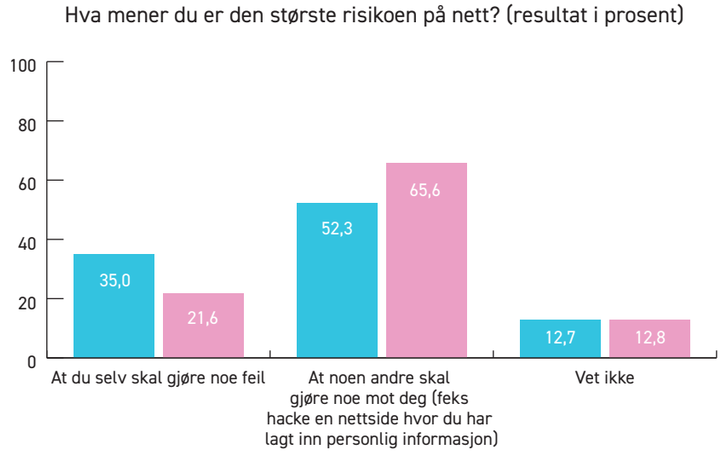
22: http://www.fin24.com/Tech/News/Young-people-more-naive-on-cyber-security-20151006

23: http://www.businessinsurance.com/article/99999999/NEWS030101/306019970/1248



Figur 9: Oppfatning om hva som er største risiko på nett. Tallene er signifikante, p<0,001. Phi er 0,067. N=8200.

Vi finner imidlertid visse kjønnsforskjeller for dette spørsmålet. Gutter er i noen grad mer bekymret for at de selv skal gjøre noe feil, enn det jenter er.



Figur 10: Kjønnsforskjeller på oppfatning om hva som er største risiko på nett. Tallene er signifikante, p<0,001. Phi er 0,153.

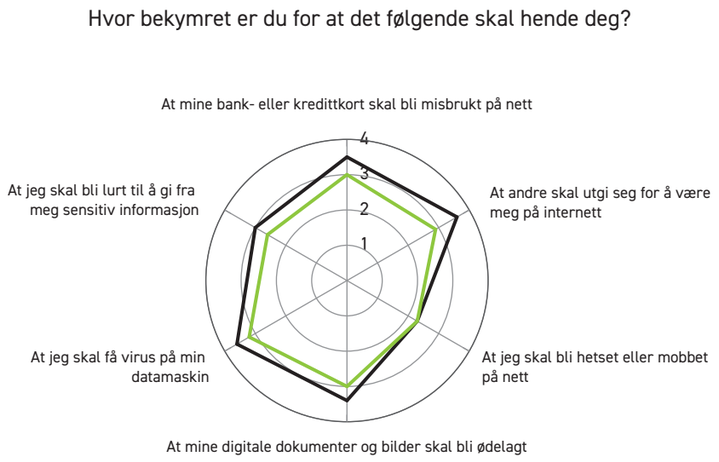
Før vi ser nærmere på ungdommenes risiko-oppfattelse, skal vi se hvorvidt de føler seg i stand til å vurdere hva som er trygt å gjøre på nettet. Hele 81,8 % mener at de er i stand til å gjøre en slik vurdering, mens kun 7 % sier at de ikke kan vurdere det. Ungdommene vurderer egne ferdigheter på dette området som langt bedre enn det som er vanlig i befolkningen forøvrig der 61,1 % sier at de kan gjøre en slik vurdering.

I vår hovedstudie valgte vi et sett med digitale trusler som nordmenn blir, eller kan bli, utsatt for. Disse er nettsvindel, ID-tyveri, nettmobbing, ødeleggelse av informasjon, ondsinnet kode og sosial maniulering. Vi spurte deltakerne i studien hvor bekymret de var for at disse truslene skulle ramme dem, på en skala fra 1 til 5, der 1 er «Ikke bekymret» og 5 er «Svært bekymret». I vår presentasjon av resultatene benytter vi gjennomsnittsverdiene for aldersgruppene under 20 år, sammenlignet med gjennomsnittsverdiene for befolkningen forøvrig.

Figur 11: Gjennomsnittsverdi for risiko-oppfattelse for vanlige digitale trusler. Tallene er signifikante, p<0,001. Phi ligger mellom 0,101 og 0,192. N=8200

Hvor bekymret er du for at det følgende skal hende deg?	Ungdommene	Befolkningen generelt
At mine bank- eller kredittkort skal bli misbrukt på nett	3,0	3,5
At andre skal utgi seg for å være meg på internett	2,9	3,6
At jeg skal bli hetset eller mobbet på nett	2,3	2,3
At mine digitale dokumenter og bilder skal bli ødelagt	3,0	3,4
At jeg skal få virus på min datamaskin	3,2	3,6
At jeg skal bli lurt til å gi fra meg sensitiv informasjon	2,6	3,0

I følgende grafiske fremstilling betyr et større areal at risikoen oppfattes som større. Datapunktene er gjennomsnittsverdiene fra tabellen over.



Figur 12: Grafisk fremstilling av risiko-oppfattelse for vanlige digitale trusler. Tallene er signifikante, p<0,001. Phi ligger mellom 0,101 og 0,192. N=8200

Vi observerer at ungdommene generelt betrakter risiko for de ovennevnte truslene som lavere enn det som er vanlig i befolkningen generelt, med ett unntak. Ungdommene vurderer risikoen for hets og mobbing på nett like høyt som befolkningen forøvrig. En mulig årsak til dette er at nettmobbing både er relativt vanlig i de yngre aldersgruppene, og at det i tillegg har vært mye fokus på denne type hendelser hos de under 20 år. Merk at effektstørrelsen er lav for disse tallene.

Også her finner vi kjønnsforskjeller, der gutter generelt vurderer risiko knyttet til digitale trusler som lavere enn det jenter gjør.

I vår hovedstudie fra 2016 undersøkte vi hvilke faktorer som har sammenheng med en endring i risiko-oppfattelse. Mange opplæringstiltak og bevisstgjøringskampanjer har som ambisjon å øke mottakernes oppfatning av risiko gjennom å tilby informasjon og kunnskap om trusler og sårbarheter. Studien viste imidlertid ikke at det er en sammenheng mellom opplæring i informasjonssikkerhet, og endring i risiko-oppfattelse. De som har fått, og de som ikke har fått, opplæring vurderer risiko for de ovennevnte truslene likt.

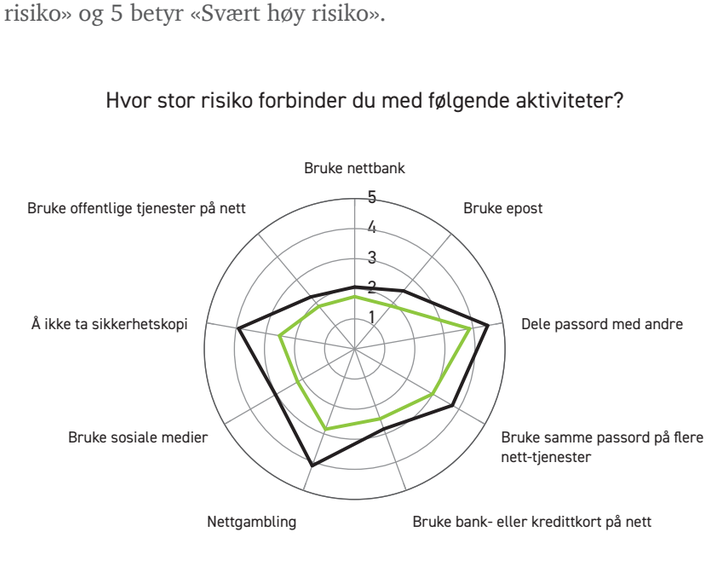
Figur 13: Kjønnsforskjeller for hvordan risiko oppfattes for digitale trusler. Tallene er signifikante, p<0,001. Phi ligger mellom 0,101 og 0,192. N=8200

Vi fant derimot en sammenheng mellom risiko-oppfattelse og troen på at en er i stand til å vurdere risikoene korrekt. Nærmere bestemt, dersom en tror at en er i stand til å vurdere risiko, er det en tendens at man vil vurdere risikoene som lavere. Ungdommene mener i høyere grad enn befolkningen generelt at de kan vurdere risiko (81,8 % vs. 61.1 %). Ungdommene har altså en høy «digital selvtillit», uten at den ser ut til å være fundert i noen objektive observasjoner av en reelt høyere evne til å vurdere digital risiko.

I følge SSB[24] har 96 % av alle nordmenn brukt internett i løpet av de siste tre månedene. Det finnes åpenbart et enormt mangfold i internettbaserte aktiviteter, der alle kan knyttes til risiko for brukeren. I vår hovedstudie fra 2016 valgte vi imidlertid ut noen internett-aktiviteter som vi mener er representative for de fleste norske innbyggere. Vi innser samtidig at det vil være enkelte forskjeller mellom ulike grupper i samfunnet. Yngre mennesker bruker trolig epost i mindre grad enn det som er vanlig i de eldre aldersgruppene. Vi mener likevel at personer i aldersgruppen under 20 år vet hva epost er, og at de har en oppfatning om risiko knyttet til bruken av det.

24: Statistisk sentralbyrå, *Bruk av IKT I husholdningene*, 2616, 2. kvartal. https://www.ssb.no/teknologi-og-innovasjon/statistikker/ikthus/aar

Vi spurte ungdommene hvor stor risiko de forbinder med de ulike internettbaserte aktivitetene på en skala fra 1 til 5, der 1 betyr «Svært lav risiko» og 5 betyr «Svært høy risiko».

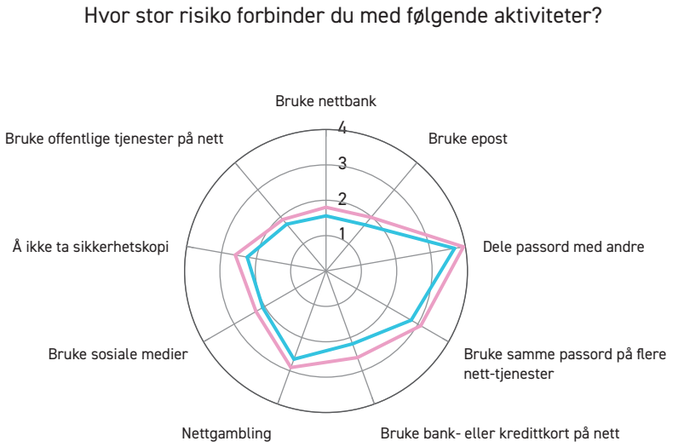


Figur 14: Grafisk fremstilling av risiko-oppfattelse for vanlige internettbaserte aktiviteter. Forskjellene mellom unge og voksne er signifikante, p<0,001. Phi ligger mellom 0,144 og 0,272. N=8227.

Vi observerer at ungdommene vurderer risikoen knyttet til egne internettbaserte aktiviteter lavere enn det som er vanlig for befolkningen forøvrig.

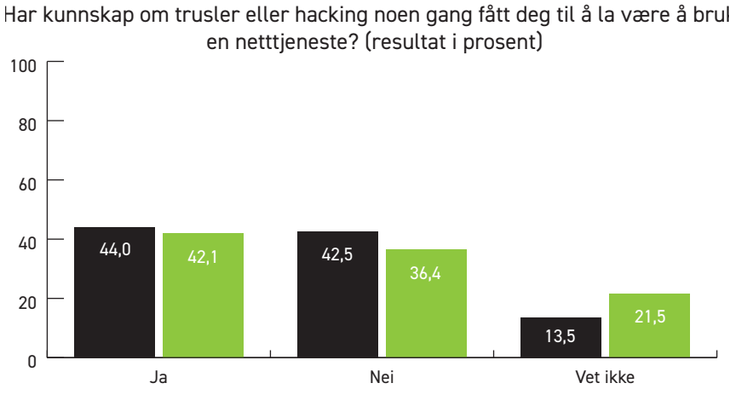
Det er også kjønnsforskjeller for dette spørsmålet. Generelt oppfatter gutter at det er lavere risiko knyttet til aktivitetene, enn det jenter gjør.

Vi finner ikke sammenheng mellom opplæring i informasjonssikkerhet, og endring i risiko-oppfattelse for vanlige internettbaserte aktiviteter. I hovedstudien fant vi en sammenheng mellom interesse for teknologi og IKT, og oppfatning av risiko knyttet til det å ikke ta sikkerhetskopi og det å bruke samme passord på flere nett-tjenester.



Figur 15: Kjønnsforskjeller for hvordan risiko oppfattes for nett-aktiviteter. Forskjeller mellom kjønn er signifikante, p<0,01 (merk at de ikke er signifikante på 0,001-nivå). Phi er mellom 0,151 og 0,226. N=772

Det er av interesse å vite hvordan de ser på risiko knyttet til ulik bruk av internett, fordi vi i hovedstudien avdekket at frykt for digitale trusler vil føre til en digital nedkjølingseffekt. Frykt for datakriminalitet kan føre til at folk avstår fra å bruke digitale tjenester.



Figur 16: Frykt for digitale trusler og digital nedkjølingseffekt. Forskjellen mellom unge og voksne er signifikante, p<0,001. Phi = 0,076. N=8164.

Vi observerer at ungdommene har latt være å bruke nett-tjenester i like stor grad som befolkningen forøvrig. Dette på tross av at de vurderer risiko som lavere for de ulike truslene og nettbaserte aktivitetene. Den digitale nedkjølingseffekten er med andre ord like sterk i denne aldersgruppen, som i resten av samfunnet.

Vurdering

Vi tolker ikke resultatene etter hvor «korrekte» de er. Risiko-oppfattelse er subjektivt av natur, og det er flere faktorer som kan og vil påvirke risikoene som vi undersøker i denne studien. Nettbankene kan oppfattes som sikre fordi vi «vet» at de har strenge sikkerhetsrutiner. Antakelsen om at banker er sikre kan påvirke vårt syn på risiko knyttet til nettbanker. På samme måte kan nett-gambling sees på som mer risikofylt fordi det er knyttet risiko til gambling i utgangspunktet.

Det er likevel nyttig å undersøke hvordan ungdommene oppfatter risiko, og hvordan den endrer seg over tid. Vi ser derfor denne studien som et utgangspunkt for digital risiko-oppfatning, og vi vil kunne oppdage trender ved å bruke samme metode over tid.

I hovedstudien i 2016 så vi at opplæring i informasjonssikkerhet ikke endrer hvordan folk oppfatter risiko. Dette er i motstrid til slik mange fagfolk ser på hensikten med slik opplæring. Tanken er at opplæring (overføring av kunnskap) om trusler og sårbarheter vil forbedre evnen til å vurdere risiko. En subjektiv risiko-oppfatning er imidlertid ikke basert på kalkulasjoner av fakta og faktorer. Personlige erfaringer, følelser og hendelser i nær fortid spiller en mye større rolle i slike vurderinger. Når opplæring ikke fører til en forbedret evne til å vurdere digital risiko så kan det skyldes at måten vi gir opplæring på ikke er hensiktsmessig, verken i form eller innhold.

Vår studie viser at det er en sammenheng mellom alder og risiko-oppfatning, og at folk generelt oppfatter digital risiko som høyere etterhvert som man blir eldre. Et sentralt spørsmål er hvorvidt ungdommene undervurderer digital risiko, og om det i så fall kan lede til at de tar større risiko enn de burde. For samfunnets digitaliseringstakt er den enkeltes risiko-oppfatning av betydning fordi mennesker som frykter digitale trusler avstår fra å bruke nett-tjenestene de opplever som utrygge. En studie[25] av *The US Department of Commerce National Telecommunications & Information Administration* støtter våre funn, og viser at mange amerikanere avstår fra å delta i viktige økonomiske og sosiale aktiviteter på nettet på grunn av bekymringer rundt personvern og digital sikkerhet.

42,1 % av ungdommene sier at de har latt være å bruke nett-tjenester pga. frykt for digitale trusler, samtidig som de generelt vurderer digital risiko lavere enn resten av befolkningen. Det er interessant å følge denne aldersgruppen over tid. Vil risiko-oppfattelsen endres etterhvert som den enkelte modnes og blir eldre? Vil det føre til en økning i den digitale nedkjølingseffekten for denne gruppen?

25: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

Risiko-oppfattelse ser ut til å være knyttet til hvordan folk tenker omkring deres egen evne til å vurdere hva som er trygt og utrygt på nett. Dette er et uttrykk for en digital selvtillit, noe ungdommene har mer av enn befolkningen forøvrig. Denne studien svarer ikke på hvorfor ungdommene har dette synet.

Adferdsmønstre

Introduksjon

Informasjonssikkerhetsadferd og adferdsmønstre har lenge vært gjenstand for både forskning og andre undersøkelser. Primært i bedrifter og organisasjoner. Motivasjonen er vanligvis å sørge for at ansatte følger de reglene som bedriften har fastsatt slik at sikkerhetshendelser som påvirker virksomheten kan unngås.

Norske bedrifter baserer sin risikostyring på ulike rammeverk, som for eksempel *ISO/IEC 27001/27002, COBIT, Sikkerhetsloven*[26], *Sikkerhetsnormen*[27] og mange andre eksterne eller interne informasjonssikkerhetsrammeverk og –policyer. Slike rammeverk er trolig ikke kjent for ungdommene ettersom de ikke brukes i familier eller skoleklasser. Likevel er ungdommene en del av det digitaliserte samfunnet. De er en del av vår nasjonale informa-

sjonssikkerhetskultur, og vi forventer at de skal ha en sikkerhetspraksis som gjør dem til trygge digitale innbyggere.

Om vi ser bort fra selve rammeverkene, er det ingen tvil om at fagekspertene innen informasjonssikkerhet promoterer visse adferdsmønstre som de mener er «sikre». Disse adferdsmønstrene kan sees på som normative, selv om de endrer seg over tid ettersom både bruken av teknologi og trusselen også endrer seg. I denne studien har vi valgt ut et sett med sikkerhetshandlinger som vi mener er gyldige for ungdommene. Disse er identitetskontroll og beskyttelse, trygg bruk av internett, netthygiene og sikring av digitale enheter, beskyttelse av personlig informasjon og bruk av sikkerhetsprogramvare.

Vi ønsker at ungdommene skal oppleve og bidra til en trygg digital hverdag. Vår studie viser at ungdommene ikke mottar like mye opplæring som voksne arbeidstakere, og at de vurderer digital risiko annerledes enn befolkningen forøvrig. Gir dette også utslag på deres adferdsmønstre innen informasjonssikkerhet?

Våre funn

Vi oppfordrer til å undersøke om nettsteder er trygge før man velger å bruke dem, og at man bør gjøre dette ofte fordi truslene endrer seg relativt hurtig. På tross av at ungdommene i langt større grad mener at de er i stand til å gjøre en slik vurdering, ser vi ingen signifikante forskjeller på om de gjør slike vurderinger eller ikke, sammenlignet med befolkningen forøvrig. Vi observerer at de som sier at de gjør slike vurderinger, gjør dette sjeldnere enn det som er vanlig i befolkningen.

I arbeidslivet er det vanlig at arbeidsgiver setter opp reglene for bruk av IKT på arbeidsplassen, og vi legger til grunn at det også er vanlig at skolene trekker opp regler for hva som er akseptabel bruk av IKT i skolen. Eksempelvis settes det noen steder opp regler[28] for *Itslearning*[29] som angår både informasjonssikkerhet og personvern. Det er opp til hver

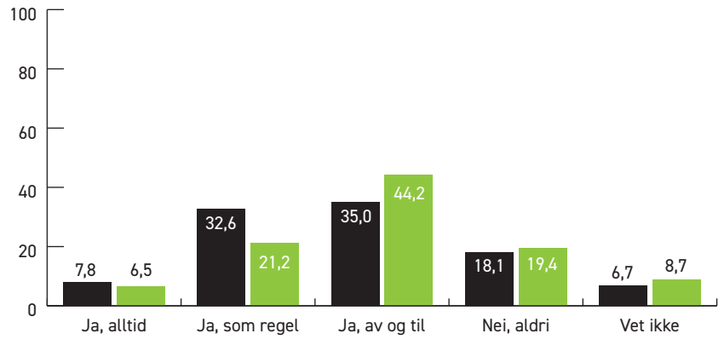
26: Lov om forebyggende sikkerhetstjeneste (LOV-1998-03-20-10)

27: Norm for informasjonssikkerhet, https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

28: https://onedrive.live.com/view.aspx?resid=36C72F58E6728093!218&ithint=file%2cdoc&app=Word&authkey=!AN_I00DyCuLundU

29: https://www.itslearning.com/

Undersøker du om en nettside er trygg før du bruker den? (resultat i prosent)



Figur 17: Ungdommenes vurdering om nettsteder er trygge. Forskjellene mellom unge og voksne er signifikante, p<0,001. Phi=0,087. N=8227.

skoleeier å trekke opp mer generelle regler for informasjonssikkerhet. Vi finner at 50,2 % av ungdommene kjenner til at skolen har regler for informasjonssikkerhet. Dette er vesentlig færre enn for ansatte i offentlig sektor, hvor 86,6 % sier at de kjenner til at arbeidsplassen har slike regler. Andelen ungdom som sier at de ikke vet om slike regler finnes er også langt høyere, 38,2 % mot 10,6 % blant ansatte i offentlig sektor. 54,4 % av de spurte ungdommene forteller at det er tillat å bruke private datamaskiner på skolen.

Selv om skolene fastsetter regler for informasjonssikkerhet, betyr ikke det at alle vil følge reglene hele tiden. Vi finner at 17 % av ungdommene som deltok i undersøkelsen sier at det hender at de bevisst bryter reglene. Vi kan ikke slå fast hvorfor de velger å bryte reglene, men vi antar at noe av forklaringen kan være at enkelte ser på reglene som unyttige eller til hinder for det de ønsker å gjøre. Det trenger med andre ord ikke være slik at den enkelte ikke, i utgangspunktet, har respekt for reglene eller den som har fastsatt dem, men at de opplever at reglene er til hinder for at de skal kunne utføre sine oppgaver på en effektiv måte.

Figur 18: Overholdelse av regler for informasjonssikkerhet. Forskjellen mellom unge og voksne, og mellom anstatte privat og offentlig, er signigikante, p<0,001. Phi (unge vs voksne) er 0,219 og for mellom anstatte privat og offentlig 0,181. N=8227

Det hender at jeg bevisst bryter regler for informasjonssikkerhet.	Ungdom, %	Ansatte privat sektor, %	Ansatte offentlig sektor, %
Ja	17,0	14,1	7,8
Nei	36,8	64,7	74,9
Vet ikke	46,2	21,2	17,3

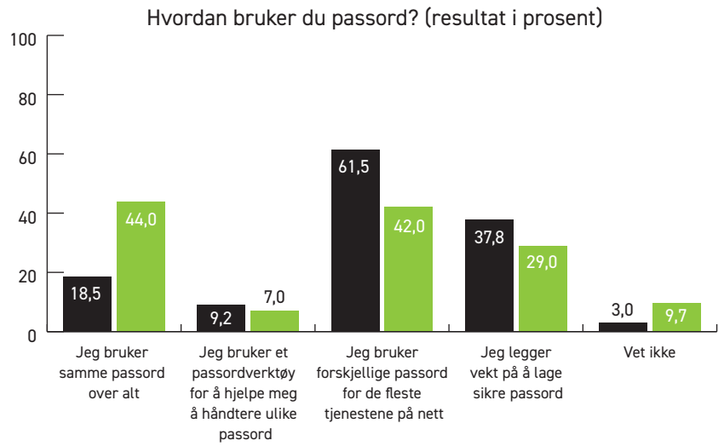
For dette spørsmålet registrerer vi en vesentlig kjønnsforskjell. Gutter oppgir å bevisst bryte reglene mer enn jenter, der henholdsvis 23,6 % og 11,1 % oppgir at de bryter reglene.

Passord

Å håndtere sin digitale identitet er en sentral del av den vi omtaler som en god sikkerhetspraksis. Selv om det finnes mange måter å håndtere sin digitale identitet, som for eksempel biometriske løsninger, benytter de fleste digitale tjenester fremdeles passord eller en kode for dette formålet. Identitetstyveri begås som en del av datakriminalitet, og vi ser ofte at passordet er det eneste som hindrer noen å begå kriminelle handlinger mot enkeltpersoner. Passord har vært en del av informasjonssikkerhet gjennom år-tier, men de representerer fortsatt en vesentlig utfordring for både sikkerhetsansvarlige og for den enkelte. Det britiske *Government Communications Headquarters (GHCQ)* og *UK Centre for the Protection of National Infrastructure* utga sine råd[30] i 2015, der de blant annet hevdet at britiske innbyggere i gjennomsnitt må forholde seg til 22 passord på nett. Dette er naturligvis langt fler passord enn folk flest kan huske, spesielt dersom en blir tvunget til å lage komplekse passord som skal skiftes med jevne mellomrom. Vi har ingen grunn til å tro at nordmenn må forholde seg til færre passord enn det britene må. Det må derfor være en balanse der en kan håndtere sine passord både effektivt og sikkert.

30: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf

Vår undersøkelse fokuserer på noen kjerneelementer for sikker bruk av passord. Vi finner at ungdommene som deltok i studien har en langt mer usikker bruk av passord enn det som er vanlig i befolkningen.



Figur 19: Passordbruk blant ungdommene. Forskjellene mellom unge og voksne er signifikante, p<0,01 (men ikke på 0,001-nivå). Phi varierer mellom 0,025 og 0,212. N=8227.

Vi finner at det er mer vanlig å gjenbruke passordene på flere nettsteder, og at ungdommene ikke legger like stor vekt på å lage sikre passord. Å bruke samme passord på de fleste nettsteder gjør det enklere å begå identitetstyveri, fordi et passord på avveie kan brukes mange steder. Studien kartlegger ikke hvorvidt en også bruker to-trinns verifisering (kodebrikke eller tilsvarende). Dersom det er tilfelle, er skadepotensialet ved å bruke samme passord over alt langt mindre.

Medietilsynets undersøkelse fra 2016[31] viser at totalt 19 % av barn i alderen 9–16 å svarer at de kjenner til passordet på sosiale medier til en

31: Medietilsynet. (2016). Barn & medier 2016. 9–16-åringers bruk og opplevelser av medier.

eller fere av vennene sine. Andelen er økende fra 13-årsalderen, både blant jenter og gutter. 25 % av guttene og 29 % av jentene i alderen 15–16 år kjenner til venners passord. Ser man på 14-og 16-åringene isolert, er det en høyere andel jenter enn gutter som kjenner til venners passord, mens det er små forskjeller mellom kjønnene blant 15-åringene.

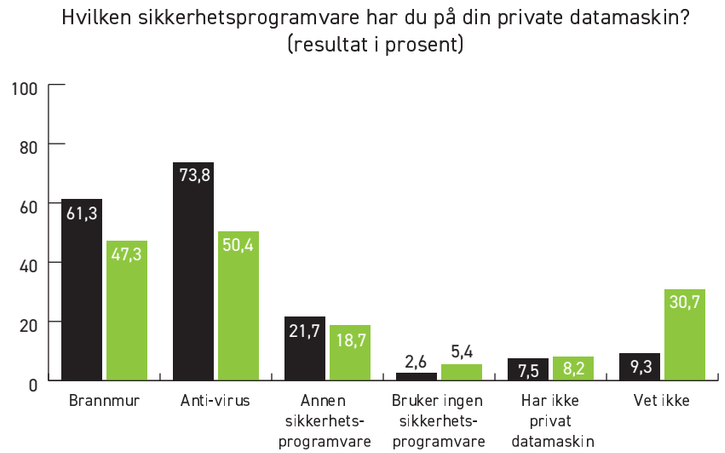
11 % oppgir at de selv har delt passordet sitt på sosiale medier med en eller flere av sine venner. Det er altså en lavere andel som sier de selv har delt passord enn som sier at de kjenner andre sine passord (differanse på åtte prosentpoeng).

Andelen som selv har delt passord er økende fra 13-årsalderen, både blant gutter og jenter. Samtidig er det et tydelig mønster at jenter i større grad enn gutter har delt sine passord til sosiale medier med venner. 24 % av jentene i alderen 15–16 år har delt passord med en eller ere av sine venner, mot kun 14 % av guttene i samme alder.

I vår hovedstudie fra 2016 avdekket vi at de som har interesse for teknologi og IT generelt har en sikrere passordbruk enn de som ikke er interessert. Vi fant også at de som har fått opplæring i informasjonssikkerhet i løpet av de to siste årene også har en sikrere passordbruk enn de som ikke har fått slik opplæring.

Sikkerhetsprogramvare

Sikkerhetsprogramvare er programmer som overvåker brukerens aktiviteter, eller som kjenner til digitale trusler, og som iverksetter tekniske sikkerhetsmekanismer på vegne av brukeren. De fleste kjenner til antivirus og brannmurer, men det finnes også en rekke annen sikkerhetsprogramvare som kan bidra til at brukeren har en tryggere bruk av nettet. Vi anbefaler at en bruker slike programmer i henhold til trusselnivået, og at en som et minimum bruker anti-virus og brannmur. I dag er det vanlig at slike programmer kommer ferdig installert nå en kjøper ny datamaskin, men det er ikke like vanlig for mobiltelefoner og nettbrett.



Figur 20: Bruk av sikkerhetsprogramvare. Forskjellene mellom unge og voksne er signifikante, p<0,01 for alle sammenligninger, bortsett fra for «Har ikke privat datamaskin». Phi ligger mellom 0,009 og 0,238.

Sammenlignet med befolkningen forøvrig, finner vi at ungdommene benytter seg av sikkerhetsprogramvare i mindre grad. Vi observerer også at det er en langt større andel som sier at de ikke vet om de bruker slik programvare.

I hovedstudien fant vi at interesse for teknologi og IT også her er en faktor som påvirker resultatene. De som har slik interesse bruker sikkerhetsprogramvare i langt større grad enn de som ikke har slik interesse. Når det gjelder opplæring i informasjonssikkerhet og bruk av slik programvare, fant vi i hovedstudien imidlertid ikke at det var noen forskjell mellom de som har fått opplæring, og de som ikke har fått det.

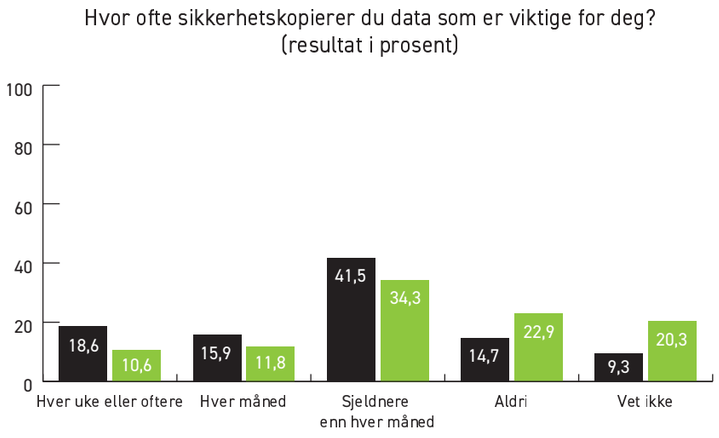
Beskyttelse av data

Nordmenn er generelt opptatt av personvern, og vi finner at 83,8 % av ungdommene sier at de vil slette personlig informasjon fra sine enheter før de selger eller kaster dem. 6,1 % sier at de ikke vil gjøre dette og 10,1 % sier at de ikke vet om de vil slette informasjonen.

En god sikkerhetspraksis innebærer å ha fokus på å beskytte informasjon mot uautorisert tilgang, manipulasjon eller at den skal være tilgjengelig når brukeren har behov for den. Noen digitale trusler, slik som løsepengevirus[32] kan gjøre informasjonen utilgjengelig for brukeren, og en sikkerhetskopi er i mange tilfeller det eneste virkemiddelet mot slike trusler.

Sammenlignet med befolkningen generelt, har ungdommene en svakere praksis rundt sikkerhetskopiering.

32: http://www.trendmicro.com/vinfo/us/security/definition/ransomware



Figur 21: Sikkerhetskopiering av viktige data. Forskjellene mellom unge og voksne er signifikant, p<0,001. Phi=0,156. N=8227.

Vurdering

I denne rapporten har vi valgt ut noen elementer av det vi anser for å være god sikkerhetspraksis. Vi anser praksisen for a være normativ, men vi er samtidig klar over at det vi anser for å være «best practice» også endrer seg over tid. Det er også slik at normene kan være forskjellige for ulike grupper. For eksempel: Vi anbefaler å sikkerhetskopiere viktige data hyppig, men dersom du ikke oppdaterer informasjonen oftere enn hver måned, gir det liten mening i å anbefale å ta sikkerhetskopi hver uke.

I vår hovedstudie fra 2016 så vi nærmere på noen av de underliggende faktorene i en god sikkerhetspraksis. Opplæring og interesse for teknologi og IT har en positiv innvirkning på sikkerhetspraksisen, dog ikke på alle områder.

Når det gjelder ungdommene som deltok i studien finner vi at de har en jevnt over svakere sikkerhetspraksis enn det som er tilfellet for befolkningen forøvrig. Dette er som forventet ettersom god sikkerhetspraksis har sammenheng med opplæring i informasjonssikkerhet, og fordi ungdommene ikke mottar opplæring i like stor grad som befolkningen forøvrig. Vi legger også merke til at kun 7 % av ungdommene sier at de lærer om informasjonssikkerhet av en ekspert, og at det trolig fører til at innholdet i opplæringen ikke holder tilstrekkelig kvalitet.

Vår studie evaluerer ikke deg faglige innholdet i de enkelte undervisningsopplegg, eller de læringsmetodene som blir brukt. Resultatene indikerer imidlertid at det er behov for å se nærmere på hvordan opplæring i informasjonssikkerhet gis til ungdom. Denne aldersgruppen er allerede digitale innbyggere, men har en tydelig svakere sikkerhetspraksis enn det som er vanlig i Norge.

Å følge reglene for informasjonssikkerhet er noe som både har betydning for den enkelte, og for de rund en. En kan ikke forvente at alle skal være eksperter, og holde seg oppdatert på trusselbildet og hva som er de mest effektive sikkerhetstiltakene akkurat nå. Vi må derfor forvente at folk flest forholder seg til de anbefalingene og reglene som ekspertene setter opp.

Det er imidlertid slik at ungdommene i mindre grad kjenner til at reglene eksisterer. En alternativ forklaring på dette er at det ikke er like vanlig å trekke opp regler for informasjonssikkerhet i skolene, eller at reglene faktisk ikke blir kommunisert til den enkelte.

Vi ser også at det er mer vanlig at ungdom bevisst bryter reglene. Her finner vi at det er kjønnsforskjeller når det kommer til spørsmålet om ungdom bevisst bryter reglene for informasjonssikkerhet. Jenter er generelt mer lojale i forhold til reglene enn det gutter er.

Kunnskap om hvordan en skal vurdere hva som er trygt å gjøre på nett er essensielt for å unngå svindel og annen nettkriminalitet

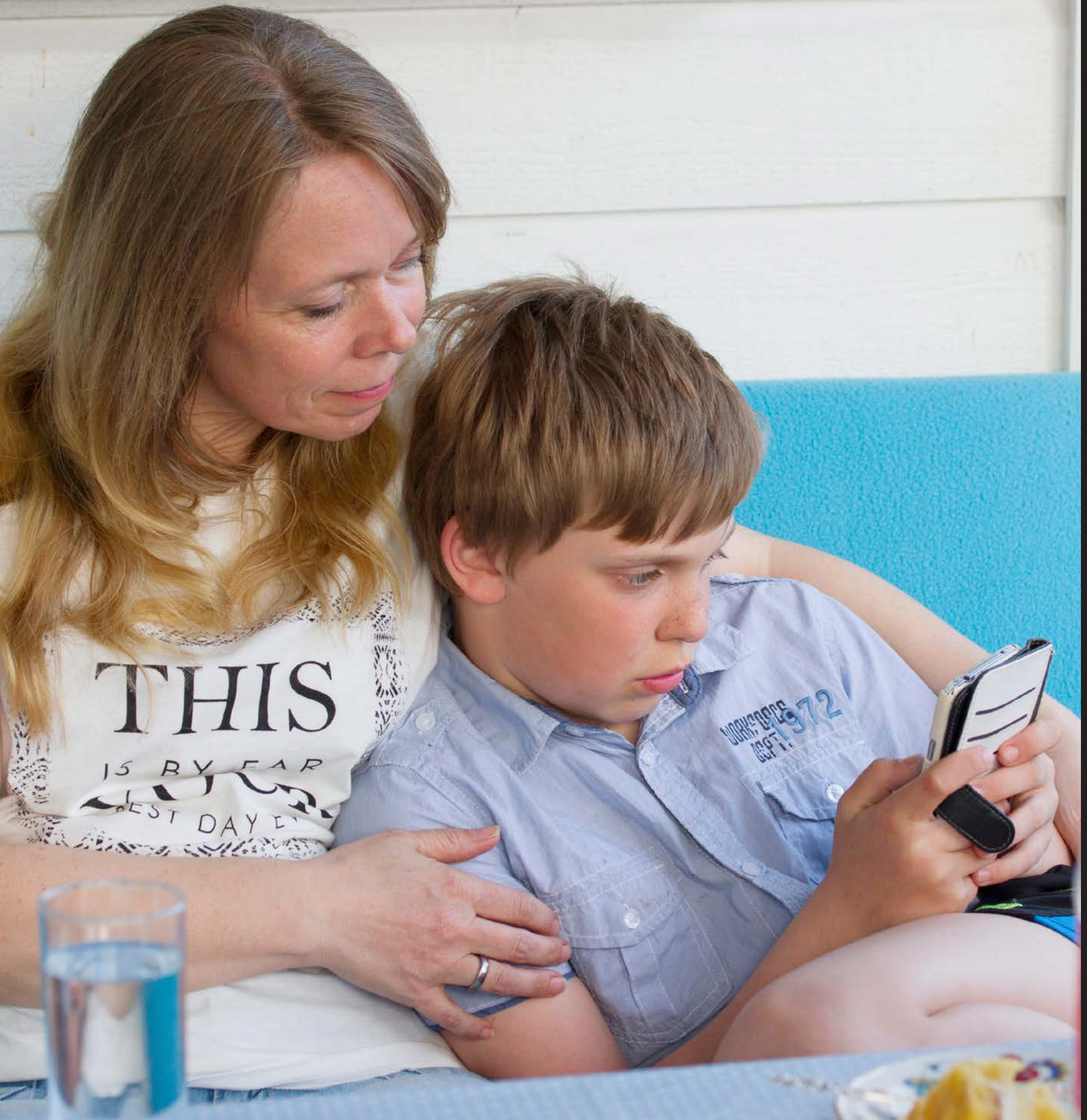
Trusselbildet er i konstant endring, og det som var trygt i går er ikke nødvendigvis trygt i dag. 81,8 % av ungdommene som deltok i studien sier at de føler seg i stand til å vurdere hva som er trygt å gjøre på nett. 19,4 % av ungdommene sier imidlertid at de aldri undersøker om en nettside er trygg før de bruker den. 8,7 % sier at de ikke vet om det gjør det eller ikke.

Mange teknologiske framskritt gjør det enklere, på noen områder, å være trygge på nett. Stadig flere digitale enheter kommer med krypterte filsystemer, noe som reduserer behovet for å slette data når enheten selges eller kastes. Apple, Google og Microsoft leverer digitale øko-systemer med integrerte løsninger for sikkerhetskopiering av dokumenter, bilder og musikk. Biometri kommer i tillegg til, eller overtar for, passord. Alle disse fremskrittene skaper utvilsomt et mer sikkert digitalt landskap,

men likevel så er datakriminaliteten økende[33]. Når nett-kriminelle får problemer med å angripe teknologien, skifter de fokus til å angripe menneskene som bruker den. Evnen til å vurdere hva som er trygt, og en praksis for å gjøre det, blir derfor mer viktig for å sikre alle en trygg digital hverdag.

Å sørge for at ungdommene blir utstyrt med nødvendige ferdigheter for å kunne gjøre dette, ser ut til å være et forsømt område.

33: http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/cybercrime.html



Hovedkonklusjon

I denne studien trekker vi i hovedsak frem to sammenligninger: Forskjellene mellom ungdom og befolkningen forøvrig, og forskjellene mellom gutter og jenter.

Kunnskapsnivået

Ungdommene som har deltatt i denne studien får lite opplæring i informasjonssikkerhet, sammenlignet med befolkningen forøvrig. Læringsmetodene er også annerledes for ungdommene, enn det de er for resten av befolkningen. Der 27 % av befolkningen oppgir at de lærer av eksperter, oppgir kun 7 % av ungdommene det samme. Dette gir grunn til bekymring fordi mye av praksisen omkring informasjonssikkerhet både kunnskapsbasert og «ferskvare». Trusselbildet endrer seg over tid, og det samme gjør beskyttelsestiltakene.

Dette krever at den enkelte får jevnlig påfyll av kunnskap om hvordan en skal sørge for at de er trygge på nett. Kun 6 av 10 sier at de vet hva informasjonssikkerhet er.

Norske ungdommer er blant de mest «digitaliserte» i verden, og de fleste bruker digitale plattformer til lek, læring og sosial omgang. Samtidig erfarer NorSIS at foreldregenerasjonen i for liten grad engasjerer seg i de unges digitale liv. Dette er uheldig fordi de unge trenger rollemodeller og veiledere som både kan trekke opp grenser, og som kan hjelpe dem å utvikle verdier og holdninger som bidrar til en trygg digital hverdag for alle. I tillegg til opplæring og forebygging, må det finnes sikkerhetsnett som kan hjelpe de unge når noe har gått galt. Her spiller både foreldre, skolen og samfunnet forøvrig viktige roller.

Vi observerer at ungdommene har en mindre sikker adferd på nett, og at de anser risiko på nettet for å være lav. Det er generelt mye usikkerhet i besvarelsene, de unge vet ofte ikke hva de kan, hvordan de lærer eller hva de gjør for å være trygge på nett. I sum er dette klare indikasjoner på at kunnskapsnivået er lavt i denne aldersgruppen.

Verdier og holdninger

Denne studien indikerer at ungdommene har en lavere fellesskapsfølelse når det gjelder digital sikkerhet enn befolkningen forøvrig, og at de er mer kritiske til overvåking av deres aktiviteter på nett. De har høyere tillit til at politiet vil hjelpe dem dersom de blir utsatt for kriminalitet på nett, men samtidig mener flere at aktivistgrupper har en rolle i kampen mot slik kriminalitet, sammenlignet med befolkningen forøvrig. Ungdom er opptatt av personvern, men har samtidig mye usikkerhet omkring kunnskap og ferdigheter som faktisk beskytter deres personopplysninger. Kun 4 av 10 sier at de har interesse for teknologi og IT.

Verdier og holdninger er viktige fordi de er underliggende faktorer som blant annet hjelper oss å forutse tendensene i handlings- og reaksjonsmønstre. Verdier og holdninger dannes tidlig i livet. Dette handler ikke bare om kunnskap og ferdigheter, men om grunnleggende verdier som tillit, fellesskap, trygghet, integritet og verdighet. Det er i samfunnets og den enkeltes interesse at alle innbyggere får tilbud om å ta del i vårt moderne samfunn på en trygg måte.

Holdninger og normer endrer seg, og nye grenser trekkes opp i forhold til hva som er lov og ikke lov. Rettsvesenet behandler saker der ungdom er involvert, både som offer og gjerningsperson. Spørsmålet er om ungdommene får med seg disse normendringene. Dommer som avsies i rettsvesenet skal ha en preventiv effekt, men har de dersom de unge ikke får høre om det? Hvem skal sørge for at det finnes rom for diskusjon og refleksjon omkring disse grunnleggende og prinsippielle tema?

Vi er allerede et digitalt samfunn, men vi har til en viss grad en foreldregenerasjon som har et dårlig utgangspunkt for en digital foresatt-rolle, og en skole som i for liten grad lærer ungdommene hvordan de skal ha et godt nettvett. Dette må det være et kontinuerlig fokus på i hele oppveksten. Vi er ikke tjent med at det blir utviklet et normsett i ungdomsgruppen som går på tvers av samfunnets normer.

Kjønnsforskjellen

Vi har i denne studien avdekket signifikante forskjeller mellom kjønnene. Gutter er mer interessert i teknologi og IT. Jenter lærer primært av sine venner, mens gutter lærer primært av seg selv. Gutter har større tro på egne ferdigheter enn det jenter har, men har samtidig større tro på at de selv skal gjøre noe feil. Jenter oppfatter ulike aktiviteter på nett som mer risikofyllte enn det gutter gjør.

Dette tyder på at det dannes kjønnsforskjeller tidlig i livet når det gjelder digital sikkerhet, men vi vet for lite om hvilke konsekvenser dette kan føre til senere. Tjenester som Slettmeg.no, ung.no og korspahalsen.no møter ungdom som opplever at noe har gått galt. Det kan være mobbing, hets eller at bilder og filmer blir delt mellom andre eller på digitale tjenester uten deres samtykke. Det finnes ingen undersøkelser som sier at

jenter rammes oftere enn gutter, men vi vet at det er langt flere jenter enn gutter som søker hjelp.

En mulig forklaring er at gutter har større interesse for teknologi og IT, og dermed oftere oppsøker kunnskap slik at de ikke opplever problemer i like stor grad som jenter. En annen forklaring kan være at gutter får problemer like ofte som jenter, men at det er mindre sosial aksept for at gutter skal søke hjelp for krenkelser på nett.

Denne studien viser at det er tildels store forskjeller mellom kjønnene når det gjelder digital sikkerhetskultur, men den gir ikke svar på hvorfor det er slik. Det er etter vårt syn behov for at det gjennomføres mer forskning på dette.

Anbefaling

Utdanningsmyndighetene må ta et større ansvar for at norske ungdommer blir trygge digitale innbyggere, og sørge for å utvikle mer kunnskap om ungdom og digital sikkerhetskultur.

Digital oppdragelse er både foreldre og skolens ansvar. Digital oppdragelse handler ikke bare om å forstå forskjellen på rett og galt, men alle de små og store tingene den enkelte må gjøre hver eneste dag for at de selv og de rundt en skal være trygge digitale innbyggere. For et samfunn som allerede er avhengig av digitale tjenester, og som i fremtiden skal gå gjennom ytterligere digitale transformasjoner, er dette av svært stor betydning. Dette er så viktig for samfunnet at vi ikke kan overlate det til mer eller mindre tilfeldig oppdragelse i det enkelte hjem. På samme måte som samfunnet

tar ansvar for at den enkelte skal ha holdninger, kunnskap og adferd som gir trygghet i trafikken, trenger vi at samfunnet tar et større ansvar for at alle skal være trygge på nett.

Dette bør skje strukturert, gjennom fag i skolen. Det må være en helhetlig tilnærming som har fokus på verdier, holdninger, normer, kunnskap og adferd – på sikkerhetskultur.

I dag er det i hovedsak bedrifter som sørger for opplæring i informasjonssikkerhet, men vi kan ikke forvente at ungdommene først skal bli trygge digitale innbyggere når de trer inn i arbeidslivet. Verdier og holdninger dannes tidlig i livet, og derfor må slik opplæring inn i skolesystemet på et tidlig tidspunkt. Informasjonssikkerhet og personvern er i noen grad tatt inn i læreplaner og utdanningsmål i skolen. Denne studien gir imidlertid grunn til å stille spørsmål ved om utdanningsmålene nås, og eventuelt om utdanningsmålene er ambisiøse nok. Utdanningsmyndighetene bør derfor ta initiativ til en større kartlegging av digital sikkerhetskultur blant unge for å avdekke om dagens tiltak og utdanning har ønsket effekt.

Det er mange som kommer i en digital oppdrager- eller veilederrolle for barn og ungdom. Lærere, helsepersonell, politi og ulike offentlige og private aktører, for å nevne noen. Disse må også ha tilstrekkelig kunnskap om de utfordringer som de unge møter på nett, og hvordan de skal veilede dem. En forutsetning for dette er at de selv har oppdatert kunnskap om informasjonssikkerhet. Utdanningsmyndighetene bør derfor ta initiativ til en gjennomgang av læreplanene for de som naturlig kommer i kontakt med ungdom omkring slike spørsmål, og sørge for at informasjonssikkerhet gis nødvendig prioritet. Det bør spesielt sees på utdanningen av lærere, helsepersonell og politi.

Skolene må gå foran som gode forbilder for de unge, og sørge for at alle barn og ungdommer får arenaer der de kan lære mer om hvordan de skal bli trygge digitale innbyggere.

Barn og unge tar ikke bare til seg kunnskap i skolen, de tar også til seg lærernes verdier og holdninger. Skolen er forbilder for de unge, men i følge Datatilsynets undersøkelse[34] er det grunn til å stille spørsmål ved om de er gode eller dårlige forbilder når det kommer til informasjonssikkerhet. Skolene må selv ha god sikkerhetspraksis, og de må selv utvikle normer og holdninger som bidrar til sikker nettbruk. Skoleeierne bør derfor sørge for god sikkerhetsstyring, og at den enkelte lærer og ansatt selv har holdninger og kunnskap som fremmer godt nettvett.

34: https://www.datatilsynet.no/Om-Datatilsynet/rapporter-og-utredninger/Personvern-i-skole-og-barnehage---samlerapport/

Den enkelte lærer bør sørge for at de unge ikke bare lærer minimumskravene i læreplanen, men også skape arenaer der de unge får anledning til å utvikle verdier, normer og holdninger. De bør ha fokus på kjønnsforskjellene der de er store, og bidra til at de unge får en økt forståelse for konsekvensene ved dårlig informasjonssikkerhet. Lærere er trolig best posisjonert for å sørge for at elevene gis en god mulighet til å ta del i vårt moderne samfunn, som trygge digitale innbyggere.

Spørreskjema

Takk for at du deltar i denne undersøkelsen om informasjonssikkerhetskultur. Resultatet fra undersøkelsen skal brukes til å gi råd om en tryggere digital hverdag for alle. Undersøkelsen tar 8–9 minutter. Besvarelsene er helt anonyme og kan ikke spores tilbake til deg.

Først vil vi vite litt om hvem du er.

1) * Kjønn

- ☐ Kvinne
- ☐ Mann

2) * Alder

- ☐ Under 15
- ☐ 15–19
- ☐ 20–25
- ☐ 26–35
- ☐ 36–45
- ☐ 46–55
- ☐ 56–65
- ☐ 66 og over

3) * Hva er ditt høyeste utdanningsnivå?

- ☐ Grunnskole
- ☐ Videregående skole
- ☐ Universitets- og høgskolenivå lavere grad
- ☐ Universitets- og høgskolenivå høyere grad
- ☐ Annet
- ☐ Ønsker ikke å svare

4) * Arbeider du i privat eller offentlig sektor?

- ☐ Privat
- ☐ Offentlig
- ☐ Er ikke i arbeid

5) * Hvor bor du?

- ☐ Østfold
- ☐ Akershus
- ☐ Oslo
- ☐ Hedmark
- ☐ Oppland
- ☐ Buskerud
- ☐ Vestfold
- ☐ Telemark
- ☐ Aust-Agder
- ☐ Vest-Agder
- ☐ Rogaland
- ☐ Hordaland
- ☐ Sogn og Fjordane
- ☐ Møre og Romsdal
- ☐ Sør-Trøndelag
- ☐ Nord-Trøndelag
- ☐ Nordland
- ☐ Troms
- ☐ Finnmark

6) Hvor mange ansatte er det i din bedrift?

- ☐ Under 10
- ☐ 11–25
- ☐ 26–50
- ☐ 51–100
- ☐ 101–250
- ☐ Over 250

7) * Hvilke radiostasjoner lytter du mest til?

(Du kan krysse av flere)

- ☐ NRK P1
- ☐ NRK P2
- ☐ NRK P3
- ☐ Radio Norge
- ☐ P4
- ☐ P5
- ☐ Radio 1
- ☐ Annet
- ☐ Lytter ikke på radio
- ☐ Vet ikke

8) * Hvilke nettaviser leser du mest?

(Du kan krysse av flere)

- ☐ Aftenposten
- ☐ VG
- ☐ Dagbladet
- ☐ Nettavisen
- ☐ Dagens Næringsliv
- ☐ Teknisk Ukeblad
- ☐ ComputerWorld
- ☐ Digi.no
- ☐ Wired
- ☐ SeHer.no
- ☐ Lokalaviser
- ☐ Andre
- ☐ Leser ikke nettaviser
- ☐ Vet ikke

Våre verdier påvirker våre holdninger og meninger. Vi spør derfor om hvilken partitilhørighet du har. Det er valgfritt å svare på dette, og vi minner om at undersøkelsen er helt anonym og kan ikke spores tilbake til den enkelte.

9) Hva ville du stemt dersom det var stortingsvalg i dag?

- ☐ Ønsker ikke å svare
- ☐ Arbeiderpartiet
- ☐ Fremskrittspartiet
- ☐ Høyre
- ☐ Kristelig Folkeparti
- ☐ Miljøpartiet De Grønne
- ☐ Senterpartiet
- ☐ Venstre
- ☐ Sosialistisk Venstreparti
- ☐ Rødt
- ☐ Annet parti
- ☐ Har ikke stemmerett
- ☐ Vet ikke

10) I denne delen stiller vi deg noen spørsmål om hvordan du ser på trygg nettbruk i et samfunn der teknologi blir stadig viktigere.

	Helt uenig	Delvis uenig	Delvis enig	Helt enig	Vet ikke
Jeg er positiv til å ta i bruk ny teknologi					
Jeg vet hva informasjonssikker-het er					
Jeg utsetter meg selv for risiko når jeg bruker internett					
Jeg synes at jeg får tilstrekklig informasjon om de truslene som finnes på internett					
Det er greit at min aktivitet på internett blir overvåket dersom det fører til at jeg blir tryggere på nett					

	Helt uenig	Delvis uenig	Delvis enig	Helt enig	Vet ikke
Politiet vil hjelpe meg dersom jeg blir utsatt for datakriminalitet					
Det bør være mulig å være anonym på internett					
Internett blir ikke tryggere selv om min datamaskin er sikker					
Jeg har tillit til at myndighetene sikrer informasjonen de har registrert om meg					
Aktivistgrupper (f.eks. Anonymous) har en rolle i kampen mot datakriminalitet og cyber-krig					

11) * Det hender at jeg bevisst bryter regler for informasjonssikkerhet

- ☐ Ja
- ☐ Nei
- ☐ Vet ikke

12) Føler du deg i stand til å vurdere hva som er trygt eller utrygt å gjøre på nett?

- ☐ Ja
- ☐ Nei
- ☐ Vet ikke

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

- ☐ Norske nettsteder er tryggere
- ☐ Utenlandske nettsteder er tryggere
- ☐ De er like trygge/utrygge
- ☐ Det avgjørende er om nettstedet er velkjent
- ☐ Vet ikke

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

- ☐ Hjemme
- ☐ På jobb eller på skolen
- ☐ Det er like viktig begge steder
- ☐ Det er ikke viktig noen steder
- ☐ Vet ikke

«Informasjonssikkerhet» er et begrep som viser til hvordan vi beskytter informasjon som er viktig for oss. I delen som kommer nå lurer vi på hvordan du forholder deg til ulike trusler.

15) * Hvor bekymret er du for at det følgende skal hende deg?

(1: Ikke bekymret for at dette skal skje. 5: Svært bekymret for at dette skal skje)

	1	2	3	4	5	Vet ikke
At mine bank- eller kredittkort skal bli misbrukt på nett						
At andre skal utgi seg for å være meg på internett						

	1	2	3	4	5	Vet ikke
At jeg skal bli hetset eller mobbet på nett						
At mine digitale dokumenter og bilder skal bli ødelagt						
At jeg skal få virus på min datamaskin						
At jeg skal bli lurt til å gi fra meg sensitiv informasjon						

16) * Hvor stor risiko forbinder du med følgende aktiviteter?

(1: Svært lav risiko. 5: Svært høy risiko)

	1	2	3	4	5	Vet ikke
Bruke nettbank						
Bruke epost						
Dele passord med andre						
Bruke samme passord på flere nett-tjenester						
Bruke bank- eller kredittkort på nett						
Nettgambling						
Bruke sosiale medier						
Å ikke ta sikkerhetskopi						
Bruke offentlige tjenester på nett						

17) * Hva er det sannsynlig at du vil gjøre dersom det følgende skjer deg?

	Ikke gjøre noe	Ordne opp selv	Få hjelp av en ekspert	Anmelde det til politiet	Vet ikke
Du blir hetset på internett					
Du blir utsatt for nettsvindel					
Du får virus på datamaskinen hjemme					
Du blir utsatt for ID-tyveri					

18) Har kunnskap om trusler eller hacking noen gang fått deg til å la være å bruke en nett-tjeneste?

☐ Ja

☐ Nei

☐ Vet ikke

19) Hva mener du er den største risikoen på nett?

☐ At du selv skal gjøre noe feil

☐ At noen andre skal gjøre noe mot deg (f.eks. hacke en nettside hvor du har lagt inn personlig informasjon)

☐ Vet ikke

Interesser, kunnskap og atferd henger gjerne sammen. Vi vil nå spørre deg om hva du er opptatt av, og hvordan du skaffer deg kunnskap om informasjonssikkerhet.

20) * Hvor interessert er du i teknologi og IT?

(1: Svært lite interessert. 5: Svært interessert)

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5
- ☐ Vet ikke

21) * Kan du mer eller mindre om informasjonssikkerhet i forhold til resten av befolkningen?

- ☐ Jeg kan mer enn gjennomsnittet
- ☐ Jeg kan mindre enn gjennomsnittet
- ☐ Jeg kan omtrent det samme som gjennomsnittet

22) * Hvem lærer du mest om informasjonssikkerhet av?

- ☐ Jeg lærer meg selv
- ☐ Eksperter
- ☐ Sjefer eller lærere
- ☐ Venner, kolleger eller klassekamerater
- ☐ Vet ikke

23) Hvordan lærer du vanligvis om informasjonssikkerhet?

- ☐ Prøver og feiler selv
- ☐ Kurs eller utdanning
- ☐ Hører om ting fra andre i en mer uformell situasjon
- ☐ Vet ikke

24) * Har du fått opplæring i informasjonssikkerhet i løpet av de siste to årene?

- ☐ Ja
- ☐ Nei
- ☐ Vet ikke

25) * Har arbeidsplassen eller skolen din regler for informasjonssikkerhet?

- ☐ Ja
- ☐ Nei
- ☐ Vet ikke

26) * Er det tillatt å bruke privat datamaskin på din arbeidsplass eller skole?

- ☐ Ja
- ☐ Nei
- ☐ Vet ikke

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

- ☐ Ja
- ☐ Nei
- ☐ Vet ikke

28) * Hvilken sikkerhetsprogramvare har du på din private datamaskin?

(Kryss av alle du bruker)

- ☐ Brannmur
- ☐ Anti-virus
- ☐ Annen sikkerhetsprogramvare
- ☐ Bruker ingen sikkerhetsprogramvare

- ☐ Har ikke privat datamaskin
- ☐ Vet ikke

29) * Undersøker du om en nettside er trygg før du bruker den?

- ☐ Ja, alltid
- ☐ Ja, som regel
- ☐ Ja, av og til
- ☐ Nei, aldri
- ☐ Vet ikke

For dette spørsmålet tenker vi primært på hvordan du bruker passord i privat sammenheng, ikke på jobb.

30) * Hvordan bruker du passord?

(Du kan krysse av flere)

- ☐ Jeg bruker samme passord over alt
- ☐ Jeg bruker et passordverktøy for å hjelpe meg å håndtere ulike passord
- ☐ Jeg bruker forskjellige passord for de fleste tjenestene på nett
- ☐ Jeg legger vekt på å lage sikre passord
- ☐ Vet ikke

For dette spørsmålet tenker vi primært på sikkerhetskopiering i privat sammenheng, ikke på jobb.

31) * Hvor ofte sikkerhetskopierer du data som er viktige for deg?

- ☐ Hver uke eller oftere
- ☐ Hver måned
- ☐ Sjeldnere enn hver måned
- ☐ Aldri
- ☐ Vet ikke

32) * Hvis du skulle selge eller kaste en privat datamaskin, ville du da sørget for at alle personlige data blir slettet?

- ☐ Ja
- ☐ Nei
- ☐ Vet ikke

33) * Har du rutiner for å oppdatere operativsystemene og programmene på din private datamaskin?

- ☐ Oppdateringene skjer automatisk
- ☐ Jeg oppdaterer med én gang de er tilgjengelige
- ☐ Jeg har ingen rutiner for å oppdatere
- ☐ Vet ikke

34) Har du kommentarer eller innspill til denne undersøkelsen?

Teknologiveien 22
2815 Gjøvik
Org.nr: 995 195 003

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