NORDMENN OG DIGITAL SIKKERHETSKULTUR

NorSIS
Norsk senter for informasjonssikring

Nordmenn
og digital sikkerhetskultur

Innhold


Windows Update
Oppdater status
Se etter oppdateringer
Oppdateringsinnstillinger
Har du spørsmål?
Få hjelp
Gjør Windows bedre.
BenQ

Innledning

NorSIS publiserte i 2016 en rapport om den norske informasjonssikkerhetskulturen[1]. Forut for dette tildelte Justis- og beredskapsdepartementet midler til å utvikle en metode for kartlegging av sikkerhetskultur på et nasjonalt nivå for å lære mest mulig om hvordan disse forholder seg til informasjonssikkerhet i en digital hverdag.

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

I 2017 fulgte NorSIS opp med rapporten Ungdom og digital sikkerhetskultur[2], der vi undersøkte kunnskap, holdninger og adferd til digital sikkehet for de under 20 år. Datagrunnlaget til denne rapporten ble innhentet i forbindelse med studien i 2016.

2: https://norsis.no/ungdom-digital-sikkerhetskultur/

Kunnskap om digitale trusler og hvordan man best beskytter seg mot slike endrer seg over tid. Kryptovirus og direktørsvindel er eksempler på trusler som har økt i omfang de siste årene, og kunnskap om hvordan man skal gjenkjenne slike angrep, og unngå å bli rammet er også til en viss grad ny kunnskap. Vi gir nye råd om god passordbruk enn det vi gjorde før, men i hvor stor grad har befolkningen fått med seg dette?

Digitaliseringen gjennomsyrer hele samfunnet og dette skaper nye diskusjoner og nye problemer. I løpet av det siste året har vi hatt en nasjonal debatt om hvorvidt myndighetene skal få etablere et digitalt grenseforsvar. Store hendelser, som for eksempel Wannacry, har fått stor oppmerksomhet i media. Hvordan endrer slike diskusjoner og hendelser innbyggernes oppfattelse omkring digital sikkerhet? Endrer tilliten til digi-

tale tjenester seg over tid? Blir innbyggerne mer eller mindre bekymret for sin sikkerhet på nett? Øker kunnskapen i befolkningen om hvordan man skal være trygge på nett?

Svaret på slike spørsmål kan vi kun få dersom vi jevnlig kartlegger den digitale sikkerhetskulturen i befolkningen. Utviklingstrender er ny kunnskap, og den er helt nødvendig for at myndighetene og andre beslutningstakere skal kunne utvikle gode strategier for å sørge for at alle i Norge kan være trygge på nett.

Årets rapport er utarbeidet med støtte fra Nasjonal Sikkerhetsmyndighet.

Direktør NorSIS

Samfunnets og nasjonens egenevne til å beskytte seg er avhengig av at både offentlige og private virksomheter, samt at privatpersoner har tilstrekkelig IKT-sikkerhetskompetanse. Samfunnet forventer at den enkelte skal klare å beskytte seg selv, og bidra til å beskytte andre. Det betyr at alle må vite hva man skal gjøre, og hva man ikke skal gjøre. Dette er enklere sagt enn gjort, for kompleksiteten øker og stadig nye områder digitaliseres. Digital sikkerhet gjelder alt fra husholdningsapparater og leker til medisinsk utstyr. Hva som er «gode sikkerhetsvaner» endrer seg også over tid. Sikker bruk av passord er et eksempel på dette. Dette kommer som en følge av at bruken av passord øker, og at vi har ny kunnskap om hvordan mennesker klarer å forholde seg til disse.

Regjeringen vil legge til rette for en langsiktig oppbygging av IKT-sikkerhetskompetanse gjennom en nasjonal kompetansestrategi for IKT-sikkerhet. Regjeringen sier i den forbindelse at IKT-sikkerhet gjelder alle. De unge skal lære tidlig trygg bruk og forstå nødvendigheten av IKT-sikkerhet. Slik skal det legges et grunnlag for at den oppvoksende generasjonen har med seg IKT-sikkerhetskompetanse inn i det videre utdanningsløpet og senere i arbeidslivet. Dette arbeidet er meget viktig fremover.

Dagens digitale samfunn fordrer at alle har et minimum av kunnskap om informasjonssikkerhet. Interesse og læring går hånd i hånd. Hvilke konsekvenser kan det medføre at noen er lite eller veldig lite interessert i å lære seg å ferdes trygt digitalt?

NorSIS har spurt nordmenn om deres sikkerhetsholdninger, -kunnskap og -atferd på nett. Det er viktig å vite hvordan befolkningen og virksomheter forholder seg til digitalisering og opplæring innen informasjonssikkerhet.

Det er i hovedsak bedrifter og virksomheter som gir opplæring, de yngre, de eldre og de uten arbeid stiller svakere i et digitalt samfunn. Dette er grunn til bekymring, for digitaliseringen av samfunnet berører alle. Samfunnet forventer av den enkelte at man i det minste har noen basisferdigheter slik at man kan bruke digitale tjenester på en trygg måte.

Samfunnet kan ikke bære risikoen det er å ikke sørge for at befolkningen er i stand til å beskytte seg mot digitale trusler når vi samtidig digitaliserer alle områder av livene våre.

Samarbeid på tvers av sektorer er nødvendig for å lykkes med å heve kompetansen vi så sårt trenger for å beskytte oss og våre verdier i det digitale samfunnet. Dette er en forutsetning for at alle kan bidra i på likt nivå i et digitalt samfunn og ha samme forutsetninger for å kunne ha et trygt digitalt liv.

Peggy Sandbekken Heie
Administrerende direktør
NorSIS

Metode

Digital sikkerhetskultur er et komplekst område, og flere av mekanismene som påvirker den er drøftet i hovedstudien.

En vesentlig endring i innhentingen av datagrunnlaget er at årets undersøkelse baserer seg helt på data innhentet i en befolkningsundersøkelse utført av YouGov, mens undersøkelsen i 2016 både omhandlet data innhentet av YouGov i 2015, i tillegg til data fra 36 virksomheter i Norge i 2016. Endringen i metoden for datainnhenting innebærer at vi ikke gjør en omfattende sammenligningsstudie med resultatene fra 2016. Der sammenligninger gjøres er det kun mellom befolkningsundersøkelsene i 2015 og 2017.

I denne rapporten brukes informasjonssikkerhetskultur og digital sikkerhetskultur som synonymer.

Indikatorer på digital sikkerhetskultur

Indikatorene for digital sikkerhetskultur er utviklet som en del av hovedstudien, hvor de ble utformet som et elektronisk spørreskjema på norsk og engelsk.

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. Det er gjort noen mindre språklige til-

passinger i årets indikatorer for å forbedre forståelsen til spørsmålene. Noen spørsmål som omhandlet spesifikke forskningsspørsmål i 2016-undersøkelsen er fjernet, og det er lagt til noen spørsmål for å fange opp spesifikke sider ved sikker adferd.

Indikatorene er gjengitt i vedlegg A.

Analyse

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


NACKS
SNA

Den Norske digitale sikkerhetskulturen

Beskrivelse av digital sikkerhetskultur: 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 befolkningens digitale sikkerhetskultur.

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 befolkningen 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 befolkningens digitale sikkerhetskultur? 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 betyr 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[3].

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*[4 5]» . 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*».

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

Digital sikkerhet i befolkningen

I det følgende beskriver vi hva som karakteriserer den digitale sikkerhetskulturen i befolkningen. Vi benytter en kvalitativ analyse der en rekke indikatorer sammen bidrar til en vurdering av den enkelte av de 8 dimensjonene. Vedlegg B beskriver sammenhengen mellom indikatorer og dimensjoner.

Fellesskap

En del av det digitale fellesskapet er hvorvidt den enkelte forholder seg til fellesskapets normer og regler. I synet på overvåking og kontroll er flertallet enige i påstanden *Det er greit at min aktivitet på internett blir overvåket dersom det fører til at jeg blir tryggere på nett*. 56% av befolkningen er enten helt eller delvis enige i dette. I spørsmålet ligger det en forutsetning om at det å gi fra seg noe privatliv her skjer under forutsetning om at den enkelte skal være tryggere på nett. Spørsmålet om anonymitet er beslektet, og her sier imidlertid 64% seg helt eller delvis enige i at *Det bør være mulig å være anonym på internett*. En annen side ved dette er hvorvidt den enkelte aksepterer samfunnets normer for hvem som lager reglene, og hvem som håndhever dem. Hele 62% er helt eller delvis enig i påstanden *Privatpersoner og aktivistgrupper (f.eks. Anonymous) har en rolle i kampen mot datakriminalitet og cyber-krig.* Det legges til at 27% sier at de ikke vet.

En annen vinkling er om den enkelte ser seg selv som ansvarlig for trygghet på nett. Forståelsen av at ens egne datamaskiner kan forvolde skade på nett krever både kunnskap, og en forståelse for sammenhenger og årsaksforhold. 85% sier seg helt eller delvis enige i påstanden *Internett blir tryggere når min datamaskin er sikker*.

11% av befolkningen sier at det hender at de bevisst bryter regler for informasjonssikkerhet. Her observerer vi en signifikant forskjell mellom kvinner og menn, der de svarer henholdsvis 7% og 14% på dette. Det er også aldersforskjeller. De yngre aldersgruppene (18-35) bryter reglene vesentlig mer enn de eldre (55+), henholdsvis 17% or 3%. Vi finner derimot ingen signifikante forskjeller mellom ulike utdanningsnivåer.

Styring og kontroll

En side ved befolkningens syn på digital styring og kontroll, er synet på overvåking av ens egen aktivitet på nett. Som nevnt over mener 56% prosent at dette er greit, forutsatt at det fører til at de blir tryggere på nett. Det er også verdt å merke seg at 6% sier at de ikke vet hva de mener om dette. Synet på hvorvidt det skal være mulig å være anonym på nett, altså å kunne unndra seg visse former for styring og kontroll er også nevnt over. Også her mener 6% at de ikke vet hva de mener om dette.

I befolkningen sier 44% seg helt eller delvis enige i påstanden *Politiet vil hjelpe meg dersom jeg blir utsatt for datakriminalitet*. Det er samtidig 13% som sier seg helt uenige i denne påstanden, mens 25% sier seg delvis uenig. Styring og kontroll vil i mange tilfeller dreie seg om inngripende metoder og maktbruk overfor den enkelte. Befolkningens tillit til politiet er derfor av stor interesse. I sammenheng med dette må vi også betrakte befolkningens syn på hvorvidt privatpersoner og aktivister skal ha en rolle i kriminalitetsbekjempelse. Som beskrevet over mener hele 62% at disse har en slik rolle.

Etterlevelse av regler er også en del av dette bildet, og som nevnt over sier 11% at de noen ganger bryter reglene for informasjonssikkerhet. NorSIS erfarer at det er forskjeller mellom ulike virksomheter og bedrifter, og at noe av dette kan forklares med at noen legger mer vekt på å forklare betydningen av reglene enn det andre gjør. Vi er også kjent med at mange opplever, noen ganger med rette, at reglene er uhen-

siktsmessige og til skade for produktivitet og effektivitet. 41% av de som er i arbeid sier at de er kjent med at deres arbeidsplass har slike regler. 15% sier at de ikke vet om arbeidsplassen har slike regler.

Vi er også opptatt av om den enkelte vil oppsøke hjelp fra de som er satt til å håndheve kriminalitetsbekjempelse på nett. Hets, nettsvindel og ID-tyverier kan være ulovlig, og noe som bør etterforskes av politiet. I befolkningen svarer 28% av de vil kontakte politiet dersom de blir utsatt for hets på internett. Når det gjelder nettsvindel og ID-tyverier, svarer henholdsvis 68% og 80% det samme.

Tillit

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

Vi har allerede sett på befolkningens syn på overvåking, anonymitet og kontroll. Tilliten til at politiet skal hjelpe en er relativt lav (44%), men det er også verdt å legge merke til at langt de fleste sier at de vil be politiet om hjelp dersom de blir utsatt for nettsvindel eller ID-tyveri.

Overraskende svarer 28% av befolkningen at de anser norske nettsteder som tryggere enn utenlandske. 2% svarer at de anser utenlandske som tryggere. Her svarer også 32% at de mener at norske og utenlandske nettsteder er like trygge/utrygge, altså at nasjonalitet ikke spiller noen rolle. 27% mener at det er avgjørende om nettstedet er velkjent.

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.

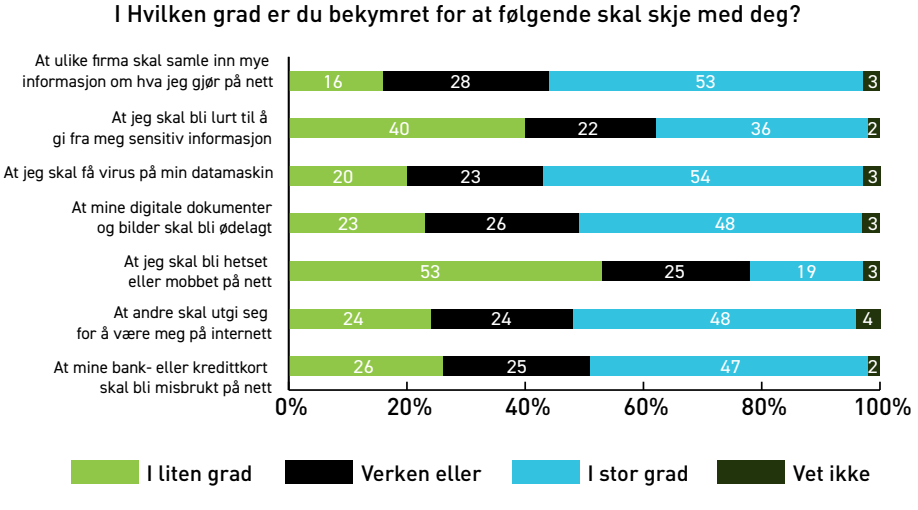
3 av 4 mener at de utsetter seg for risiko når de er på nett

75% av befolkningen er enten helt eller delvis enig i påstanden *Jeg utsetter meg selv for risiko når jeg bruker internett*. Samtidig sier 65% seg helt eller delvis enig i påstanden *Jeg synes at jeg får tilstrekkelig informasjon om de truslene som finnes på internett*. 29% sier seg helt eller delvis uenig i denne påstanden, mens 6% sier at de ikke vet. Vi observerer her ingen forskjell mellom kjønnene eller de ulike aldersgruppene.

58% av de spurte sier at de er i stand til å vurdere hva som er trygt og utrygt på nett, mens 26% sier at de ikke er det. 16% sier at de ikke vet. Vi finner her en forskjell mellom aldersgruppene der 68% av de som er mellom 18–34 sier at de er i stand til å vurdere dette, mens kun 44% av de som er 55 og over sier det samme.

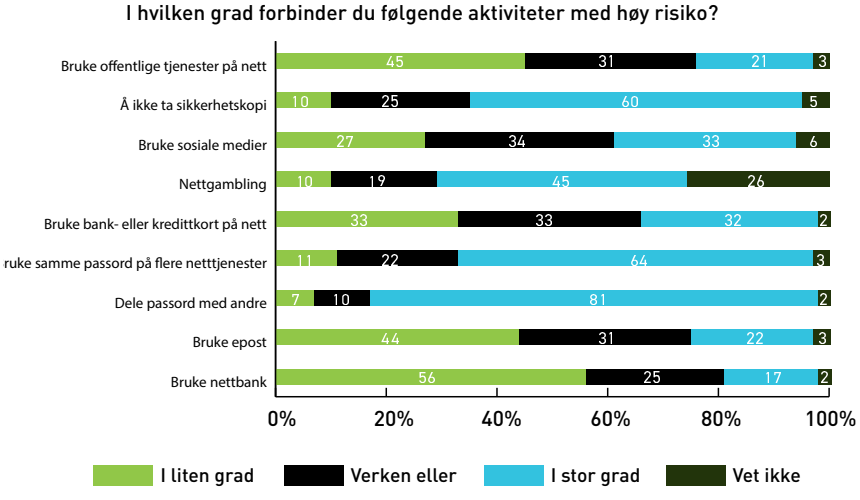
At 71% mener at det er like viktig å tenke på informasjonssikkerhet både hjemme og på jobb er også en indikator på risikooppfattelsen i befolkningen. Vi observerer her at det er flere (15%) som mener at det er viktigst hjemme, mens 6% mener at det er viktigst på jobb eller på skolen.

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



Figur 1: I hvilken grad frykter befolkningen trusler på nett

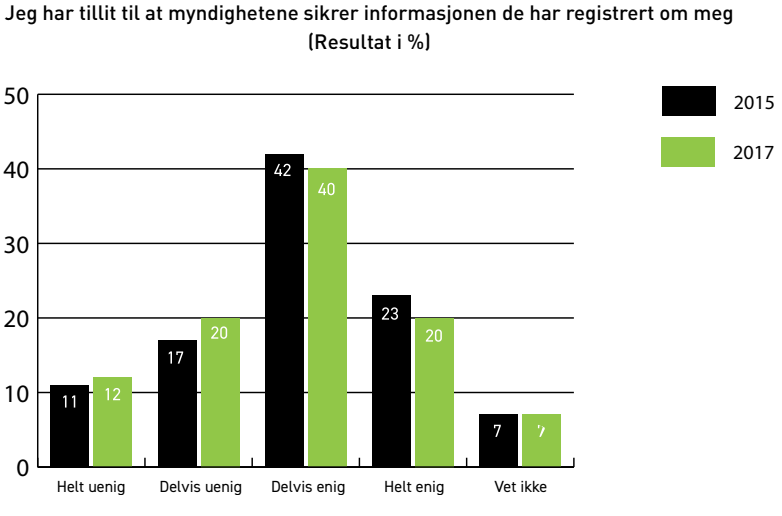
Vi spør også i hvilken grad befolkningen forbinder en del vanlige nett-aktiviteter med høy risiko.



Figur 2: I hvilken grad forbinder befolkningen vanlige nett-aktiviteter med høy risiko

Befolkningens risiko-oppfattelse for det å bruke offentlige tjenester på nett har endret seg siden vi undersøkte dette i 2015. Den gang svarte 13% at de anså risikoen ved bruk av offentlige tjenester på nett å være enten ganske stor eller svært stor. I 2017 svarer 21% det samme. Vi observerer med andre ord en økning i en slik frykt i befolkningen. Tilsvarende øker frykten for bruk av nettbank i den samme perioden. I 2015 svarte 10% at de anså risikoen ved bruk av nettbank å være ganske stor eller svært stor, mens i 2017 svarer 17% det samme.

Dersom vi ser på endring i befolkningens tillit til at myndighetene sikrer informasjon som de har om den enkelte, observerer vi en redusert tillit til dette i befolkningen generelt.



Figur 3: Hvor stor tillitt befolkningen har til at myndighetene sikrer informasjonen de har om den enklete

Som tidligere nevnt er tillit en forutsetning for at vi skal utnytte de muligheter som digitaliseringen presenterer. På samme tid kan frykt

for digitale trusler redusere tilliten og føre til at den enkelte lar være å bruke digitale tjenester. På spørsmålet *Har kunnskap om trusler eller hacking noen gang fått deg til å la være å bruke en nettjeneste*, svarer 33% Ja. 51% svarer Nei til dette, mens 16% sier at de ikke vet. Frykt for trusler på nett blir da en motvekt til digitaliseringsarbeidet, og kan føre til en nedkjølingseffekt, altså at folk avstår fra å bruke nettjenester. Bekjempelse av datakriminalitet og opplæring i trygg nettbruk er tiltak som trolig kan motvirke dette i noen grad.

Vi er også interessert i å vite om den enkelte ser på seg selv eller andre som den største risikoen på nett. Dette kan kanskje tolkes som et uttrykkt for ens egen selvtillit når det gjelder digital sikkerhet. På spørsmålet *Hva mener du er den største risikoen på nett?* sier 19% at de frykter at de selv skal gjøre noe feil, mens 72% sier at de frykter at noen andre skal gjøre noe mot dem. 9% sier at de ikke vet. Vi observerer noen kjønnsforskjeller på dette spørsmålet. 23% av menn frykter at de selv skal gjøre noe feil, mens 14% av kvinner mener det samme.

Risikooppfattelse må også sees i sammenheng med den digitale sikkerhetsadferden. Dette blir belyst i et senere avsnitt.

Vilje til digitalisering

Befolkningen er generelt svært positiv til å ta i bruk ny teknologi. 90% sier at de er helt eller delvis enig i påstanden *Jeg er positiv til å ta i bruk ny teknologi*, mens 8% er helt eller delvis uenig. Samtidig sier 48% av befolkningen at de er ganske eller svært interessert i teknologi og IT. 25% sier at de er ganske lite eller svært lite interessert i dette. Også her observerer vi forskjeller mellom kjønnene, der flere menn enn kvinner sier at de er interessert i teknologi og IT.

Kompetanse

Nordmenn er generelt kunnskapsrike når det kommer til informasjonssikkerhet. De ser også på seg selv som relativt kunnskapsrike, og mener at de kan gjøre riktige vurderinger for sin sikkerhet på nett.

Imidlertid er det kun 21% av de spurte som sier at de har fått opplæring i informasjonssikkerhet i løpet av de to siste årene. 72% sier at de ikke har fått opplæring, mens 7% sier at de ikke vet. På tross av dette har flertallet av de spurte tro på egne ferdigheter. 58% mener at de er i stand til å vurdere hva som er trygt eller utrygt å gjøre på nett.

76% mener at de har fått bedre ferdigheter etter slik opplæring, mens 17% mener at de ikke har fått det.

Nordmenn har høy digital selvtillit

Generelt mener nordmenn at de kan like mye eller mer enn gjennomsnittet, når det kommer til informasjonssikkerhet. I befolkningen mener 51% at de kan omtrent det samme som folk flest, mens 26% mener at de kan mer en gjennomsnittet. 15% mener at de kan mindre enn gjennomsnittet, og 7% sier at de ikke vet.

På spørsmålet *Hvem lærer du mest om informasjonssikkerhet av?* oppgir kun 18% at de lærer av eksperter. Langt flere lærer av seg selv (34%) eller av venner og kolleger (31%). 13% sier at de ikke vet hvem de lærer mest av.

På spørsmålet *Hvordan lærer du vanligvis om informasjonssikkerhet?* oppgir hele 50% at de hører om ting fra andre i en mer uformell situasjon, mens kun 17% sier at de lærer på kurs eller utdanning. 21% sier at de vanligvis prøver og feiler selv.

Interesse

Som tidligere nevnt forteller nesten halve befolkningen (48%) at de har en interesse for teknologi og IT, mens 25% sier at de er ganske lite eller svært lite interessert i dette. Også her observerer vi forskjeller mellom kjønnene. Flere menn enn kvinner (19% vs 7%) sier at de er svært interessert i teknologi og IT, mens flere kvinner enn menn (10% vs 3%) sier at de er svært lite interessert.

Adferdsmønstre

71% forteller at de undersøker om en nettside er trygg før de bruker den, og 21% sier at de aldri gjør dette. Merk at 58% mener at de er i stand til å vurdere hva som er trygt eller utrygt å gjøre på nett.

NorSIS erfarer at sikker bruk av passord er krevende for mange. Tidligere var det vanlig å gi råd om passord som vi i dag tror er skadelig for sikkerheten. Kravene om at passordene skal være bygget opp av tilfel-

dige bokstaver, tall og spesialtegn (RyDH5#33) og at de må skiftes med jevne mellomrom, fører til at mange bruker det samme passordet over alt. Slike passord er vanskelige å huske for mennesker, og paradoksalt nok ganske lette for en datamaskin å bryte. I dag gir vi råd om å bruke lange passord som er lette å huske (strofe fra en bok eller sang), gjerne med en tilpassing til det enkelte nettsted slik at det er mulig å velge forskjellige passord på de fleste nettsteder. Et annet, og kanskje enda viktigere, råd er å skru på to-trinns verifisering der det er mulig. Da vil det ikke være mulig å logge seg inn på nett-kontoen, selv om passordet har kommet på avveie.

Imidlertid er det kun 29% av befolkningen som sier at de bruker to-trinns verifisering der det er mulig. Vi ser her forskjeller mellom kjønnene, der 34% av menn og 23% av kvinner sier at de gjør dette. Det er også en forskjell mellom noen aldersgrupper, der de over 55 er dårligst på dette (21% mot ca 32% i de øvrige aldersgruppene).

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

42% av de spurte sier at de legger vekt på å lage sikre passord.

18% sier at de ikke har noen rutiner for å oppdatere programvare, og 8% sier at de ikke vet om de har slike rutiner. 49% sier at oppdateringene skjer autmatisk, og 25% sier at de oppdaterer selv med én gang oppdateringene er tilgjengelige. NorSIS erfarer at det pågår et skifte når det gjelder sikkerhetsoppdatering av programmer og enheter. De fleste større systemer (mobiltelefoner, nettbrett, operativsystemer (f.eks. Windows, Mac og Linux) og større programvare begynner å få gode løsninger for automatisk oppdatering. Det betyr at brukeren i liten grad trenger å tenke på det. Enten blir systemene oppdatert uten noen handlinger fra brukeren, eller så får man et varsel der den enkelte kun trenger å godta for at oppdateringen skal skje.

Samtidig er det en eksplosjon av nye typer enheter og systemer som kobles til nettet, de såkalte «Internet of Things». Hvitevarer, TV'er, lyspærer, dørlåser, leker m.m. trer inn i de tusen hjem. I følge Gartner Group[6] vil det være 8.3 milliarder slike enheter på nett i 2017. I 2020 spår de at antallet vil ha passert 20 milliarder. Foreløpig ser vi at svært mange av disse systemene og enhetene ikke har like gode løsninger for oppdatering av kode. Dette betyr at dersom brukeren ikke selv tar aktive steg for å oppdatere dem, så vil disse være sårbare for datakriminalitet. I mange tilfeller finnes det heller ikke oppdateringer til enhetene. Konsekvensene av dette har vi allerede sett, blant annet da det såkalte Mirai-botnettet[7] (som i hovedsak besto av enheter i private hjem) ble brukt til å slå ut globale nettsteder som Twitter, Netflix og mange andre.

6: http://www.gartner.com/newsroom/id/3598917

7: https://en.wikipedia.org/wiki/Mirai_(malware)

16% sier at de aldri tar sikkerhetskopi av sine data og 12% sier at de ikke vet om de gjør dette. De fleste som tar sikkerhetskopi (40%) sier at de gjør dette sjeldnere en hver måned.

Sikkerhetsprogramvare som antivirus, brannmurer og VPN-løsninger kan gi beskyttelse mot datakriminalitet og andre uønskede sikkerhetshendelser. Kun 4% forteller at de ikke bruker noen former for sikkerhetsprogramvare, og 11% sier at de ikke vet om de bruker slik programvare. 65% oppgir at de bruker brannmur og 73% oppgir at de bruker anti-virus. Vi kan anta at det i realiteten er enda fler som har brannmur på sine enheter fordi det er i dag vanlig at dette er en integrert del av alle moderne operativsystemer. Det er derfor ikke sikkert at dette er et valg som den enkelte i realiteten tar selv, og som en følge av det kan det være slik at mange ikke er klar over at de har slik sikkerhetsprogramvare.


swix

Hovedkonklusjon

Normenn er dårlig rustet til å møte den digitale revolusjonen

De hurtige endringene i både trusselbilde og hva som anses å være effektive sikringstiltak medfører at kunnskap om digital sikkerhet må oppdateres jevnlig. På tross av dette observerer vi at kun 21% av befolkningen sier at de har mottatt slik opplæring i løpet av de to siste årene. Vi ser samtidig at ferdighetene er for dårlige, og at mange ikke gjør de enkle tingene som gir effektiv beskyttelse mot datakriminalitet og andre uønskede hendelser på nett. To-trinns verifisering, sikkerhetskopiering og oppdatering av digitale enheter nevnes som eksempler.

Myndighetene, private og offentlige virksomheter og utdanningsinstitusjonene gjør mye for å legge tilrette for at den enkelte skal få opplæring, men våre funn viser at dette ikke er nok. Digitaliseringen av samfunnet skaper nye og tettere gjensidige avhengigheter mellom systemer, organisasjoner og enkeltindivider. Web-kameraet som står i et privat hjem kan brukes av kriminelle til å slå ut kritiske samfunnssystemer. Det er ikke lenger nok å tenke sikkerhet kun for de som tilbyr slike kritiske systemer, når hele samfunnets sårbarheter kan utnyttes av dem som ønsker oss vondt. Et digitalt samfunn må også være et trygt samfunn, og da må vi ha en helhetlig tilnærming der også den enkeltes kunnskap og ferdigheter inngår. Vår undersøkelse

viser at det er behov for en opptrapping av utdanning og opplæring av befolkningen. Et digitalt kompetanseløft som må omfatte digital sikkerhet.

Frykt for digitale trusler hindrer effektiv digitalisering

NorSIS erfarer at det er utfordringer med frykt og tillit i befolkningen til digitalisering og nye digitale tjenester. For at digitaliseringen skal være effektiv, må befolkningen omfavne de muligheter som gis. De må ha tillit til at de nye tjenestene er trygge, og de må ikke frykte at deres informasjon skal bli borte, bli endret eller komme på avveie. En mulig konsekvens når tilliten uteblir er at befolkningen velger å ikke ta tjenestene i bruk av frykt for digitale trusler. 33% sier at de har latt være å bruke digitale tjenester av frykt for slike trusler. Følelse av trygghet, og innstilling til digitaliseringen bør derfor være en prioritet for alle som arbeider med slike endringsprogram og ikke minst for myndighetene. Vi mener at tilliten til at politiet skal kunne hjelpe den enkelte er helt vesentlig når det kommer til den enkeltes opplevelse av frykt og tillit på nett. Vår undersøkelse viser imidlertid at politiet ikke nyter tilstrekkelig tillit når det gjelder det å hjelpe den enkelte som blir utsatt for datakriminalitet. Til påstanden *Politiet vil hjelpe meg dersom jeg blir utsatt for datakriminalitet*, svarer 44% at de er helt eller delvis enige i dette, mens 38% er helt eller delvis uenig.

Ny teknologi og digitalisering endrer samfunnet. Måten vi samhandler med hverandre og med teknologien endres. En kan allerede se hvordan disse endringene påvirker hvordan vi må tenke omkring digital sikkerhet. De digitale verdikjedene er lange og komplekse, og sikkerheten hos underleverandører (gjerne i flere nivåer) får direkte betydning for sikkerheten til funksjonen eller systemet som leveres. På samme måte blir sårbarhetsbildet også mer komplekst. Sammenhenger og årsakskjeder kan være vanskelig å forutse slik at målrettet forebygging blir mer utfordrende. Vi vet fortsatt for lite om hvordan befolkningens holdning til digitaliseringen påvirkes av store sikkerhetshendelser eller av samfunnsdebatter som berører den digitale innbygger. Hvordan påvirker for eksempel befolkningens holdning til styring og kontroll på nett etter en debatt omkring et Digitalt Grenseforsvar? Eller; er befolkningen utrustet med de holdninger og ferdigheter som må til for at vi kan ta imot en bølge av *Internet of Things* i de tusen hjem? Dette er kun to eksempler som kan få store samfunnsmessige konsekvenser.

Samfunnet trenger mer kunnskap om digital sikkerhetskultur

Kunnskap om trender og utviklingstrekk innen digital sikkerhet i befolkningen er styringsinformasjon som myndighetene trenger for å kunne utvikle god politikk på området, og som både offentlige og private virksomheter trenger for å utvikle og implementere trygge løsninger som befolkningen har tillit til. Myndighetene må derfor sørge for at det blir gjennomført slike undersøkelser minimun hvert annet år, og at resultatene deles med virksomheter i både offentlig og privat sektor. NorSIS mener at dette vil øke kunnskapsgrunnlaget i den enkelte virksomhet, og at disse dermed kan utvikle hensiktsmessige og effektive sikringstiltak.

Vedlegg A – Spørreskjema

Befolkningsundersøkelse om informasjonssikkerhets-kultur

Takk for at du deltar i denne undersøkelsen om informasjonssikker-hetskultur. Resultatet fra undersøkelsen skal brukes til å gi råd om en tryggere digital hverdag for alle.

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

1) * Hvor enig er du i følgende påstander?

	Helt uenig	Del-vis uenig	Del-vis enig	Helt enig	Vet ikke
Jeg er positiv til å ta i bruk ny teknologi					
Jeg vet hva informasjonssik-kerhet 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					
Politiet vil hjelpe meg dersom jeg blir utsatt for datakrimi-nalitet					
Det bør være mulig å være anonym på internett					

	Helt uenig	Del-vis uenig	Del-vis enig	Helt enig	Vet ikke
Internett blir ikke tryggere selv om min datamaskin er sikker					
Jeg har tillit til at myndighe-tene sikrer informasjonen de har registrert om meg					
Aktivistgrupper (f.eks. Anon-ymous) har en rolle i kampen mot datakriminalitet og cy-ber-krig					

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

☐ Ja

☐ Nei

☐ Vet ikke

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

☐ Ja

☐ Nei

☐ Vet ikke

4) 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

5) 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

6) * 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 kreditt-kort skal bli misbrukt på nett						
At andre skal utgi seg for å være meg på internett						
At jeg skal bli hetset eller mobbet på nett						
At mine digitale dokumenter og bilder skal bli ødelagt						

	1	2	3	4	5	Vet ikke
At jeg skal få virus på min datamaskin						
At jeg skal bli lurt til å gi fra meg sensitiv informasjon						
At ulike firma skal samle inn mye informasjon om hva jeg gjør på nett						

7) * 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						

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

	Ikke gjøre noe	Ordne opp selv	Få hjelp av en ekspert	An-melde 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					

9) Har kunnskap om trusler eller hacking noen gang fått deg til å la være å bruke en netttjeneste?

☐ Ja

☐ Nei

☐ Vet ikke

10) 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.

11) * Hvor interessert er du i teknologi og IT?
(1: Svært lite interessert. 5: Svært interessert)

☐ 1

☐ 2

☐ 3

☐ 4

☐ 5

☐ Vet ikke

12) * 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

13) * Hvem lærer du mest om informasjonssikkerhet av?

☐ Jeg lærer meg selv

☐ Eksperter

☐ Sjefer eller lærere

☐ Venner, kolleger eller klassekamerater

☐ Vet ikke

14) 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

15) * Hvem lærer du mest om informasjonssikkerhet av?

☐ Jeg lærer meg selv

☐ Eksperter

☐ Sjefer eller lærere

☐ Venner, kolleger eller klassekamerater

☐ Vet ikke

16) 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

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

☐ Ja

☐ Nei

☐ Vet ikke

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

(Kryss av alle du bruker)

☐ Brannmur

☐ Anti-virus

☐ Annen sikkerhetsprogramvare

☐ Bruker ingen sikkerhetsprogramvare

19) * 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 eller skole.

20) * 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

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

☐ Hver uke eller oftere

☐ Hver måned

☐ Sjeldnere enn hver måned

☐ Aldri

☐ Vet ikke

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

☐ Ja

☐ Nei

☐ Vet ikke

23) * 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

Teknologiveien 22
2815 Gjøvik
Org.nr: 995 195 003

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

NorSIS
Norsk senter for informasjonssikring