Prosjektoppgave i MSA115 – Risiko og samfunnssikkerhet
Høsten 2019
Universitetet i Stavanger

# *«Å godta det ukjente*

# *– en undersøkelse om risikopersepsjon knyttet til åpne nettverk»*

***Forord***

Vi vil med dette gjerne få rette en stor takk til alle som har vært med på å forme prosjektet. Først og fremst vil vi takke Vy, for gjestfriheten og muligheten til å foreta undersøkelser på deres togreiser. Med dette følger også en stor takk til passasjerene som velvillig lot seg intervjue.

Det er også på sin plass å rette en stor takk til veilederen vår, Ole Andreas Hegland Engen, for gode råd og tips underveis. Innspillene hans førte til ny motivasjon når skrivingen stagnerte, og ga oss dermed meget god støtte.

Til slutt må vi takke hverandre: for at alle har bidratt jevnt, for gode diskusjoner, og for at alle har gjort sitt beste. I en slik blandet gruppe lærer man seg å sette pris på varierte kunnskapsbidrag og gode diskusjoner.

God lesing!

# Innholdsfortegnelse



**Tabelloversikt:**

## 1.0 Innledning

Åpne nettverk tilsier gratis tilkobling til internett for alle, og er i dag svært utbredt i det offentlige rom. Man finner det på kafeer, kollektivtransport, på flyplasser, hos kommuner, på skoler, kjøpesentre, og lignende. Dette tilbudet er så vanlig at de fleste av oss, med relativt høy tillit til institusjonen nettverket tilhører, ofte vil være raske med å koble oss til. Likevel er det kanskje ikke alle som tenker over farene en utsetter seg for. For dersom du velger et åpent nettverk, kan det bety at tilkoblingene er usikret. Dette betyr at uvedkommende kan overvåke din nettaktivitet. Nettaktiviteten din innebærer alt du sender og mottar over internett, som ikke er kryptert. Dette kan være alt fra søkelogg, brukernavn, passord, bankkontoinformasjon, og lignende.

Norge er et av de ledende landene når det kommer til å ta i bruk ny teknologi (Departementene, 2019, s. 8). Digitaliseringen fører til store samfunnsmessige endringer, som videre bringer med seg utfordringer knyttet til risiko og sårbarhet. Med de lange og uoversiktlige digitale verdikjedene er det utfordrende å opprettholde god beredskap (NOU 2015: 13, 2015, s. 17). En forutsetning for vellykket digitalisering i Norge vil derfor avhenge av at det skjer innenfor rammer der sikkerhet ivaretas, samt at vi sørger for robuste beredskapsløsninger (Justis- og beredskapsdepartementet, 2019). Dette kan være utfordrende, da det er krevende å forutse hvilke trusler som vil prege risikobildet i fremtiden når utviklingen skjer så raskt. I Regjeringens rapport (Helhetlig IKT-risikobilde) kan vi se at det identifiseres visse trusler som trolig vil fortsette å prege risikobildet i årene fremover, deriblant personutpressing, krenkelser på nett og ID-tyveri (Departementene, 2019, s. 6). De siste årene har faktisk så mye som 150 000 mennesker i Norge blitt utsatt for sistnevnte, der noen har benyttet deres identitet for å begå straffbare handlinger (Norsk senter for informasjonssikring, 2018). Disse hendelsene skjer ofte av såkalte man-in-the-middle-angrep. Dette kan forklares som en form for sniklytting, der data fra den private maskinen som logger seg på (A) blir sendt til serveren til det åpne nettverket (B), hvor sårbarheter gjør at en utenforstående 'hacker'(C), kan gå mellom transaksjonene som sendes, og lese dem. Slike mulige hendelser, sett ut fra datatilgangen (C) eventuelt får, er med på å gjøre påloggingen til det åpne nettverket spesielt sårbar (Vondráček, Pluskal, & Ryšavý, 2018, s. 65)

Med dette trusselbildet i bakhodet vet man at det er viktig at folk kjenner til risikoen som følger med det å logge seg på et åpent nettverk. Til tross for dette ligger det i vår kultur å ha tillit til institusjonene rundt oss.

### 1.2 Problemstilling

I oppgaven vår er vi ute etter å identifisere hvordan menneskers risikopersepsjon er knyttet til åpne nettverk, og videre se hvilke risikovurderinger de foretar seg basert på dette. Vi kommer til å vektlegge nettverk som tilbys av en institusjon man kan anta at befolkning har høy tillit til for å videre se på hvordan dette tillitsforholdet kan påvirke risikoopplevelsen og tilbøyeligheten personer har til å logge seg på slike nettverk. På bakgrunn av dette har vi utarbeidet følgende problemstilling:

*«Hvilke risikovurderinger foretar passasjerer hos Vy med hensyn til nettverksløsninger?»*

For å besvare studiens problemstilling har vi et teoretisk rammeverk som omfatter teori om risikopersepsjon og tillit. Valget av dette teoretiske rammeverket er gjort på bakgrunn av at disse anses som både relevante for temaet studien omhandler, og videre hensiktsmessige for å besvare studiens problemstilling.

### 1.3 Avgrensning

I denne studien vil vi undersøke en organisasjon innenfor ett av Nordens største transportkonsern. Vy, tidligere kjent som NSB, ivaretar daglig sentrale oppgaver nødvendige for samfunnets funksjonalitet i form av effektiv og sikker transport av personer, varer og gods. Sett i lys av Vy sitt viktige samfunnsoppdrag er det viktig at organisasjonen viser at de behersker oppgavene de er ansvarlige for, og at de fungerer pålitelig over tid, slik at samfunnstilliten til organisasjonen er og forblir høy. På bakgrunn av dette ønsker vi å kartlegge befolkningens tillit til denne organisasjonens nettverkstilbud, og videre undersøke om vi kan se en sammenheng mellom grad av tillit og tilbøyelighet til å bruke åpne nettverk. Vi kommer ikke til å ta for oss hvilke tillitsskapende virkemidler organisasjonen bruker for å sørge for økt grad av tillit i befolkningen. Vi kommer heller ikke til å gå inn i detalj på hvordan åpne nettverksløsninger er satt opp og designet, eller gå i detalj om hvilke faktorer som gjør disse nettverkene usikre. I stedet kommer vi til å bruke teori om risikopersepsjon for å få innblikk i de subjektive- og skjønnsmessige vurderingene som blir gjort av reisende

passasjerer i forbindelse med pålogging til nettverket. Det er viktig å påpeke at vi har fokus på nettverket Vy tilbyr, og ikke på Vy som institusjon. Vi vektlegger heller ikke hvordan ondsinnede aktører arbeider for å tilegne seg sensitive opplysninger i form av personopplysninger, bankinformasjon og passord.

# 2.0 Teori

I dette avsnittet skal vi gjøre rede for det teoretiske rammeverket vi benytter for å besvare studiens problemstilling. Teoriene som vil bli gjennomgått i dette kapittelet omhandler begrepene risiko, risikopersepsjon og tillit. Disse tre begrepene er valgt sammen på bakgrunn av at de påvirkes av og korrelerer med hverandre.

## 2.1 Perspektiver på risiko

Risiko er et begrep det ikke foreligger noen entydig forståelse av. Begrepet brukes i ulike sammenhenger – ofte med forskjellig og uklar betydning (Aven, Boyesen, Olsen, & Sandve, 2004, s. 37). En forståelse av risiko er at det kan forstås som et produkt av sannsynlighet og konsekvens (Engen et al., 2016, s. 41). I vårt tilfelle vil det bli sannsynligheten for å oppleve en uønsket hendelse på Vy sitt åpne nettverk, og den eventuelle konsekvensen av dette. Selv om det finnes ulike oppfatninger av hva risiko er, er det vanlig å dele risiko inn i to hovedperspektiver med tilhørende teorier og perspektiver. Et viktig skille mellom disse perspektivene, selv om de ikke nødvendigvis er gjensidig utelukkende fra hverandre, er ulike oppfatninger om hva risiko er og hvilke forhold som er relevante når risikoen skal analyseres og håndteres (Aven et al., 2004, s. 38).

I vår oppgave ønsker vi å se på hvordan passasjerer på togene til Vy forholder seg til risikoen ved å koble seg til nettverket som tilbys på toget. På bakgrunn av dette har vi valgt en samfunnsvitenskapelig tilnærming til risiko. Denne tilnærmingen er mer opptatt av hvordan individer og grupper opplever og forstår risiko enn den tradisjonelle tekniske-naturvitenskapelige tilnærmingen som fokuserer mer på ekspertkunnskap knyttet til matematiske og statistiske beregningsmetoder (Aven et al., 2004, s. 40). I en samfunnsvitenskapelig tilnærming til risiko er det de subjektive forholdene som legges til grunn for menneskers risikoforståelse. Dette innebærer at individuelle faktorer som sosiale og kulturelle faktorer samt erfaringer kan påvirke måten mennesker forstår, opplever og forholder seg til risiko.

## 2.2 Hva er risikopersepsjon?

Forskning på hvordan mennesker vurderer og forholder seg til ulike risikokilder har vist at det foreligger et ulikt risikobegrep blant eksperter og befolkningen, i forhold til hva som ligger til grunn for deres risikoforståelse. I studier av risikopersepsjon har man i større grad beveget seg bort fra ekspertenes statistiske- og matematiske risikovurderinger for å heller vektlegge de mer subjektive forholdene som ligger til grunn for hvordan lekfolk oppfatter og vurderer risiko (Boyesen, 2003, s. 9). Ifølge Boyesen (2003) er det påvist en sammenheng mellom opplevd risiko og hvordan mennesker responderer og forholder seg til risiko. Når vi undersøker risikopersepsjon er vi derfor opptatt av hvordan folk forstår, opplever og responderer på risiko og farer knyttet til åpne nettverk.

### 2.2.1 Hva påvirker folks opplevelse av risiko?

I denne teoridelen skal vi gjennomgå utvalgte faktorer som kan være med å påvirke folks risikopersepsjon. Dette vil vi gjøre med utgangspunkt i forskning gjort av Marit Boyesen (2003) og Wibecke Brun (1997).

Ifølge Boyesen har folk normalt vanskeligheter for å vekte sannsynlighet og konsekvens i forhold til hverandre. I noen tilfeller vil konsekvensene tillegges uforholdsmessig stor betydning uavhengig av sannsynlighetene for at risikokilden vil inntreffe. *Styrke-dimensjonen* anses å være den viktigste komponenten i lekfolks risiko-opplevelse og går ut på at dess mer alvorlige og urovekkende konsekvensene en mulig risikokilde har, dess større opplever folk risikoen forbundet med denne risikokilden, uavhengig av tilhørende sannsynligheter (Brun, 1997, s. 4). Dersom noen for eksempel får høre om de store konsekvensene av å bli utsatt for et identitetstyveri ved tilkobling til et åpent nettverk, er det naturlig å anta at vedkommende blir ekstra bevisst på sikkerheten rundt tilsvarende nettverk.

På samme måte som at konsekvensene i noen tilfeller kan tillegges for stor oppmerksomhet, kan de i andre tilfeller bli undervurdert når sannsynligheten oppleves som liten (Boyesen, 2003, s. 10). Gjennom *eksponerings-dimensjonen* viser Brun (1997) til hvordan lekfolk operer med et individualistisk sannsynlighetsbegrep. Dette går ut på at man vurderer sannsynligheter opp mot relativ risiko for den enkelte utsatte person. Videre hevder Brun at det er påvist at lekfolk har en tendens til å tenke at negative hendelser har mindre sjanse for å

inntreffe en selv enn andre. Dette kan i mange tilfeller resultere i at sannsynlighetene undervurderes fordi man tenker at man ikke befinner seg i samme risikogruppe som andre mennesker (Brun, 1997, s. 6).

Sett i lys av dimensjonen nevnt ovenfor kan mediefokusering, og hvordan ulike farer presentert gjennom media, også påvirke folks vurdering av risiko opp mot ulike farekilder (Brun, 1997, s. 8). Dette kan man forklare ved å henvise til kognitive heuristikker, og da spesielt tilgjengelighetsheuristikken, som omhandler hvordan informasjon som er lettere tilgjengelig i hukommelsen vurderes som mer sannsynlig enn informasjon som er mindre fremtredende i bevissthetsbilde (Brun & Kobbeltvedt, 2005, s. 170). Dette påvirker den enkeltes risikoopplevelse ved at de langt mer sjeldne og katastrofale farene som får store mediedekning oppleves som mer sannsynlig enn de mer hverdagslige farene.

Folk er ofte villige til både å akseptere og utsette seg for et høyere risikonivå når de selv velger farene, enn når de utsettes for farer de mener de burde ha blitt advart mot (Boyesen, 2003, s. 11). Dette korresponderer med *aktiv-passiv dimensjonen*, som viser til hvordan grad av frivillighet og kontroll forbundet med en gitt aktivitet er med på å påvirke den enkeltes risikoopplevelse (Brun, 1997, s. 5). Med grad av kontroll mener man at risikoen vil være lettere å akseptere i de tilfeller man opplever det slik at en gjennom personlig egnethet og kompetanse har kontroll over risikoen. Med tanke på at folk selv velger å logge seg på det åpne nettverket, vil det være naturlig å tro at de føler på en viss trygghet og kontroll.

*Nyhet-dimensjonen* er også relevant å knytte opp mot problemstillingen, ettersom den vektlegger de personlige erfaringene forbundet med risikoen. Dersom risikoen oppleves som ny og ukjent, vil dette kunne oppleves som verre enn en kjent risikokilde, uavhengig om sistnevnte har en høyere ulykkesrate (Brun, 1997, s. 4). Med ande ord kan presentasjonen av problemstillingen og informantens kjennskap til fenomenet påvirke hvordan folk vil respondere under et intervju.

### 2.3 Tillit

Det er lett å se for seg: man sitter på kafeen i nabolaget og kobler seg på det åpne nettverket. Ville man ha gjort det samme dersom man befant seg på en fremmed kafé, kanskje i et annet land? Det er logisk å tenke at man vil ha lettere for å logge seg på et åpent nettverk hos en institusjon man kjenner og har tillit til, enn hos en man ikke kjenner. Ettersom det er lett å forestille seg at tillit kan spille en stor rolle i en slik beslutning, er det relevant å se nærmere på teorien rundt begrepet.

Som sosiale vesener ønsker mennesker å stole på hverandre. Ifølge Harald Grimen er tillit «*samfunnets lim, smøremiddel og grunnmur*» (Grimen, 2009, s. 11). Forskningen som er gjort på tillit er riktignok noe uoversiktlig og uforenlig, ettersom det er mange diskusjoner rundt begrepet. Likevel er det noen teori innenfor begrepet det er stor enighet om, nemlig at tillit er nødvendig for at mennesker skal kunne gå overens med hverandre, samt benytte seg av institusjonene og funksjonene som tilbys. Hvis man, i vårt tilfelle, ikke har tillit til Vy som institusjon, vil man antakeligvis ikke benytte seg av tilbudene deres heller.

Engen et al. påpeker tydelig at tilliten i samfunnet også er et viktig element dersom man vil forstå hvordan folk oppfatter ulike farer og trusler (Engen et al., 2016, s. 49). Dersom tilliten er lav er det sannsynlig å tenke at det henger sammen med at folk ikke har tro på at institusjonen og, i dette tilfellet, at det åpne nettverket kan takle farer og trusler. Velger reisende hos Vy å benytte seg av det åpne nettverket kan en ut fra dette anta at de har tillit til både togselskapet og nettverket som funksjon. De gir Vy et såkalt tillitsmandat, hvor en sannsynligvis regner med at ens informasjon og sikkerhet blir ivaretatt.

Det vil også være hensiktsmessig å se på hvordan tillit blir til. Tillit kan sies å komme av erfaringer vi har tilegnet oss over tid (Engen et al., 2016, s. 49). Noen vil også påstå at tillit har lett for å føre til mer tillit (Grimen, 2009, s. 15). Disse påstandene blir forsterket av hverandre. Eksempelvis kan man si at dersom man føler en viss trygghet ved å reise med Vy, er det lett å tolke det dithen at man har tillit til Vy. Likeså kan man anta at dersom man har logget seg på et nettverk tidligere, og det gikk tilsynelatende fint, er det lett å se for seg at man vil logge på igjen. Positive erfaringer av den ene og den andre typen er med andre ord et element det kan være relevant å se på i forbindelse med den enkeltes tillit. Dette kan

sammenlignes med styrke-dimensjonen innenfor risiko, der man forbinder det man vet om konseptet til den opplevde følelsen [av risiko], som videre styrker følelsen.

Med utgangspunkt i det vi har sagt om teorien rundt risiko, risikopersepsjon og tillit her i teoridelen, ønsker vi å koble det opp mot den enkeltes oppfatning av trusler og farer til det åpne nettverket til Vy. Vi tenker eksempelvis at det er interessant å undersøke om de som velger å *ikke* koble seg til nettet hos Vy, gjør det fordi vedkommende ikke har tillit til systemet rundt, og dermed opplever risikoen som større. Dette vil vi se nærmere på når vi legger frem resultatene fra undersøkelsen og drøfter funnene i lys av begrepene som er presentert.

## 3.0 Metode

For å kunne besvare oppgavens problemstilling, har vi gjennomført en case-studie av passasjerene på et av togene til Vy. Vi fikk tillatelse av markeds- og kommunikasjonssjefen i Vy til å gjennomføre studien på et lokaltog til Bryne med avgang fra Stavanger 15:33 en fredag ettermiddag. Dette var et tog vedkommende mente flere vanligvis tok på vei hjem fra jobb, og at det dermed ville være større sannsynlighet for at reisende benyttet seg av nettverket.

Vi valgte å bruke semi-strukturert intervju, da vi så det som best egnet metode for vår datainnsamling. Videre formulerte vi seks korte spørsmål som vi ønsket å spørre passasjerene om. Semi-strukturerte intervjuer er en mer fleksibel metode som gjør det mulig å endre og legge til spørsmål underveis i intervjuprosessen. Dette gjorde at vi eventuelt kunne stille oppfølgingsspørsmål dersom det var noe vi ønsket å gå mer i dybden på og få en bedre forståelse av. Denne metoden tillot at intervjuprosessen ble mindre formell og ble formet mer som en samtale. Metoden ville også være gunstig tatt i betraktning av vårt begrensede tidsrom til å utføre oppgaven, og for å kunne være tilgjengelig til å møte folk som er på reisefot. Med tanke på at det ville være flere folk i vognen under intervjuene, tenkte vi det ville være en lavere terskel hos informantene for å gjennomføre et kort intervju fremfor en mer detaljert spørreundersøkelse. Slik kunne vi også intervjue flere passasjerer i løpet av den korte tiden vi hadde, og dermed i større grad danne oss et overordnet bilde av folks generelle vaner knyttet til problemstillingen.

Som en bieffekt av metodebruken vår tenker vi det er relevant å se på Hawthorne-effekten. Dette er situasjoner der man opplever at forskningsobjekter endrer atferd dersom forskerne er til stedet. I noen tilfeller virket det som vi gjorde enkelte av informantene ekstra oppmerksom på sin bruk av nettverket, og at vi således trigget risikopersepsjonen til vedkommende. Dette så vi blant annet ved at enkelte virket til å endre holdning til temaet underveis i intervjuprosessen.

Vi valgte Vy som institusjon for vår datainnsamling fordi vi anså dette som en institusjon folk flest har en viss grad av tillit til. Vi antar, som nevnt i teorien, at ved høy tillit til en institusjon vil terskelen for å logge seg på nettverk være betydelig lavere. Vi tok utgangspunkt i å intervjue cirka 30 reisende, på cirka én times togreise. Dataene vi samler her vil bli grunnleggende for videre diskusjon og drøfting av oppgaven.

Angående forventningen vår til spredning av informanter tror vi dette ville vært nokså likt dersom vi gjennomførte intervjuene på samme tog og tidspunkt bare en annen dag. Dette fordi vi valgte et tog med avgang fra Stavanger 15:33, hvor en stor andel av de reisende var på vei hjem fra jobb eller skole, og dermed kom innenfor de sosiale dimensjonene vi ønsket å studere. Hadde vi endret tidspunktet for når undersøkelsen ble gjennomført kunne dette ha påvirket resultatene i noen grad.

### 3.1 Oversikt over informanter

Vi intervjuet til sammen 33 informanter, hvor alle var reisende på Vys tog. Intervjuene ble utført ansikt til ansikt, hvor to av gruppemedlemmene spurte informantene spørsmål, mens to noterte informantenes svar underveis. Vi valgte å gå hver for oss i to grupper, hvor den ene gruppen intervjuet menn og den andre kvinner. Dette var fordi vi ønsket likest mulig fordeling mellom kvinner og menn i utvalget vårt. Vi forsøkte å intervjue folk av ulik alder slik at vi hadde et bredt utvalg også her. Grunnen til dette var at vi ønsket å se på om svarene på intervjuspørsmålene varierte ut fra de sosiale dimensjonene: kjønn, alder og utdanning. I tabellene under presenteres informantene vi bruker i oppgaven. Informantene omtales som M1 til M17, og K1 til K16. Kolonnene presenterer informasjon om informantene. Fra venstre til høyre presenteres informantenes alder, samt deres høyeste fullførte utdanning.

*Tabell 1: Oversikt over informanter*

| Informanter | Alder | Utdanning |
|---|---|---|
| M1 | 65 | Bachelor |
| M2 | 46 | Bachelor |
| M3 | 39 | Bachelor |
| M4 | 66 | Doktorgrad |
| M5 | 44 | Master |
| M6 | 44 | Master |
| M7 | 57 | Fagbrev |
| M8 | 24 | Videregående |
| M9 | 30 | Videregående |
| M10 | 32 | Fagbrev |
| M11 | 24 | Bachelor |
| M12 | 38 | Master |
| M13 | 35 | Bachelor |
| M14 | 44 | Fagbrev |
| M15 | 63 | Master |
| M16 | 24 | Bachelor |
| M17 | 73 | Bachelor |

| Informanter | Alder | Utdanning |
|---|---|---|
| K1 | 21 | Videregående |
| K2 | 52 | Høyskole |
| K3 | 45 | Master |
| K4 | 23 | Bachelor |
| K5 | 25 | Videregående |
| K6 | 22 | Videregående |
| K7 | 60 | Videregående |
| K8 | 22 | Videregående |
| K9 | 20 | Master |
| K10 | 47 | Videregående |
| K11 | 51 | Master |
| K12 | 29 | Videregående |
| K13 | 28 | Apotektekniker |
| K14 | 34 | Master |
| K15 | 25 | Bachelor |
| K16 | 69 | Lærerutdanning |

Som det kommer frem i tabellen har vi tilnærmet lik spredning blant kvinner og menn, vi fikk intervjuet 16 kvinner og 17 menn. Alderen på kvinnene varierer fra 20 til 69 år, mens spredningen i alder hos mennene er mellom 24 til 73 år. Informantenes utdanningsbakgrunn varierer mellom videregående og master blant kvinnene, og videregående og doktorgrad blant mennene. Dette fordi vi ønsket god spredning innenfor kjønns-, alders- og utdanningsvariablene.

### 3.2 Etiske refleksjoner

I og med at vi undersøker folks nettvaner beveger vi oss ikke inn på et betydelig sensitivt tema. Likevel var det viktig å være oppmerksomme på hvordan deltakerne opplevde intervjuprosessen. Dette fordi vi intervjuer mennesker og det er deres meninger vår empiri består av. Derfor var vi klare på å informere om hva studien vår omhandlet, og hva den skulle

brukes til. Vi var også konsekvente på å opplyse om at det var frivillig å delta og at man ikke måtte svare på spørsmål man ikke ønsket. Hele intervjuprosessen foregikk anonymt, det vil si at vi noterte ikke navn på deltakerne, samt at vi i oppgaven refererer til deltakerne på en anonym måte. Informasjonen hentet til denne oppgaven vil heller ikke bli brukt i andre sammenhenger.

### 3.3 Styrker og svakheter med metoden

Det som først og fremst styrker oppgavens reliabilitet, er at vi har gjort rede for fremgangsmåter for innsamling av data, forskningsstrategi og metodiske valg. Dette er med på å styrke oppgavens pålitelighet ved at det gir leseren innsikt i hvordan vi som forskere har kommet frem til våre konklusjoner (Thagaard, 2013, s. 202). Det at vi snakket med alle informantene gjennom et personlig møte mener vi også var en styrke, og vi ser ingen grunn til at noen av disse informantene skulle snakket usant i intervjuprosessen.

Ettersom intervjuprosessen foregikk på et tog, førte dette til at det var flere mennesker tilstede under prosessen. Dette kan ha vært med på å svekke vårt metodevalg i form av at enkelte av informantene kunne høre hva andre deltakere svarte, og således kan ha tilpasset sitt eget svar deretter. For å unngå dette i størst mulig grad prøvde vi konsekvent ikke å intervjue for mange passasjerer i samme togvogn, slik at vi fikk individuelle svar og ikke svar basert på sidemannens meninger. En annen faktor som kan ha svekket relabiliteten til oppgaven er at vi ikke tok lydopptak under intervjuene. Hadde vi tatt i bruk lydopptak ville vi i større grad fått med oss alt intervjuobjektene sa, noe som blir vanskeligere når man tar notater fortløpende. I utgangspunktet ble resultatet av undersøkelsen som forventet.

## 4.0 Empiri og drøfting

I denne delen av oppgaven skal vi presentere empiriske funn innhentet gjennom en rekke samtaleintervjuer med reisende togpassasjerer på Vy. De kvalitative dataene fra intervjuet vil presenteres gjennom informantenes uttalelser. I de tilfeller vi bruker direkte sitater fra informantene, gjøres det ved at sitatene markeres i kursiv. Når vi skal referere til spesifikke kjønn vil dette gjøres enten som kvinne (K1, K2, K3, ...) eller mann (M1, M2, M3, ...). Vi har valgt å strukturere empiri og drøfting sammen i et kapittel, hvor kapittelet er inndelt i fire underkapitler med basis i de spørsmålene informantene ble stilt under intervjuprosessen. Vi

har valgt denne løsningen fordi vi på denne måten best får presentert og drøftet de empiriske funnene opp mot vårt teoretiske rammeverk.

### 4.1 Pleier du å benytte deg av åpent nettverk? Hvorfor/ hvorfor ikke?

Risikopersepsjon er som allerede nevnt hvordan mennesker forstår, opplever og responderer til risiko (Boyesen, 2003). Risikopersepsjon henger i vår studie tett sammen med befolkningens tillitt til åpne nettverk. Empirien vår viser at 17 av 33 deltakere (53 %) svarte klart ja på at de tok i bruk Vy sitt nettverk under togreiser. Syv av deltakerne (21 %) svarte at de brukte nettverket av og til. Dette viser oss at reisende generelt har høy tillitt til bruk av nettverket Vy tilbyr. Det er viktig å påpeke at noen av deltakerne svarte at de brukte nettverket av og til, mens de i andre tilfeller lot være på grunn av nettverks*kvaliteten*, og ikke på grunn av opplevd risiko. Selv om over halvparten svarte at de brukte nettverket, svarte en del av denne gruppen at selv om de tok i bruk nettverket, var de forsiktige med hva de brukte det til. Flere av deltakerne var påpasselige med å ikke bruke nettverket til f.eks. nettbank eller i jobbsammenheng.

*"Jeg bruker nettverket av og til, men kun på telefonen. Jeg bruker nettet som regel bare til nyheter og diverse."* (M5)

*"Ja, jeg bruker nettverket. Jeg vil ikke bruke 4G, jeg bruker som regel nettet bare til streaming og Netflix."* (M8)

Nettverket ble mest brukt til streaming, sosiale medier og lesing av nyheter og det kommer frem at folk generelt opplevde en større risiko knyttet til å bruke nettverket til mer sensitiv aktivitet. Dette kan være en direkte konsekvens av tillitten de har til nettverket Vy tilbyr. Ut i fra dette ser vi at styrke-dimensjonen påvirker, i og med at undersøkelsen vår viser at reisende opplever at det er større konsekvenser knyttet til å bruke nettverket til mer sensitiv data som nettbank og i jobbsammenheng (Brun, 1997). Man anser at konsekvensene hvis noe skulle skje blir i større omfang enn hvis man kun bruker nettet til mindre privat aktivitet som streaming og nyheter. Selv om mange anser det som mindre risikofylt å bruke åpne nettverk til kun streaming og for eksempel Netflix, innebærer dette også at man gir fra seg opplysninger om både kontonummer og andre personopplysninger av relativt privat karakter.

Empirien vår viser ikke noe stort skille mellom kvinner og menn når det kommer til opplevd risiko. Åtte av mennene svarte klart ja på at de bruker det åpne nettverket samt ni av kvinnene. Den største forskjellen var de som ikke brukte nettverket. Her svarte seks menn nei opp mot kun to kvinner. Dette kan vise til at menn i noe mindre grad har tillit til nettverket som tilbys. Derimot svarte fem av kvinnene at de tok i bruk nettverket av og til, opp mot kun to av mennene. I og med at vi har et lite utvalg av informanter, kan man ikke trekke konklusjon til at tendensene gjelder for alle menn eller alle kvinner. Likevel, på bakgrunn av det utvalget vi har hatt for denne undersøkelsen kommer det frem at menn kan virke noe mer skeptiske til å logge seg på åpne nettverk enn kvinner.

Når det kommer til grad av utdanning og bruk av nettverket ser vi heller ingen generell sammenheng knyttet til spørsmålet om pålogging av åpne nettverk. Vi så derimot at flere av de som bruker nettverket i forbindelse med jobb, ofte velger andre løsninger enn å ta i bruk åpne nettverk. Dette på grunn av sikkerhetsmessige grunner. Vi så heller ikke noe markert skille mellom den eldre og den yngre generasjonens valg av tilkobling til åpne nettverk.

Det er tydelig at det noen anser som en risiko, ikke alltid blir oppfattet på samme måte av andre. Vi kan se at deltakerne i undersøkelsen har ulik risikopersepsjon. Noen vil kanskje undervurdere en risiko andre ser på som høy. Dette viser empirien vår tydelig, mens noen av passasjerene er svært skeptiske til hva de bruker nettverket på, har andre ikke tenkt over risikoen dette kan medføre. Brun (1997) forklarer gjennom eksponerings-dimensjonen hvordan enkeltindivider opererer med et individualistisk sannsynlighetsbegrep. Dette innebærer at man vurderer sannsynlighet opp mot relativ risiko for hver enkelt utsatt person. Dette ser vi tydelig blant våre informanter, da noen ikke oppfatter det som en risiko å logge seg på Vy sitt nettverk, mens andre er mer skeptiske. For å vise denne forskjellen svarte to av informantene følgende på første spørsmål:

*"Nei, jeg har eget nettverk av sikkerhetsmessige grunner."* (M7)

*"Ja, jeg pleier å bruke nettverket som tilbys."*(K1)

Det kan være flere grunner til at reisende har ulik risikopersepsjon knyttet til åpne nettverk. Hvis man tidligere har opplevd en hendelse med Vy som har ført til svik i tillit, er det ofte en sammenheng mellom tidligere hendelse og nåværende risikopersepsjon. Har man på den

andre siden generell tillit og gode erfaringer med Vy, kan man regne med at man i større grad også har tillit til nettverket som tilbys. Tillit har ofte lett for å føre til mer tillit (Grimen, 2009, s. 15) og kommer ofte av erfaringer man har tilegnet seg over tid (Engen et al., 2016, s. 49).

*"Jeg bruker nettet noen ganger på togreiser, men det gjelder ikke for alle som tilbyr gratis nettverk. Jeg stoler på noen organisasjoner fremfor andre [...]"* (K10)

Dette viser oss, som K10 sier, at tilliten og opplevelsene man har knyttet til en organisasjon er avgjørende for tilliten man har til nettverk og tjenester de tilbyr. Dette henger sammen med perspektivet Engen (2016) presenterer knyttet til tillit til institusjoner. Har man generelt tillit til en institusjon, er det større sannsynlighet for at man også stoler på tjenestene institusjonen tilbyr, som i dette tilfelle er Vy som institusjon og deres nettverk.

### 4.2 Mener du at du er i stand til å vurdere om et åpent nettverk er sikkert nok? Hvorfor, hvorfor ikke?

På spørsmål der informantene selv skulle vurdere i hvilken grad de er i stand til å vurdere om et åpent nettverk er sikkert nok eller ikke, ser vi at det store flertallet av våre respondenter selv mener de ikke er i stand til dette. Totalt er det 25 av 33 informanter (76 %) som svarer nei på dette spørsmålet hvorav 11 av disse er menn og 14 er kvinner. Det gis ulike begrunnelser for hvorfor de mener de ikke er i stand til å vurdere sikkerheten på nettverket selv. Felles for den store majoriteten av våre respondenter er at de henviser til personlig egnethet og teknisk kompetanse til å utføre en slik vurdering selv.

*«Nei, jeg vil ikke si jeg er i stand til å vurdere om nettverket er sikkert eller ikke. jeg har verken nok informasjon eller kompetanse til å vurdere dette.»* (K5)

For andre virker det ikke som at dette er noen bevisst vurdering, foruten at det er viktig at de har kjennskap til organisasjonen som tilbyr nettverket. *«… Jeg tenker at det er sikkert nok så lenge man kjenner til organisasjonen» (K9).* For andre som faller inn under samme kategori med sin besvarelse på dette spørsmålet, sitter vi med et inntrykk av at en slik vurdering ikke vektlegges eller prioriteres noe særlig. *«nei det vet jeg ikke, det har jeg ikke tenkt på ... selskapet må jo ha sikkert nett regner jeg med»* (M11).

Blant våre informanter er det totalt fem (15 %) som mener de er i stand til å vurdere om sikkerheten på nettverket som tilbys er sikkert nok. Det er tre menn og to kvinner som mener de kan gjøre en slik vurdering selv, og felles for disse er at samtlige har en eller annen form for høyere utdanning enten i form av universitetsutdanning eller fagskole. Selv med høyere utdanning er det allikevel et ulikt erfaringsgrunnlag innenfor datasikkerhet blant våre informanter som har svart ja på dette spørsmålet. Det er gjerne de informantene med relevante erfaringer og/eller bakgrunn innenfor datasikkerhet som selv med kunnskap til å vurdere sikkerheten på nettverket, likevel gir uttrykk for skepsis og usikkerhet i forhold til i hvilken grad dette er fullt mulig. *«Ja, jeg har IT-bakgrunn så jeg kan sikre meg, men det finnes alltids noen som er flinkere»* (M6). Felles for informantene med erfaring og bakgrunn innenfor datasikkerhet er videre at de anser sannsynligheten for å bli utsatt for digitale hendelser som høy i tillegg til at de fremstår langt mer skeptiske både i forbindelse med bruk og i hvilken grad de er tilbøyelige for å logge seg på åpne nettverk eller ikke. «*Jeg har et eget nettverk jeg bruker av sikkerhetsmessige grunner*» (M7).

Empiriske funn fremhevet ovenfor tolker vi som en indikasjon på at det ikke foreligger noen tydelige ulikheter i kjønn og i hvilken grad informantene mener de er i stand til å vurdere om et åpent nettverk er sikkert nok eller ikke. Det samme gjelder utdanning, der empiriske funn viser en jevn fordeling av informantene med- og uten høyere utdanning som har svart nei på dette spørsmålet. Selv om 76 % av informantene mener de ikke er i stand til å vurdere sikkerheten på nettverket, virker ikke dette å ha de store implikasjonene på andre forhold, som i hvilken grad nettverket som tilbys brukes eller i hvilken grad informantene anser risikoen for å bli utsatt for digitale hendelser som høy. At risikoen vurderes som liten i dette utvalget kan begrunnes ved at det det er få som gir uttrykk for at de har opplevd å bli utsatt for digitale hendelser tidligere. Det er med andre ord få personlige erfaringer og opplevelser tilknyttet digitale risikoer. *«Jeg anser sannsynligheten som liten ... men det er nok fordi jeg ikke har opplevd det ennå»* (M4). Andre gir uttrykk for at de har kjennskap til at uønskede hendelser kan oppstå, men at det er først og fremst noe som går ut over større organisasjoner og ikke enkeltpersoner (K16). Sistnevnte kan forklares ved å henvise til hvordan informasjon fra media om ulike risikoer kan påvirke menneskelige vurderinger og opplevelser i tilknytning til ulike farer (Brun, 1997).

Foruten personlig kjennskap og erfaring med risikoene kan reisende passasjerers atferd i forbindelse med digitale risikoer forklares ved å henvise til hvordan mennesker er mer

tilbøyelige for å akseptere og utsette seg for et høyere risikonivå når de selv velger farene (Boyesen, 2003). Når reisende togpassasjerer tilbys åpne nettverk, kan det for enkelte oppleves som at en har en større grad av kontroll ovenfor risikoen en utsetter seg for. Det er eksempelvis opp til den enkelte å selv bestemme om en ønsker å koble seg på nettverket eller ikke, i tillegg til at det er opp til den enkelte å bestemme hva nettverket skal brukes til. Sistnevnte kan vi videre relatere til det Brun omtaler som aktiv-passiv dimensjonen og hvordan grad av frivillighet og kontroll påvirker menneskers risikoopplevelse (Brun, 1997).

På en annen side blir skillet mellom vanlige mennesker og eksperters risikoopplevelser større når vi ser på de informantene med mer kunnskap og informasjon på dette området. Selv med økt kunnskap om datasikkerhet gir disse informantene uttrykk for et komplekst og dynamisk trusselbilde der man aldri fullt ut kan få kontroll. Sistnevnte tydeliggjøres av den informanten som hevder det alltid er noen som er flinkere og kan mer (M6). På bakgrunn av vår undersøkelse og med henvisning til det utvalget vi har, kan empiriske funn indikere et skille mellom lekfolks og eksperters risikovurderinger. For lekfolk som ikke har samme forutsetning og informasjonsgrunnlag til å vurdere risikoen på samme måte som eksperter, kan det foreligge en viss naivitet der de vurderer sannsynligheten for å bli utsatt for digitale hendelser som liten.

### 4.3 Hva tenker du om sannsynligheten for å bli utsatt for en uønsket hendelse ved å benytte deg av nettet som tilbys?

På spørsmålet om folks sannsynlighetsvurdering av å bli utsatt for en uønsket hendelse ved bruk av åpne nettverk fikk vi ganske så varierende svar.

32 av 33 besvarte spørsmålet, og av disse svarte hele 16 av respondentene (50 %) at de anså sannsynligheten som liten. Av disse er syv menn og ni er kvinner. Alle mennene hadde utdanning, alt fra fagbrev til doktorgrad, og aldersforskjellen strakk seg fra 24 til 66. Blant kvinnene hadde fem av ni, som anså sannsynligheten for en uønsket hendelse liten, kun utdanning fra videregående. Resterende fire hadde bakgrunn fra bachelor og mastergrad.

Fem av respondentene (16 %) svarte at de ikke hadde tenkt over sannsynligheten for en uønsket hendelse når de benyttet seg av det åpne nettverket. Av disse var tre menn og to kvinner. Alle respondentene som svarte at det ikke er noe de har tenkt over hadde enten bachelor eller mastergrad. K15 uttrykte følgende:

*"Helt ærlig har jeg ikke reflektert noe over risikoen."*

Det var også åtte personer - seks menn og to kvinner - som svarte at de anså sannsynligheten som stor. Dette utgjorde 25 % av de som svarte på spørsmålet. Av disse hadde én bakgrunn fra videregående, mens resten hadde høyere utdanning.

Vi hadde også noen som besvarte spørsmålet på andre måter enn nevnt ovenfor. To av kvinnene svarte at de tenkte at uønskede hendelser kan forekomme på åpne nett, men de så det ikke som en stor risiko at det var noe som kunne skje med dem. Dette illustreres i følgende utdrag:

*«Jeg tenker at det kan skje, men ser det lite trolig at det skal skje med meg.» (K14)*

En av kvinnene svarte også at hun anså åpne nettverk som mer risikofylt enn lukkede nettverk, men at hun ikke hadde noe forhold til hvor stor sannsynligheten for en uønsket hendelse er.

Selv om det var store forskjeller i hvordan respondentene vurderte sannsynligheten så vi at det gikk igjen at folk likevel reflekterer i en viss grad over hva de bruker nettet til. Flere av respondentene oppgir blant annet at de ikke ville logget inn i eksempelvis nettbanken på det åpne nettverket.

Når vi skal drøfte de ulike svarene på spørsmålet ovenfor går vi ut i fra det samfunnsvitenskapelige perspektivet på risiko. Vi er opptatt av hvordan respondentene opplever og forstår risikoen knyttet til det åpne nettverket, ikke en matematisk beregning av risikoen. Vi er ute etter å se deres individuelle risikoforståelse i forhold til spørsmålene vi har valgt. Videre ønsker vi å få innsikt i deres opplevde risiko da det har vist seg at den påvirker hvordan mennesker forholder seg til risiko (Boyesen, 2003).

Som det fremkommer ovenfor svarte halvparten av respondentene at de så sannsynligheten som liten for å bli utsatt for en uønsket hendelse ved å benytte seg av det åpne nettverket til Vy. At så mange var enige om at det er liten sannsynlighet for en uønsket hendelse kan ha flere årsaker. Blant annet kan eksponerings-dimensjonen forsøke å gi et svar på hvorfor folks

risikoopplevelse er som den er. K14 nevner at hun tenker det kan skje, men at det er lite trolig at det skjer med henne. Vi mennesker har en tendens til å tenke at uønskede hendelser har større sjanse for å inntreffe andre heller enn oss selv. Dette kan føre til at vi undervurderer sannsynligheten i en situasjon da vi setter oss selv utenfor risikogruppen (Brun, 1997).

Media har også stor makt over folks risikoopplevelse. K8 nevner blant annet at hun antar at det er liten sannsynlighet ettersom hun ikke har hørt så mye om faktiske hendelser. Man hører lite om enkeltindivider som opplever uønskede hendelser pålogget åpne nettverk og derfor anser man sannsynligheten som liten. Når en ikke hører eller leser om faktiske hendelser opptrer risikoen som liten ettersom tidligere uønskede hendelser ikke er tilgjengelige i hukommelsen. Dette påvirker igjen folks opplevde risiko da de større hendelsene som medfører store konsekvenser oppleves som mer sannsynlige enn de hverdagslige hendelsene (Brun & Kobbeltvedt, 2005).

Åpne nettverk er heller ikke en ny og ukjent risiko med økende ulykkestall. En er godt kjent med åpne nettverk og nettverk generelt da det er noe folk flest benytter seg av daglig. Da kan vi gå videre inn på aktiv-passiv dimensjonen. Opplevelsen av frivillighet og kontroll er en viktig dimensjon i forhold til hvordan folk opplever en gitt risiko. Ettersom nettverk er noe de fleste er godt kjent med kan en få en falsk følelse av kontroll. Det er heller ikke en risiko som blir påtvunget en, en kan velge å logge inn eller ikke. Denne frivilligheten kan også gjøre at folk opplever det som mer sikkert enn det gjerne er (Brun, 1997).

En kan videre anta at de som vurderer sannsynligheten som liten har tillit til nettverket Vy tilbyr, samt tillit til Vy som institusjon. Tillit fører til mer tillit, og tilegnes av erfaringer gjort over tid (Engen et al., 2016). K12 sier at hun ser sannsynligheten som liten ettersom hun aldri har opplevd noen uønskede hendelser. Hun har altså bare hatt gode erfaringer når det kommer til nettverket Vy tilbyr og ser derfor ingen grunn til å ikke stole på det. Fem av respondentene (M2, M11, M12, K4, K15) sier at de ikke har tenkt noe over sannsynligheten for en uønsket hendelse på nettverket. Dette kan tilsi at de har stor tillit til Vy som institusjon samt nettverk generelt og at de derfor ikke har tenkt over at det kan forekomme en uønsket hendelse.

Her kan medias fokus også spille inn. K15 nevner at hun ikke har tenkt noe over sannsynligheten og at hun logger på nettet uavhengig av om det er åpent eller lukket. Hun nevner også at hun har hørt om såkalt «hacking» som går utover organisasjoner, men ikke at

det er noe som rammer enkeltpersoner. Da kommer vi tilbake til tilgjengelighetsheuristikker, som påpeker at hendelser som er lett tilgjengelig i hukommelsen vurderes som mer sannsynlig enn hendelser som er mindre fremtredende i bevissthetsbildet. Ettersom hendelser på åpne nettverk som rammer enkeltpersoner ikke er tilstede i K15´s bevissthetsbilde kan det medføre at hun ikke opplever at det er risiko forbundet med handlingen (Brun & Kobbeltvedt, 2005).

8 av respondentene sier derimot at de anser sannsynligheten for en uønsket hendelse på det åpne nettverket som stor. Dette begrunnes blant annet med at de ikke stoler på Vy, noen har hørt om historier fra bekjente som har blitt utsatt for en uønsket hendelse eller fra media (M17, K2). En nevner at det er dårlig kvalitet på nettet og at han derfor tenker at det ikke er en prioritet for Vy og at det derfor gjerne heller ikke er sikret tilstrekkelig (M15), ellers nevner folk at uønskede hendelser kan skje over alt og at ingenting er 100 prosent sikkert (M6, M15).

For de som har hørt om historier enten fra bekjente eller media kan man anta at de anser sannsynligheten som stor i og med at uønskede hendelser ligger lett tilgjengelig i deres bevissthetsbilde. For M15 kan en tenke seg til at tillit kan spille en rolle i hvorfor han anser det som stor sannsynlighet for at en uønsket hendelse skal oppstå. Dette fordi tillit fører til mer tillit, hvis han da ikke har tillit til nettverket fordi det er så dårlig kan dette også føre til at han ikke har tillit til at det er sikkert. M6 og M15 stiller seg også kritiske til nettverket, men de nevner også at uønskede hendelser kan kje over alt og at ingenting er 100% sikkert. En kan ut fra dette anta at de ikke har liten tillit til Vy i seg selv som institusjon, men heller liten tillit generelt.

### 4.4 «Stoler du på at Vy gir deg et tilstrekkelig sikkert nettverk?»

Det siste spørsmålet i undersøkelsen, «stoler du på at Vy gir deg et tilstrekkelig sikkert nettverk», kan ses direkte opp mot de reisendes tillit til institusjonen. Også her har 32 av de totalt 33 intervjuobjektene svart på spørsmålet. Svarene deres kan i prinsippet deles grovt inn i tre: de som svarte ja, de som svarte nei, og de som ikke hadde et klart svar.

Det er 19 av 33 personer som svarte *ja* til at de stolte på at Vy ga dem et tilstrekkelig sikkert nettverk. Ettersom dette utgjør cirka 59 % av de som har svart, vil det altså si at majoriteten av intervjuobjektene har tillit til nettverkssikkerheten til Vy. Blant disse 19 var det 13 kvinner og seks menn. Av alle sammenlagt hadde 11 utdanning, mens de resterende åtte hadde fullført

videregående skole. 10 personer var yngre enn 40 år, mens ni var eldre. En interessant bemerkning er at ni av 19 sier de har tillit fordi det er Vy, som en stor, kjent og statlig institusjon, som tilbyr nettverket. Deriblant sier K14 følgende:

*«[Jeg] tenker at Vy, som er så stort, tilbyr et nettverk som er sikret godt nok. Det tror jeg de fleste som regel tenker, med tanke på hvilke klager og oppmerksomhet det kunne ha medført dersom det ikke var det.»*

På den andre siden var det ni personer (28 %) i undersøkelsen som svarte *nei* på spørsmålet om de stoler på sikkerheten til Vys internett. Her var åtte av ni menn, mens én var kvinne. Alle hadde utdanning, åtte fra universitetet/høyskole og én med fagbrev. Seks av disse ni respondentene var over 40, mens de resterende var 24, 25 og 38 år. Tre av ni sa at de kunne finne på å koble seg til åpne nettverk, til tross for at de ikke hadde tillit til sikkerheten.

Av de 32 svarene vi fikk, var det fire som *ikke hadde et klart svar* på dette spørsmålet. Disse fire utgjorde altså 12,5 % av det responderende utvalget, og bestod av to kvinner og to menn. Tre av fire hadde utdanning – én med yrkesutdanning og to med universitetsutdanning. Alderen lå på mellom 28-45 år, og kan sies å ligge rundt medianen av alle aldrene i undersøkelsen sett sammenlagt. Følgende sitater illustrerer grunnene til at folk ikke hadde et klart svar på spørsmålet:

*"Jeg vet ikke, jeg reiser ikke så mye med tog."* (M9)

"*Jeg vet ikke, jeg tenker det er litt opp til forbrukeren hvordan man bruker nettet"* (M10)

"*Jeg tenker ikke så mye over det ... Ser mer på hvilken informasjon de krever å få tilgang til. Jo mer de krever, dess mer skeptisk blir jeg." (*K13)

Ut fra svarene som er presentert over kan vi altså se at tilliten til Vys nettverkssikkerhet er gjennomgående god. Sett i sammenheng med kjønn kommer det frem at mennene her er litt mer skeptiske enn kvinnene, da det av ni personer er åtte menn og én kvinne som svarer nei på dette spørsmålet. Selv om vi ser et tydelig skille mellom kjønnsfordelingen, der kvinner kan sies å ha mer tillit enn menn, kan vi ikke generalisere disse funnene ettersom størrelsen på utvalget er såpass lite. Det samme gjelder for argumenter sett fra et utdanningsperspektiv.

Selv om det er interessant å se at alle de ni har høyere utdanning, blir utvalget igjen for tynt til å komme med et utsagn som tilsier at utdanning er en tyngende faktor for skepsisen til sikkerheten rundt åpne nettverk.

Informant M7 er én av de som svarer nei på spørsmålet om de stoler på nettverkssikkerheten hos Vy, og sier følgende: *«Nei. Går det an å stole på Vy?»*. Selv om vi ikke kan si noe sikkert om M7 sine tidligere opplevelser eller spesielle grunner til å ha mistillit til Vy, kan vi her se at mistillit til en institusjon kan føre til mistillit til institusjonens tilbud. På samme måte kan vi se hvordan tillit til institusjonen fører til mer tillit, til eksempelvis tilbudene, ved å se på de ni som sa de stolte på nettverkssikkerheten til Vy fordi det var en kjent og statlig institusjon. Disse påstandene kan sees i lys av Engen et al. (2016) sin forskning, som vi gjennomgikk i teoridelen.

Det er også interessant å se hvordan enkelte av intervjuobjektene kom med noe motsigende uttalelser i første og siste spørsmål i intervjuet. Eksempelvis svarte K5 «*ja*» på det første spørsmålet om vedkommende pleide å benytte seg av åpne nettverk. Når hun skal svare på om stoler på nettverkssikkerhet uttrykker hun: «*Jeg er litt usikker. Men jeg tenker egentlig nei på dette [spørsmålet]*.» Flere av de intervjuede kommenterte ved intervjuets slutt at de ikke hadde tenkt noe særlig på disse spørsmålene før da, og at det hadde fått dem til å tenke. Underveis i intervjuet med K7, observerte vi noe som kan sees sammen med dette. Da vi gikk bort til kvinnen bemerket vi oss at hun var inne på sosiale medier på mobilen, og fikk bekreftet at hun for øyeblikket var koblet til det åpne nettverket. Under samtalen med oss la hun bort mobilen, men idet vi kom til det siste spørsmålet, tok hun igjen opp mobilen og koblet seg fra det åpne nettverket. Alt dette kan sees opp mot nyhetsdimensjonen og styrkedimensjonen innenfor Boyesens (2003) teori om hva som kan påvirke folks risikoopplevelse, ved at ny informasjon om risikokilder og konsekvenser kan virke farligere enn det nødvendigvis er. Dersom intervjuobjektene under intervjuet ble presentert for et nytt tema de ikke har tenkt på før, kan det være at konsekvensene anses som større enn de kanskje er. Dersom konsekvensene anses som større enn de er, vil det videre kunne være med på å styrke folks følelse og opplevelse av risiko. Slik kan disse dimensjonene være en av grunnene til at enkelte delvis endret mening underveis, og at K7 til slutt valgte å logge seg av nettet.

## 5.0 Konklusjon

Hovedfunnene i studien vår konsentrerer seg rundt tillit. Det er vanskelig å si om det er Vy eller nettverket det er tillit til, men det er igjen viktig å påpeke at vårt fokus er på nettverket og ikke Vy som institusjon. Funnene våre viser at det generelt er høy tillit til nettverket Vy tilbyr. Et funn som riktignok går igjen er at informantene i større grad er skeptiske til å bruke nettverket til aktiviteter som inneholder mer sensitiv informasjon. Eksempler som ble nevnt var blant annet bruk av nettbank og nettverket i forbindelse med jobb. Vi kan se tendenser til at det er forskjeller knyttet til kjønn og utdanning i funnene vi har gjort, men ettersom utvalget vårt er relativt lite er det vanskelig å generalisere disse funnene.

Gjennom denne studien har vi fått et innblikk i folks oppfatninger og holdninger til åpne nettverk. Risikopersepsjonen knyttet til bruk av åpne nettverk på Vy viser oss at befolkningen generelt har høy tillit til tjenesten som tilbys. Dette kan vi se ved at 53% av informantene svarte at de logget seg på nettverket og 21% svarte av og til. Det kommer frem i studien at reisende har høy tillit til Vy som institusjon noe som er med på å styrke tilliten til nettverket. Dette viser oss at tillit og tilbøyeligheten til nettverket som tilbys henger sammen. Vi opplevde at flertallet forventet og stolte på at Vy tilbød et nettverk som var både bra nok og tilstrekkelig sikkert.

Selv om det generelt var høy tillitt til nettverket, viser studien at 25% av deltakerne i undersøkelsen ikke tar i bruk nettverket når de reiser. Av denne prosenten er flesteparten menn. Ut ifra dette kan vi konkludere med at i dette utvalget var menn i noe større grad mer skeptiske til tjenesten enn kvinner. Det var knyttet mest usikkerhet til tjenester som krevde mer sensitiv informasjon, som jobb og nettbank. Vi ser ikke noen betydelige forskjeller i svarene med bakgrunn i utdanning eller alder, men det kom frem at de som var mest skeptiske til å bruke nettverket var i stor grad de med IT-bakgrunn eller de som hadde spesiell kompetanse til å vurdere om nettverket var sikkert eller ikke.

Vi kan også se en sammenheng mellom personlige erfaringer tilknyttet digitale risikoer og den enkeltes oppfatning av risikoen for å bruke nettverket. De med høy kjennskap til risikoen, er naturlig mer skeptiske. Det samme gjelder de som har dårlige erfaringer eller har vært utsatt for en uheldig hendelse når vedkommende har vært koblet på et åpent nettverk. En god

andel av de som svarte de ikke tok i bruk nettverket, påpekte at dette ikke var på grunnlag av sikkerheten, men heller kvaliteten på nettverket som tilbys. Vi ser også en tydelig usikkerhet blant informantene, da flere av dem endret svar underveis i intervjuprosessen. Dette kan vise at flere har manglende informasjon og evne til å kunne vurdere et nettverk, og derfor blir usikre når de blir opplyst om risikoen det kan medføre å logge seg på.

Til tross for at empirien er basert på et lite utvalg, samsvarer funnene her med forventingene våre og teorien vi presenterte tidligere.

### 5.1 Videre forskning

Da vi begynte å analysere dataen vår, så vi at oppgaven kunne vinkles i flere retninger. I henhold til oppgavens omfang var vi nødt til å avgrense dens fokus til risikopersepsjon knyttet til Vys åpne nettverk. For videre forskning ville det vært interessant og gjennomført samme studie i en større by for så å sammenligne resultatene. Dette fordi flere av deltakerne presiserte at de anså det som en større risiko å logge seg på nettverket til Vy i Oslo eller større byer.

I studien kommer vi frem til at folk generelt har høy tillit til Vy som institusjon, noe som også gjenspeiler tilliten til nettverket som tilbys. Det ville vært interessant å se hvordan utfallet ble hvis man gjennomførte studien hos en institusjon folk hadde mindre kjennskap til.

Det ville også vært interessant å sett nærmere på betydningen av kjønn og utdanningsbakgrunn i en eventuell større studie hvor man inkluderte flere informanter for å i større grad kunne generalisere studien.

Referanseliste


Aven, T., Boyesen, M., Olsen, k. H., & Sandve, K. (2004). *Samfunnssikkerhet*. Oslo: Universitetsforlaget.

Boyesen, M. (2003). Risikopersepsjon-En innføring i fagfeltet. *Direktoratet for sivilt beredskap*.

Brun, W. (1997). Subjektive determinanter for lekfolks risikovurderinger. *Nordisk Psykologi, 49*(1), 1-11.

Brun, W., & Kobbeltvedt, T. (2005). Beslutningstaking i operative situasjoner. In J. Eid & B. H. Johnsen (Eds.), *Operativ psykologi* (pp. 155-178). Bergen: Fagbokforlaget.

Departementene. (2019). Nasjonal strategi for digital sikkerhet. Retrieved from https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Grimen, H. (2009). *Hva er tillit*. Oslo: Universitetsforlaget.

Justis- og beredskapsdepartementet. (2019). Digital sikkerhet. Retrieved from https://www.regjeringen.no/no/tema/samfunnssikkerhet-og-beredskap/innsikt/digital-sikkerhet/id2340011/

Norsk senter for informasjonssikring. (2018). Nasjonal undersøkelse om ID-tyveri. Retrieved from https://norsis.no/nasjonal-undersokelse-id-tyveri/

NOU 2015: 13. (2015). *Digital sårbarhet – sikkert samfunn*. Retrieved from https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

Thagaard, T. (2013). *Systematikk og innlevelse: en innføring i kvalitativ metode* Bergen: Fagbokforlaget.

Vondráček, M., Pluskal, J., & Ryšavý, O. (2018). Automated Man-in-the-Middle Attack Against Wi-Fi Networks. *The Journal of Digital Forensics, Security and Law: JDFSL, 13*(1), 59-80.

## Vedlegg I: Intervjuguide

1. Hvilket år er du født?
2. Hva er din høyeste fullførte utdanning?
3. Pleier du å benytte deg av det åpne nettverket når du reiser?
    a. Hvis nei: går du for andre løsninger?
4. Mener du at du er i stand til å vurdere om et åpent nettverk er sikkert nok?
    b. Hvorfor?
5. Hva tenker du om sannsynligheten for å bli utsatt for en uønsket hendelse ved å bruke nettet som tilbys?
6. Vil du si at du stoler på at Vy tilbyr deg et nettverk som er tilstrekkelig sikret?