UiO : Det juridiske fakultet

«Det er jo nesten umulig å ikke la seg lure»

En kvalitativ studie av nordmenns erfaringer med digital svindel

Lotte Føyn

Masteroppgave i kriminologi

Institutt for kriminologi og rettssosiologi

UNIVERSITETET I OSLO

Vår 2025

Antall ord: 41 177

«Det er jo nesten umulig å ikke la seg lure»

En kvalitativ studie av nordmenns erfaringer med digital svindel

Sammendrag

Tittel: «Det er jo nesten umulig å ikke la seg lure»: En kvalitativ studie av nordmenns erfaringer med digital svindel
Forfatter: Lotte Føyn
Veiledere: Silje Anderdal Bakken & Solveig Laugerud
Levert ved: Institutt for kriminologi og rettssosiologi (UiO), vår 2025

Digital svindel rammer millioner av mennesker verden over, og i Norge alene ble over 1,2 millioner mennesker svindlet på nett i 2022. Denne utviklingen gjør at Økokrim omtaler digital svindel som et alvorlig samfunnsproblem. Det har ikke bare store økonomiske konsekvenser for samfunnet, men også for enkeltindividene som rammes, ofte på et dypt og personlig plan. Til tross for at digital svindel er et økende problem, preges mye av forskningen på feltet av internasjonale studier og kvantitative undersøkelser. Vi vet derfor fortsatt lite om hvordan norske ofre faktisk opplever å bli svindlet, og hvilke konsekvenser dette får for livene deres. I denne masteroppgaven retter jeg derfor fokus mot norske ofre og deres erfaringer: Hva skjer egentlig når noen lures i et digitalt rom? Hva gjør det med dem? For å utforske dette gjennomførte jeg kvalitative dybdeintervjuer med elleve personer i ulike aldersgrupper, i håp om å gi en stemme til dem som ofte forblir usynlige i statistikken.

Funnene viste et komplekst bilde. Eldre ble ofte rammet via e-post og telefon, gjerne kombinert med identitetstyveri, mens yngre oftere ble svindlet gjennom sosiale medier og i forbindelse med netthandel. Felles for begge grupper var imidlertid familiesvindel, der svindleren utga seg for å være noen de stolte på. Sårbarhet for svindel handlet ikke bare om digitale ferdigheter, men også om livssituasjon, emosjonell tilstand, økonomi, tillit og tilfeldigheter, og ikke minst om svindlernes digitale kapital og evne til å manipulere. Konsekvensene strakk seg langt utover økonomiske tap, og mange opplevde skam, selvbebreidelse og svekket tillit til seg selv og andre. Disse følelsene ble ofte forsterket av negative møter med hjelpetjenester som fremsto lite forståelsesfulle. Samtidig fantes det også lyspunkter: støtte fra familie og venner, og ikke minst en vilje til å ta kontroll tilbake ved å endre egne digitale vaner i etterkant.

Oppgaven peker på hvordan digital svindel skaper en annerledes offeropplevelse, som utfordrer etablerte forståelser av hva slike hendelser innebærer. Selv om digital svindel ofte fremstilles som et fenomen med hovedsakelig økonomiske konsekvenser, viser det seg

imidlertid ved nærmere undersøkelse at den også kan ha dype eksistensielle følger for dem som rammes. Videre viser oppgaven at ofre for digital svindel utfordrer tradisjonelle forestillinger om hvem som regnes som et «ideelt offer», og det argumenteres derfor for at vi må tenke nytt, både når det gjelder teorier som Christies «ideelle offer» og hvordan samfunnet møter dem som rammes av digital kriminalitet. I en tid med stadig mer sofistikerte svindelmetoder og økt brukt av kunstig intelligens, understrekes behovet for et felles ansvar mellom enkeltpersoner og institusjoner for å forebygge digital svindel best mulig. Avslutningsvis oppfordres det til at videre forskning bør rette seg mot hjelpetjenesters rolle og forståelser, nye svindelmetoder, og hvordan ulike grupper opplever sin sårbarhet, for å styrke forebygging og bedre ivareta dem som rammes av digital kriminalitet.

Forord

Etter fem innholdsrike og lærerike år som kriminologistudent ved Universitetet i Oslo, er det nesten uvirkelig å tenke på at jeg nå leverer masteroppgaven min. Arbeidet med denne oppgaven har vært en intens, men givende prosess, full av både oppturer og nedturer, og det har vært spesielt meningsfullt å fordype meg i temaet digital svindel. Med innlevering av oppgaven avsluttes et viktig kapittel i livet mitt, og jeg er svært spent på hva fremtiden bringer. Før jeg setter det endelige punktum for dette arbeidet, vil jeg benytte anledningen til å takke de som har bidratt og støttet meg underveis.

Først og fremst vil jeg takke informantene mine. Tusen takk for at dere tok dere tid til å dele opplevelsene deres. Jeg sitter stor pris på det! Uten dere hadde ikke denne oppgaven vært mulig.

En stor takk går også til Kirsten Moe ved Seniornett, som hjalp meg med å komme i kontakt med noen av informantene.

Jeg vil også rette en stor takk til veilederne mine, Silje og Solveig. Deres engasjement, faglige innspill og konstruktive tilbakemeldinger har vært uvurderlige og bidratt til å løfte oppgaven. Jeg har satt stor pris på alle veiledningstimene, som ikke bare ga nye perspektiver og konkrete ideer å arbeide videre med, men også rom for refleksjon og gode samtaler gjennom hele prosessen.

En varm takk går også til alle medstudenter på rom 7123. Takk for alle pauser hvor vi har kunnet dele både felles frustrasjoner og oppturer. Jeg vil også rette en spesiell stor takk til Tone: Takk for alle de hyggelige lunsjpausene nesten hver dag, og for støtten og de gode rådene underveis.

Til slutt vil jeg takke familie og venner som har heiet på meg gjennom hele prosessen og tålmodig lyttet til all prat om oppgaven. En spesiell takk går til mamma, som har lest gjennom de siste utkastene og gitt verdifulle tilbakemeldinger.

Lotte Føyn *Oslo, 21.05.2025*

Innholdsfortegnelse

1 Introduksjon

Overskrifter som «18-åring svindlet for 48.000: - Jeg ble livredd», «Lillian vart svindla for over 300.000 – må pantsette huset», og «Agnete (20) ble svindlet for nærmere 170.000 kroner: - Svindlere opptrer stadig mer profesjonelt» (Bigset, 2023; Trøen & Strande, 2020: Eliassen, 2023) har preget nyhetsbildet de siste årene. Samtidig oppfordrer banker folk til å være ekstra på vakt, mens stadig flere mobiloperatører tilbyr abonnementer med ekstra beskyttelse mot digital kriminalitet. Det er kanskje ikke så rart, da Norsk senter for informasjonssikring i 2022 registrerte at over 1,2 millioner nordmenn hadde blitt svindlet på nettet (NorSIS, 2023). I tillegg økte antall anmeldelser av svindel med nesten 60 prosent fra 2013 til 2022 (Økokrim, 2023). På grunn av det store omfanget omtaler Økokrim (2023; 2024) digital svindel som et samfunnsproblem, mens Politiet (2023; 2024) advarer om at utviklingen utgjør en betydelig trussel. En lignende utvikling er også tydelig globalt. Millioner av mennesker verden over rammes av svindel begått helt eller delvis på nett (Button mfl., 2014b). Dette skyldes at digital svindel i stor grad er et grenseoverskridende fenomen, der svindlere ofte opererer fra utlandet og benytter seg av profesjonelle, organiserte kriminelle nettverk som retter seg mot ofre i ulike land, inkludert Norge. Som NRK viser i sin dokumentar *Svindelsentralen,* er det ofte ikke norske borgere som svindler andre nordmenn, men snarere et globalt nettverk av aktører med tilgang til avanserte verktøy og teknikker (Gundersen mfl., 2025). Denne globale dimensjonen gjør digital svindel til en særlig kompleks og vanskelig kriminalitetsform å bekjempe (Gillespie & Magor, 2020; Cross, 2019).

Denne utviklingen må sees i sammenheng med hvordan hverdagen vår har blitt stadig mer digitalisert. Norge har i løpet av få år fått en av verdens mest digitalt modne befolkninger, der 88 prosent av befolkningen mellom 16 og 79 år bruker internett daglig (St.meld. nr. 27 (2015-2016), s. 114), 96 prosent hadde tilgang på smarttelefon i 2021, og ni av ti brukte sosiale medier i 2022 (Økokrim, 2023). På verdensbasis er utviklingen lik. Nesten 4,7 milliarder mennesker, omtrent 60 prosent av verdens befolkning, er i dag aktive internettbrukere (Hawdon, 2021). Den teknologiske utviklingen har gjort det enklere å kommunisere, få informasjon og utføre daglige gjøremål (Partin mfl., 2022). I tillegg har internett og sosiale medier blitt viktige for å dekke sosiale og psykologiske behov, som å få tilhørighet, styrke selvtilliten og unngå ensomhet (Mikkola mfl., 2020).

Men selv om digitaliseringen har gitt en rekke fordeler, har den også skapt nye utfordringer. Internett brukes ikke bare til legitime formål, men har også blitt en plattform for svindel og annen kriminalitet (Jewkes & Yar, 2010, s. 2). Teknologien har gjort det enklere å utføre tradisjonell kriminalitet, samtidig som den har skapt en arena for fremveksten av nye former for kriminalitet (Näsi mfl., 2023). I en stadig mer digital hverdag, der vi hele tiden er pålogget, blir vi også mer synlige, lettere tilgjengelige, og dermed mer sårbare (Politiet, 2023; Økokrim, 2023).

Selv om alle som bruker internett kan bli utsatt for svindel, er personer med svake digitale ferdigheter særlig utsatte. Svindlere utnytter ofte manglende teknologisk kunnskap, da dette gir dem et større handlingsrom for å manipulere og utnytte ofrene (Politiet, 2023, s. 6). I Norge anslås det at rundt 660 000 personer har svake digitale ferdigheter (Digitaliserings- og forvaltningsdepartementet, 2024, s. 86). Dette gjelder spesielt eldre over 65 år og førstegenerasjonsinnvandrere fra ikke-vestlige land (St.meld. nr. 27 (2015–2016), s. 114). Her ser vi konturene av det «digitale skillet», nærmere bestemt det andre nivået i det digitale skillet («the second-level divide»), som handler om forskjeller i hvordan teknologi brukes. Slike forskjeller i bruk kan over tid gi ulik digital kompetanse. Yngre brukere, ofte kalt «digitale innfødte», har vokst opp med digitale verktøy og har derfor ofte gode digitale ferdigheter. Eldre, ofte omtalt som «digitale innvandrere», har derimot måttet lære seg teknologien senere i livet og bruker ofte teknologi mindre. Dette kan gjøre at de har lavere digitale ferdigheter (Prensky, 2001; Wang mfl., 2013). Disse forskjellene bekreftes også i flere studier, som viser at eldre generelt benytter færre digitale tjenester enn yngre. Mens unge ofte bruker sosiale nettverk, interaktive digitale plattformer og teknologi til underholdning og sosiale formål, er eldre mindre aktive på slike arenaer (Loges & Jung, 2001, s 556; Metallo & Agrifoglio, 2015, s. 869).

Utnyttelsen av slike sårbarheter har vist seg å få store konsekvenser. Kriminelle tjener milliarder ved å svindle enkeltpersoner, private selskaper og offentlige institusjoner. Det er ikke bare direkte økonomiske tap for ofrene, men også store kostnader ved etterforskning og rettshåndhevelse. I tillegg kan svindel ha skadelige effekter for ofrenes mentale og fysiske helse (Europol, 2023, s. 5-6). Blant nordmenn som rammes, er det mange som opplever store økonomiske tap, noe som ikke bare får betydelige konsekvenser for privatøkonomien og livet deres, men også livet til deres familier. Dette kan igjen føre til belastninger utover det

økonomiske (Politiet, 2024, s. 37). Mange ofre for svindel sliter for eksempel med sterk skamfølelse og depresjon (Økokrim, 2023, s. 4).

Det er denne virkeligheten oppgaven tar utgangspunkt i. Digital svindel er et komplekst og raskt voksende samfunnsproblem, med alvorlige konsekvenser for både enkeltpersoner og samfunnet. Det handler om teknologi, men også om tillit og sårbarhet i en digital hverdag. I denne oppgaven rettes derfor fokuset mot ofrene og deres opplevelser.

1.1 Forskningsspørsmål

På bakgrunn av dette har jeg valgt å undersøke hvordan eldre og yngre innbyggere i Norge opplever å bli utsatt for digital svindel, og om det finnes noen forskjeller mellom aldersgruppene. Særlig ønsker jeg å utforske om det er det digitale skillet, med ulikheter i digitale ferdigheter og bruksvaner, eller andre faktorer, som livssituasjon og økonomi, som påvirker hvordan svindelhendelser forstås, forklares og håndteres.

Dette har ledet til følgende forskningsspørsmål:

> **«Hvilke typer digital svindel har eldre og yngre innbyggere i Norge opplevd, og hvilke likheter og forskjeller finnes det i hvordan de forstår, forklarer og reagerer på slike hendelser?»**

Målet med dette spørsmålet er å få frem hvilke former for svindel ulike aldersgrupper har opplevd, og hvordan alder kan prege både opplevelsen av å bli svindlet og håndteringen av slike hendelser. Mens «forstår» og «forklarer» viser til hvordan informantene oppfatter sin egen sårbarhet og årsakene til at de ble utsatt, viser «reagerer» til hvordan de opplevde og håndterte selve svindelen, samt forholdt seg til de ulike konsekvensene de opplevde i ettertid. Slik gir spørsmålet rom for å utforske nyanser i opplevelsene deres.

1.2 Oppgavens struktur

Oppgaven består av åtte kapitler. **Kapittel 1** innleder oppgaven og presenterer oppgavens problemstilling. **Kapittel 2** skisserer bakgrunnen og konteksten for oppgaven. Det redegjøres for hvordan svindel har utviklet seg i takt med den teknologiske utviklingen, og hvordan dette har bidratt til fremveksten av nye former for digital svindel som utgjør en økende trussel i det norske samfunnet. Videre presenteres de vanligste svindeltypene og teknikkene som benyttes i Norge i dag. I tillegg blir det presentert tidligere forskning som er relevant for oppgavens tematikk. Dette inkluderer forskning på sårbarhet for svindel, konsekvenser for ofre, og

aldersforskjeller i opplevelser og reaksjoner på svindel. Til slutt reflekteres det over hva oppgavens bidrag til feltet vil være.

I **kapittel 3** redegjøres det for hvordan sosiotekniske perspektiver, som digital kriminologi, digital kapital og digital habitus, samt offerteorier, som Christies teori om det «ideelle offer» og mestringsteori, kan anvendes for å forstå fenomenet digital svindel.

I **kapittel 4** redegjøres det for hvorfor kvalitative dybdeintervjuer ble valgt for å undersøke informantenes erfaringer. Deretter beskrives prosessen fra rekruttering til det endelige utvalget, utviklingen av intervjuguiden og gjennomføringen av intervjuene. Videre presenteres den analytiske fremgangsmåten, med særlig vekt på transkribering og bruk av tematisk analyse. Det gis også en vurdering av studiens datakvalitet, inkludert refleksjoner rundt validitet, overførbarhet og reliabilitet. Til slutt reflekteres det rundt sentrale forskningsetiske hensyn som har vært relevante i planleggingen og gjennomføringen av prosjektet, herunder informert samtykke, anonymitet og potensiell skade ved deltakelse.

Kapittel 5 og **kapittel 6** utgjør oppgavens analysekapitler. I disse kapitlene blir informantenes erfaringer med digital svindel sett i lys den tidligere forskningen beskrevet i kapittel 2 og det teoretiske rammeverket beskrevet i kapittel 3. Det første analysekapittelet handler om hvilke svindeltyper informantene har opplevd, samt hvordan de forklarer sin sårbarhet for digital svindel. Det andre analysekapittelet fokuserer på konsekvensene informantene opplevde som følge av svindelen, både økonomisk og emosjonelt. Det blir vist hvordan møtet med politi, banker eller sosiale omgivelser resulterte i støtte eller stigma, og hvordan svindelen påvirket informantenes digitale vaner og teknologibruk i etterkant.

Kapittel 7 diskuterer implikasjonene av oppgavens funn i en bredere teoretisk og samfunnsmessig kontekst. Det legges vekt på hvordan ofre for digital svindel utfordrer synet på det «ideelle offeret», og at det kan være et behov for bedre forebygging og håndtering av digital svindel, spesielt i møte med utfordringer skapt av fremveksten av kunstig intelligens.

Kapittel 8 utgjør oppgavens konklusjon og avslutning, med en oppsummering av hovedfunn og anbefalinger for videre forskning.

2 Bakgrunn og tidligere forskning

I dette kapittelet presenteres bakgrunnen og konteksten for oppgaven, med mål om å tydeliggjøre kunnskapsstatusen på feltet og skape forståelse for fenomenet digital svindel.

Det redegjøres først for hva som kjennetegner henholdsvis tradisjonell og digital svindel, med særlig vekt på de mest utbredte svindeltypene og metodene brukt i en norsk kontekst. Fremstillingen baseres på rapporter fra Politiet («Cyberkriminalitet 2023» og «Cyberkriminalitet 2024»), Økokrim («Årsrapport 2023» og «Bedrageri – et samfunnsproblem»), og NorSIS («Nordmenn og digital sikkerhetskultur 2023»). Det inngår også data fra en spørreundersøkelse gjennomført i 2024 av analyseselskapet Cint, blant 3010 norske internettbrukere i alderen 18-74 år. Undersøkelsen ble utført på vegne av NordVPN, en kommersiell aktør innen digital sikkerhet og personvern (Zieniūtė, 2024). I tillegg inngår funn fra en rapport fra forskningsprosjektet SODI (Samfunnssikkerhet og digitale identiteter), som bygger på kvalitative data fra personer som har opplevd misbruk av elektronisk ID (Brataas, Stokke & Svensson, 2022). Deretter blir det belyst hvordan teknologisk utvikling har påvirket sårbarhet for kriminalitet, og hvilke omstendigheter som kan forklare sårbarhet for digital svindel. Det ses også nærmere på hvilke konsekvenser slike hendelser kan ha for ofrene, og hvordan de håndterer dem. Dette er ikke ment som en uttømmende redegjørelse av all tidligere forskningslitteratur, men snarere litteratur som er relevant for oppgavens problemstilling. Avslutningsvis reflekteres det over hva denne oppgaven kan tilføre det eksisterende forskningslandskapet.

2.1 Digital svindel: utvikling og særtrekk

2.1.1 Tradisjonell versus digital svindel

Svindel, også kalt bedrageri, innebærer å lure et offer til å gi noe av verdi til en lovbryter, for eksempel personlige detaljer eller tilgang til en persons bankkontoer (Økokrim, 2023, s. 10). I straffeloven defineres det som å fremkalle seg en uberettiget vinning (Straffeloven, 2005, §371 a-b). Den teknologiske utviklingen de siste årene har imidlertid endret måtene svindel begås på. Internett, eller cyberspace, «the realm of computerized interactions and exchanges» (Yar & Steinmetz, 2019, s. 4), har blitt en sentral arena for gjennomføringen av svindel (Cross mfl., 2016, s. 1). Dette skyldes blant at internett har gjort det enklere å begå svindel, ved å fjerne geografiske barrierer og muliggjøre kontakt med mange ofre samtidig, noe som gjør at svindel nå kan begås i mye større skala (Cross, 2020a, s. 360-361).

På grunn av dette kan digital svindel ses på som en form for cyberkriminalitet, som vil si at det er et lovbrudd som enten skjer i eller er muliggjort av et nettbasert miljø og teknologi (Näsi mfl., 2023, s. 284). Mer spesifikt omtales gjerne digital svindel som en cyberaktivert forbrytelse, altså en tradisjonell forbrytelse som blir begått på nye måter ved hjelp av

teknologiske virkemidler. Dette skiller seg fra cyberavhengige forbrytelser, som kun kan begås ved bruk av datamaskiner og datanettverk, for eksempel spredning av virus (Furnell & Dowling, 2019, s. 14-15).

Selv om digital svindel skiller seg noe fra tradisjonell svindel, som historisk sett har vært en «ansikt-til-ansikt»-hendelse, der offeret og lovbryteren var i umiddelbar nærhet av hverandre (Cross, 2020b, s. 359), er det viktig å understreke at digital svindel likevel har flere likheter med tradisjonell svindel. Svindlere bruker for eksempel de samme teknikkene som i tradisjonell svindel, bare at det nå blir benyttet nye verktøy i utføringen (Holt & Holt, 2025, s. 149-150). Eksempler på slike verktøy er digitale kommunikasjonsplattformer som e-post, telefon, tekstmeldinger og chat-tjenester. Disse plattformene gjør det lettere å utføre svindel og vinne tillit, fordi svindleren kan operere anonymt og skjule identiteten sin (Yar & Steinmetz, 2019, s. 14). I lys av dette har enkelte forskere beskrevet svindel som «old wine in new bottles» (Grabosky, 2001), fordi kjernen i handlingene er den samme, men formen er tilpasset nye teknologiske omgivelser.

Med dette som bakgrunn er det relevant å se nærmere på hvilke teknikker svindlere tar i bruk i digitale kontekster for å lykkes med svindelen. Først og fremst benytter de ofte sosial manipulering, som i korte trekk handler om å forlede en person til å gjøre noe vedkommende i utgangspunktet ikke ønsker (Politiet, 2024, s. 37). Videre bruker svindlere ofte falske identiteter, og utgir seg for eksempel ofte for å være autoriteter som banker eller politi, fordi slike forespørsler vekker mindre skepsis (Dove, 2021, s. 58). En annen vanlig teknikk er å fremstille noe som at det haster og må løses umiddelbart (Cross, 2022, s. 222). Dette kan utløse sterke emosjonelle reaksjoner, som frykt og panikk, en såkalt «visceral reaksjon», som reduserer evnen til kritisk tenkning og fører til impulsive beslutninger (Cross, 2015; Dove, 2021, s. 55). I tillegg utnyttes sosiale normer og egenskaper som gjør oss til mennesker, som ønsket om å være snill, hjelpsom og lovlydig, samt vise medfølelse. Svindlere kan for eksempel late som at de er et familiemedlem i nød. Til slutt prøver svindlere også å virke vennlige og høflige for å skape tillit og redusere ofrenes årvåkenhet (Dove, 2021, s. 56-58).

2.1.2 Digital svindel i norsk kontekst

Utviklingen i Norge reflekterer de internasjonale trendene, men har også særegne trekk. Først og fremst viser tall fra NorSIS (2023), som nevnt innledningsvis, at over 1,2 millioner nordmenn ble utsatt for digital svindel i 2022. Videre blir det vist at svindel rammer bredt på tvers av alder og sosial status, og at både privatpersoner og virksomheter rammes (Økokrim,

2024; Politiet, 2024). Dette bekreftes også i en undersøkelse gjennomført på vegne av NordVPN i 2024, hvor det kommer frem at 70 prosent av norske internettbrukere i alderen 18-74 år har blitt utsatt for en eller annen form for cyberkriminalitet de siste to årene. Dette plasserer Norge på andreplass blant de nordiske landene, hvor bare Danmark har en høyere andel med 78 prosent (Zieniūtė, 2024). Selv om svindel rammer alle aldersgrupper, finner NorSIS (2023) at unge voksne i alderen 18–34 år er særlig utsatt. Likevel finnes det mørketall, blant annet på grunn av mangelfull rapportering og få anmeldelser (Politiet, 2023, s. 13)

Digital svindel forekommer i mange former i Norge. Først og fremst er svindel i forbindelse med phishing utbredt (Politiet, 2024). Phishing innebærer for eksempel forfalskede e-poster eller meldinger som lurer brukere til å oppgi sensitiv informasjon (Politiet, 2023, s. 25). I slike meldinger og e-poster etterligner svindlere ofte kjente aktører eller noen man kjenner, og bruker profesjonelt språk eller logoer for å fremstå troverdige og vinne tillit (Jakobsson & Myers, 2007, s. 16-17). Phishing kan også skje via SMS (kalt smishing), eller telefon (kalt vishing), hvor spoofing, bruk av falske nummer eller identiteter, ofte er en vanlig teknikk (Politiet, 2023, s. 25).

En annen utbredt form for digital svindel er svindel i forbindelse med kjøp og salg på nett (Politiet, 2024), også kalt forbrukersvindel eller online-shopping svindel. Dette er en form for personlig svindel hvor forbrukere blant annet opplever å ikke få varer de har bestilt på nett (Reep-van den Bergh & Jungher, 2018, s. 1-2) eller hvor selgeren ikke er å oppdrive i etterkant av kjøpet (Politiet, 2023, s. 35). Dette bekreftes også av NorSIS (2023) som rapporterer at 11,3 prosent av deltakerne betalte for varer de aldri mottok.

Videre er ID-tyveri med påfølgende svindel utbredt (Politiet, 2024). Dette innebærer bevisst bruk av andres identitet og personopplysninger, vanligvis for å oppnå økonomisk fordel i den andre personens navn og til den andres ulempe eller tap (Reep-van den Bergh & Jungher, 2018, s. 2).

I tillegg til svindeltypene som allerede er nevnt, er også BankID-svindel, kjærlighetssvindel, svindel rettet mot eldre (også kalt Olga-svindel), investeringssvindel, og kryptovalutasvindel utbredt (Politiet, 2023; 2024). De senere årene har det også vært en økning i familiesvindel, noen ganger kalt «hei mamma/pappa»-svindel, hvor svindleren utgir seg for å være et familiemedlem (Finans Norge, 2024). Felles for både de tidligere nevnte og disse formene for

svindel, er bruken av sosial manipulering og villedning, der den kriminelle utgir seg for å være en annen enn den de er, ofte via digitale kanaler (Politiet, 2024, s. 37). Selv om disse svindeltypene er blant de mest vanlige, er det viktig å påpeke at ikke alle ofre er klar over hvordan svindelen har skjedd. I undersøkelsen til NorSIS (2023) oppga for eksempel 2,7 prosent av deltakerne at de ikke visste hvordan de hadde blitt svindlet.

Når det gjelder hvilke typer svindel de ulike aldersgruppene utsettes for, og hvordan dette skjer, viser en rapport om misbruk av elektronisk ID fra forskningsprosjektet SODI (Samfunnssikkerhet og digitale identiteter), at yngre aldersgrupper (19-30 år) er nesten dobbelt så utsatt for å oppleve identitetskrenkelse som eldre (61-67 år) (Brataas, Stokke & Svensson, 2022, s. 23). I tillegg blir det vist i undersøkelsen gjennomført på vegne av NordVPN i 2024, at yngre i alderen 18-34 år oftere blir utsatt i sosiale medier, noe som kan skyldes at de er de mest aktive brukerne av sosiale medier, mens eldre personer i større grad ble utsatt for svindel via telefon, enten gjennom anrop eller SMS-er (Zieniūtė, 2024). I likhet med dette finner Politiet (2023) at svindel mot eldre ofte starter med phishing, smishing eller telefonoppringninger.

2.2 Sårbarhet i den digitale tidsalderen

I tidligere forskning har det blitt rettet mye oppmerksomhet mot hvorfor mennesker blir utsatt for kriminalitet og hvilke faktorer som påvirker deres sårbarhet, en prosess som ofte omtales som viktimisering («victimization») (Walklate, 2011, s. 180). Begrepet sårbarhet beskriver i denne sammenhengen hvor stor risiko en person har for å bli utsatt for kriminalitet: jo mer sårbar en person er, desto høyere er risikoen for å bli et offer (Green, 2007, s. 92). I denne oppgaven tar jeg utgangspunkt i Fineman (2008; 2010; 2019) og Mackenzie (2013) sine perspektiver på sårbarhet.

Fineman (2010, s. 253) argumenterer for at sårbarhet er en universell og iboende egenskap ved mennesket, som ikke kan klassifiseres basert på basert på rase, kjønn eller etnisitet. Den er ofte utenfor menneskelig kontroll (Fineman, 2019, s. 53; Fineman, 2008, s. 9). Mackenzie (2013) videreutvikler perspektivet ved å understreke at sårbarhet ikke bare er en grunnleggende del av det å være menneske, men også kan være kontekstavhengig og situasjonsbetinget. Den kan forsterkes eller utløses av sosiale, politiske, økonomiske og miljømessige forhold, og påvirkes av faktorer som alder, kjønn og helsetilstand. I tillegg trekker hun frem at sårbarheten kan være kortvarig, midlertidig eller varig. For eksempel kan livshendelser som å miste jobben eller oppleve dødsfall i nær familie gjøre en person mer

sårbar i en gitt periode. Disse kildene til sårbarhet eksisterer ikke isolert, men kan henge sammen og forsterke eller utløse hverandre (Mackenzie, 2013, s. 39-40).

I en digital kontekst innebærer dette at alle borgere kan rammes av digitaliseringens negative konsekvenser, og at sårbarhet for cybertrusler ikke er begrenset til bestemte befolkningsgrupper (Ranchordas & Beck, 2025, s. 510). I forbindelse med dette trekker Kaufmann & Lomell (2025, s. 8) frem at teknologisk utvikling har gjort at det dukker opp nye former for sårbarhet og nye måter å bli utsatt for kriminalitet på nettet. Viktimiseringen som skjer i dag er preget av romløshet, hvor kriminelle handlinger skjer på tvers av tid og rom, og dermed blir vanskelig å unngå (Walklate, 2025, s. 501-502). Sosiale medier bidrar ytterligere til denne utviklingen med sin sosiotekniske struktur som fremmer interaktivitet, deling og samhandling på tvers av grenser, noe som skaper nye arenaer for svindel, trakassering og forfølgelse (Twigt, 2025, s. 461-463; Walklate, 2025, s. 503)

Det er imidlertid viktig å understreke at selv om teknologien har endret måten kriminalitet utføres på, representerer mye av den digitale kriminaliteten en videreføring av tradisjonelle kriminalitetsformer, og opplevelsene av å være et offer har fremdeles fellestrekk på tvers av tid (Walklate, 2025, s. 507). Samtidig skaper det digitale en kontekst der eksisterende lag av sårbarhet forsterkes, og nye former for sårbarhet, som digital og algoritmisk analfabetisme, dukker opp (Ranchordas & Beck, 2025, s. 515).

2.2.1 Sårbarhet for digital svindel

I tidligere forskning har det også blitt identifisert en rekke faktorer som kan påvirke sårbarhet for digital svindel. På individnivå peker flere studier på at faktorer som ensomhet, isolasjon, godtroenhet og grådighet (Cross, 2016), samt høy tillit til andre (Ross mfl., 2014), kan øke risikoen for å bli lurt. For eksempel kan ensomhet svekke dømmekraften, fordi man mister muligheten til å diskutere situasjoner med andre (Dove, 2021, s. 77). Høy tillit alene er ikke nødvendigvis avgjørende (Carter & Weber, 2010; Judges mfl., 2017), men kombinert med lav årvåkenhet eller impulsivitet kan det gjøre personer mer mottakelige for manipulasjon (Dove, 2021, s. 73-75). Å ha høy tillit kan også gjøre at man blir godtroende og stoler «blindt på andre» (Greenspan, 2009), noe som gjør det lettere for svindlere å manipulere personer til å handle mot sitt eget beste. Svindlere utnytter også ofte slike trekk ved å fremstå som troverdige aktører, for eksempel autoriteter. Siden folk ofte har høy ettergivenhet og lydighet overfor autoriteter, kan dette svekke kritisk tenkning og føre til at man tar raske, lite gjennomtenkte beslutninger (Dove, 2021, s. 69; Button mfl., 2014b; Fischer mfl., 2013).

Lignende funn har også blitt gjort i norsk kontekst. I undersøkelsen gjennomført på vegne av NordVPN i 2024 oppga 56 prosent av nordmenn at teknologiske og psykologiske ferdigheter hos svindlerne, for eksempel i form av falske nettsider og etterligning av kjente merker og selskaper, var den primære årsaken til at de falt for svindelforsøkene. Det var kun 25 prosent av deltakerne i denne undersøkelsen som innrømte at egen grådighet, overmot eller mangel på kunnskap om svindel og teknologi, var faktorer som spilte inn (Zieniūtė, 2024).

Videre har det blitt vist at kognitive skjevheter kan gjøre enkelte mer sårbare for svindel. En vanlig feiloppfatning er at svindel bare skjer med visse mennesker, gjerne de som «fortjener det» eller som oppfattes som mindre smarte, og at det derfor aldri ville skjedd med en selv (Cross, 2015). Dette henger sammen med det som kalles en rettferdig verdenstro, der man har en oppfatning om at verden er et rettferdig sted der folk får som fortjent (Lerner & Miller, 1978). Slike tankemønstre kan føre til at man blir mindre forsiktig, overser faresignaler, og overvurderer sin egen evne til å oppdage og avsløre svindel (Dove, 2021, s. 78).

Noe annet som kan svekke dømmekraften og øke mottakeligheten for svindel er negative livshendelser og omstendigheter vi befinner oss i, som skilsmisse, dødsfall, sykdom i familien, eller tap av jobb (Voce & Morgan, 2023; Emami mfl., 2019, s. 8). Dette er i tråd med Mackenzies (2013) forståelse av sårbarhet som midlertidig og situasjonsbetinget. Samtidig viser Sur mfl. (2021) at det ikke alltid er en direkte sammenheng mellom å ha opplevd noe vanskelig i livet og å rapportere at man har blitt svindlet. I studien deres så det først ut som at personer som hadde opplevd slike hendelser oftere ble svindlet, men når de tok hensyn til andre faktorer, som utdanningsnivå og økonomisk situasjon, forsvant denne sammenhengen. Dette understreker kompleksiteten i hvordan sårbarhet virker, og at mange faktorer spiller inn.

Demografiske faktorer, som alder, er også relevante sårbarhetsfaktorer. Forskningen på dette er imidlertid delt: Noen studier viser at yngre er mer utsatt (Whitty, 2019), mens andre finner at eldre voksne er særlig sårbare (James mfl., 2014; van Wilsem, 2013), eller at det ikke er noen tydelig sammenheng (Leukfeldt & Yar, 2016; Pratt mfl., 2010). Aldring kan for eksempel gjøre eldre mer sårbare på grunn av svekkede kognitive funksjoner, noe svindlere kan utnytte ved at det blir vanskeligere å skille ekte henvendelser fra svindelforsøk (Dove, 2021, s. 76-77). Sårbarheten kan også forsterkes av sosial isolasjon, helseproblemer eller begrensede digitale ferdigheter (Burton mfl., 2022). I tillegg kan økonomiske faktorer spille inn. Eldre med oppsparte midler, som pensjon, fremstår ofte som attraktive mål (Cross,

2015), mens eldre uten slike ressurser ofte ikke blir svindlet (Kerley & Coopes, 2002, s. 31). Dette betyr imidlertid ikke at alle eldre er sårbare, men at risikoen for å bli utsatt kan være høyere i denne gruppen på grunn av aldringsrelaterte faktorer (Dove, 2021, s. 76-77).

Videre har det blitt vist at digitale vaner kan påvirke sårbarheten for svindel både hos yngre og eldre (Parti, 2023). Hyppig bruk av internett, spesielt til netthandel og nettbank, kan gi økt risiko for svindel og identitetstyveri, fordi man blir mer synlig og tilgjengelig for potensielle lovbrytere (Pratt mfl., 2010; Van Wilsem, 2013; Voce & Morgan, 2023). Yngre brukere, som ofte er mer aktive på nett, fremstår derfor som mer sårbare enn eldre (Oksanen & Keipi, 2013), mens de som bruker nettet sjeldnere ser ut til å ha lavere risiko (Kemp & Perez, 2023). Denne risikoen forsterkes ytterligere når høy digital aktivitet kombineres med risikofylt atferd, slik som å dele personopplysninger, bruke offentlige nettverk eller åpne e-poster fra ukjente avsendere (Mesch & Dodel, 2018; Akdemir & Lawless, 2020). I tillegg kan informasjon delt på sosiale medier, som fødselsdatoer og bilder, misbrukes av svindlere for å skreddersy troverdige svindelforsøk. Bruk av smarttelefoner utgjør også en særskilt risiko, ettersom disse enhetene ofte inneholder sensitiv informasjon, blant annet i bank- og kommunikasjonsapper, samtidig som de er mer utsatt for sikkerhetsbrudd (Dove, 2021, s. 78-79).

I forlengelse av dette har det blitt vist at manglende digitale ferdigheter og lite kunnskap om sikkerhet og digitale trusler kan forsterke sårbarheten på tvers av aldersgrupper (Dove, 2021, s. 78-79). Dette gjelder spesielt eldre, som ofte har lite digital erfaring fordi de tar i bruk ny teknologi senere i livet (Parti & Tahir, 2023). Samtidig påpeker Ranchordas & Beck (2025, s. 509–510) at også unge personer med gode digitale ferdigheter kan være sårbare, spesielt når de står i krevende livssituasjoner som midlertidig reduserer evnen til å kritisk vurdering. Holt, Bossler & Seigfried-Spellar (2022, s. 508) understreker dessuten at digitale ferdigheter i seg selv ikke alltid beskytter mot cyberkriminalitet. Leukfeldt (2014) finner heller ingen sammenheng mellom digitale ferdigheter og risikoen for å bli utsatt for ulike former for cyberkriminalitet. Andre studier viser derimot at personer med høy digital kompetanse kan være mer utsatt, fordi de deltar i digitale aktiviteter der risikoen er større (Van Wilsem, 2013). På den annen side finner Graham & Triplett (2017) at høy digital kompetanse kan redusere sannsynligheten for å bli offer for phishing-svindel, fordi man lettere registrerer hvilke e-poster som er ekte og hvilke som er svindelforsøk.

Til tross for at personlige faktorer og atferd har betydning, påpeker Fonseca mfl. (2022, s. 760) at de fleste studier har blandede resultater, noe som også gjenspeiles i funnene ovenfor. I forbindelse med dette understreker Emami mfl. (2019) at personlige trekk alene ikke gir en tilstrekkelig forklaring på hvem som blir utsatt. I mange tilfeller er ikke ofrene spesifikt valgt ut, men rammes tilfeldig gjennom massemålretting, hvor svindlere sender svindelforespørsler til en stor mengde mennesker (Button mfl., 2014b; van't Hoff-de Goede mfl., 2021, s. 22; Leukfeldt, 2014). Dette støtter Finemans tanke om at sårbarhet er iboende i alle mennesker, og Walklates (2025) forståelse av viktimisering som «romløs», der svindel kan ramme hvem som helst fordi vi alltid er tilgjengelige via e-post, sosiale medier og netthandel.

Samlet viser dette at sårbarhet for digital svindel er kompleks, og formes av en kombinasjon av personlige egenskaper, demografiske forhold, livshendelser, omstendigheter, atferd, overbevisninger og lignende, og derfor kan skje med hvem som helst (Dove, 2021, s. 67). Sårbarheten for svindel vil derfor sannsynligvis variere fra person til person. Dette understreker Mackenzies (2013) beskrivelse av sårbarhet som et sammensatt fenomen, hvor flere faktorer virker sammen og forsterker hverandre.

2.3 Konsekvenser av digital svindel

I tillegg til at det har blitt forsket på hva som gjør eldre og yngre individer sårbare for digital svindel, har mye av den tidligere forskningen også undersøkt hvilke konsekvenser det å oppleve digital svindel kan ha for ofrene.

Først og fremst har det blitt vist at hendelsen kan ha økonomiske konsekvenser. I Norge rapporterte 30 prosent av deltakerne i undersøkelsen gjennomført på vegne av NordVPN i 2024 at de opplevde økonomiske konsekvenser (Zieniūtė, 2024). Økonomiske konsekvenser blir ofte delt opp i direkte og indirekte økonomiske konsekvenser. Et eksempel på en indirekte kostnad er tid og ressurser brukt for å løse problemet, mens et eksempel på en direkte kostnad er pengene man mister (Barton mfl., 2013, s. 270-272). Flere studier viser at de økonomiske konsekvensene varierer avhengig av den enkeltes økonomiske situasjon, mengden tapte penger, og hvilke ressurser de har for å få tilbake penger (Notté mfl., 2021; Cross mfl., 2016). For noen har tapet liten eller ingen innvirkning, for eksempel fordi bankene klarte å stoppe svindelen (Jansen & Leukfeldt, 2018), mens andre kan oppleve alvorlige konsekvenser som stor gjeld, og tap av livsparing og hjem (Notté mfl., 2021).

Flere studier viser også at ofre for svindel rammes emosjonelt og psykisk. Vanlige reaksjoner er skyld, skam, tristhet og sinne, men følelser som frustrasjon, bekymring, ensomhet og flauhet forekommer også (Cross mfl., 2016; Jansen & Leukfeldt, 2018). Noen opplever også angst, utrygghet online og offline, maktesløshet og svekket tillit både til seg selv, andre og samfunnet generelt (Notté mfl., 2021). Det samme har blitt vist i Norge, hvor 25 prosent av deltakerne i undersøkelsen gjennomført på vegne av NordVPN i 2024 opplevde langvarige psykiske konsekvenser som angst og redusert tillit til digitale tjenester (Zieniūtė, 2024). I alvorlige tilfeller kan svindel også føre til depresjon og selvmordstanker (Notté mfl., 2021; Cross mfl., 2016). Frykt for å bli utsatt igjen er også en vanlig følge (Borwell mfl., 2022, s. 946). Disse funnene understreker hvordan den psykiske belastningen kan variere fra kortvarig irritasjon til langvarig angst og lav tillit til andre (Jansen & Leukfeldt, 2018). Videre er fysiske symptomer som søvnmangel, hodepine, kvalme, hudproblemer og vekttap også rapportert, og regnes ofte som en del av den psykiske påvirkningen (Cross mfl., 2016; Jansen & Leukfeldt, 2018; Borwell mfl., 2022). Eldre ser ut til å være mindre utsatt for økonomiske tap, men opplever oftere sterke ikke-økonomiske konsekvenser, som sinne, forlegenhet og fysiske helseplager etter svindelen (Kemp & Perez, 2023). Ifølge Parti & Tahir (2023) oppleves den emosjonelle og psykiske belastningen ofte som tyngre enn det økonomiske tapet i seg selv. For mange oppleves det som mer belastende å erkjenne at de har blitt lurt, og at noen bevisst har utnyttet dem for egen vinning (Dove, 2021, s. 40-41).

Tidligere forskning har også belyst ofres erfaringer med å rapportere og søke støtte. Svindel har generelt lavere anmeldelsesrate enn tradisjonell kriminalitet (Cross, 2018b). Avgjørelsen om å rapportere påvirkes av individuelle, kontekstuelle og økonomiske vurderinger (Kemp, 2020). Vanlige barrierer er manglende tillit til politiets kompetanse (Cross mfl., 2016, s. 7-8), frykt for å ikke bli tatt på alvor (Kemp, 2020), tidligere negative erfaringer med henleggelser og manglende oppfølging (Reisig & Holtfreter, 2007), og forvirring om hvor man skal rapportere (Button mfl., 2012). Noen ofre opplever for eksempel å bli sendt mellom ulike aktører uten å få hjelp, kjent som «the merry-go-round effect» (Button mfl., 2009a; 2009b; Cross, 2018b). Andre grunner til å ikke rapportere inkluderer små økonomiske tap (Kemp, 2020), lav tro på at saken vil bli oppklart og tiden og innsatsen som er involvert i rapporteringen (Cross mfl., 2016, s. 7-8), eller at man ikke ser på seg selv som et offer (De Kimpe, 2020). Følelser som skam, skyld og flauhet, samt en frykt for å bli sett på som naiv eller godtroende er også vanlige grunner til at mange unnlater å dele eller rapportere (Parti & Tahir, 2023; Cross mfl., 2016; Dove, 2021, s. 41). Selv om mange ikke rapporterer, er det

likevel enkelte som gjør det for å oppnå rettferdighet, for eksempel at lovbryteren får en strafferettslig sanksjon, og for å forhindre at andre blir lurt (Cross, 2018b), eller fordi de håper på å få økonomisk erstatning (Cross mfl., 2016; Fonseca mfl., 2022).

Videre har det blitt forsket på hvilke reaksjoner ofre har fått fra hjelpetjenester og nære relasjoner. Mange opplever negative reaksjoner, ofte omtalt i litteraturen som «victim blaming», både fra politi, familie og venner, der de holdes ansvarlige for det de har blitt utsatt for (Notté mfl., 2021; Cross, 2016). Dette kan føre til isolasjon, følelser av skam, og en lavere tilbøyelighet til å søke støtte (Cross, 2015; Parti & Tahir, 2023, s. 14). Slik «sekundærviktimisering» i form av negativ respons fra samfunnet eller hjelpeapparatet (Jansen & Leukfeldt, 2018), kan også forverre den opprinnelige belastningen ofre allerede føler på (Cross mfl., 2016). Dersom offerets opplevelse ikke anerkjennes, kan det føre til følelser av maktesløshet, tvil, skam og at man stiller spørsmål ved sin egen fortelling (Pemberton mfl., 2019b, s. 406). Flere av informantene i Jansen & Leukfeldt (2018) opplevde for eksempel dårlig kommunikasjon og lite forståelse hos bankansatte, og å bli møtt med at det var deres skyld. Politiet ble ofte opplevd som lite tilgjengelige, med manglende tid og kompetanse, samt liten vilje til å følge opp. Flere av informantene ble heller ikke informert om fremdriften i saken, noe som skapte frustrasjon og usikkerhet. Samtidig rapporterte noen å bli møtt empati, forståelse og ekspertise, noe som bidro positivt til bearbeidingen av opplevelsen. Det samme gjaldt informantene i Cross (2018b), som hadde blandede opplevelser med hjelpetjenestene. Videre viser forskning at det er vanlig å oppleve skuffelse over at ingen ble straffet, selv når svindleren fortsatt var aktiv på nett (Notté mfl., 2021, s. 287). På grunn av slike opplevelser etterlyser flere ofre bedre støtteordninger og mer åpenhet rundt hvordan sakene deres håndteres, for å unngå gjentatt viktimisering (Cross, 2018c, s. 10-11).

Til slutt viser tidligere forskning at mange endrer atferden sin etter å ha blitt svindlet. Flere blir for eksempel mer forsiktige og tar flere forholdsregler i måten de bruker nettet på (Ngo mfl., 2020; Reyns mfl., 2016), spesielt fordi man har endret sitt syn på verden og mistet tilliten til andre (Dove, 2021, s. 40-41; Button & Brooks, 2009). Jansen & Leukfeldt (2018) fant for eksempel at ofre installerte eller oppdaterte antivirusprogrammer, unngikk å bruke enheten som ble brukt når hendelsen skjedde, og var mer oppmerksomme ved netthandel og bruk av nettbank. De sjekket også oftere kontosaldo, nettadresser og e-poster, og reduserte bruken av digital bank. Andre tiltak inkluderte å fjerne kredittgrenser, blokkere bruk av kort i

utlandet, åpne flere bankkontoer, ha lavere beløp på brukskonto, og være mer varsomme ved ukjente telefonsamtaler. For noen var disse endringene midlertidige og ble gradvis avviklet etter hvert.

2.4 Oppgavens bidrag

Selv om det, som vist ovenfor, finnes en økende mengde kvalitativ forskning på ofre for digital svindel internasjonalt, er dette fortsatt lite utforsket i en norsk kontekst. I Norge har forskningen hovedsakelig vært kvantitativ, med fokus på offerundersøkelser, med unntak av undersøkelsen til SoDI og undersøkelsen gjennomført på vegne av NordVPN. Slike kvantitative data kan gi begrenset innsikt i hvilke opplevelser ofre har. Det finnes også en norsk masteroppgave som undersøker hvordan politiet og andre aktører håndterer bedrageri rettet mot eldre, og hvilke konsekvenser disse aktørene oppfatter at ofrene opplever (Fjellengen, 2024). Denne studien tar imidlertid utgangspunkt i aktørenes perspektiv, ikke ofrenes egne erfaringer.

Min oppgave retter i stedet oppmerksomheten mot ofrenes egne erfaringer, og tilfører derfor ny kvalitativ empiri fra et offerperspektiv i norsk kontekst. Kvalitative metoder, som dybdeintervjuer, gjør det mulig å fange opp nyanser og erfaringsbasert innsikt som ofte forblir usynlige i kvantitativ forskning (Walklate mfl., 2019, s. 210-212). Selv om personlige fortellinger er subjektive og krever validering, samt at man ikke kan være sikre på at de er sanne eller ikke, er de likevel nyttige. De gir verdifull innsikt i hvordan ofre skaper mening rundt sine opplevelser, og hvordan kriminalitet oppleves i en sosial og kulturell kontekst (Pemberton mfl., 2019a, s. 392-395; Sandberg, 2010).

Et annet originalt bidrag er at jeg trekker inn det digitale skillet i analysen og diskusjonen. Powell, Stratton & Cameron (2018) mener at det er betydelige hull i dagens forskning på cyberkriminalitet. Blant annet trekker de frem at det er lite forsking som tar for seg hvordan sosiale ulikheter, eller det digitale skillet påvirker kriminalitet og sårbarhet (Powell, Stratton & Cameron, 2018, s. 21-22). Ved å bruke begreper som digital kapital og digital habitus, rammeverk som sjelden er brukt i denne konteksten, belyser oppgaven hvordan blant annet ulik digital kompetanse og bruk av digitale enheter kan øke eller redusere sårbarheten hos ulike grupper.

Til slutt er temaet også dagsaktuelt, da vi lever i et stadig mer digitalt samfunn hvor mange hverdagsaktiviteter skjer på nett og i det digitale rom. I tillegg er det der folk vil samhandle,

markedsplassen der folk vil kjøpe varer, der vi vil gjøre våre banktjenester, og hvor en stadig økende mengde forbrytelser vil bli begått i fremtiden (Butler, 2013, s. 449-450). Ved å belyse hva som påvirker sårbarhet for svindel, hvilke konsekvenser det har for ofre, samt hvordan cyberkriminalitet med sin teknologiske natur tilfører nye dimensjoner til offerets opplevelser, kan oppgaven bidra til utvikling av mer effektive forebyggende tiltak (Daigle & Muftic, 2016, s. 15), og danne grunnlag for bedre støtteordninger for ofre og politiske prioriteringer (Borwell mfl., 2021, s. 88-89). Oppgaven er også relevant for enkeltindivider, som ved å vite mer om hvordan svindel foregår, kan bli mer bevisst på sin atferd på internett og redusere risikoen for å bli utsatt (Daigle & Muftic, 2016, s. 14).

3 Teoretisk rammeverk

Med bakgrunn i forskningsspørsmålene presentert innledningsvis, som fokuserer på hvilke svindeltyper eldre og yngre har opplevd, og hvordan de forstår, forklarer og reagerer på slike hendelser, vil jeg i følgende kapittel redegjøre for de teoretiske perspektivene og konseptene som vil bli tatt i bruk i de kommende analyse- og diskusjonskapitlene. Jeg vil beskrive hvorfor de ulike teoretiske tilnærmingene egner seg godt til å belyse oppgavens forskningsspørsmål, og vise til begrensninger ved enkelte av dem der dette har betydning for hvordan de anvendes i oppgaven. Først presenteres digital kriminologi, digital kapital og digital habitus, som er perspektiver og konsepter som er nyttige for å belyse hvordan digital svindel oppstår i et samspill mellom teknologiske, sosiale og mellommenneskelige faktorer (Powell, Stratton & Cameron, 2018, s. 190). Deretter vil jeg presentere et utvalg offerteorier, nærmere bestemt Christies «ideelle offer» og mestringsteori. Disse er nyttige for å gi innsikt i ofrenes reaksjoner og forståelser, samt møtet med hjelpetjenester (Daigle & Muftic, 2016, s. 1; Halder, 2022, s. 2). Bakgrunnen for å kombinere et sosioteknisk perspektiv med et offerperspektiv, er for å få et helhetlig rammeverk som fanger både strukturelle og individuelle sider ved digital svindel. I tillegg utfyller perspektivene hverandre, og bidrar samlet til å belyse kompleksiteten i fenomenet.

3.1 Et sosioteknisk perspektiv

3.1.1 Digital kriminologi

Digital kriminologi referer til det raskt utviklende vitenskapsfeltet som anvender kriminologiske, sosiale, kulturelle og tekniske teorier og metoder for studiet av kriminalitet, avvik og rettferdighet i et digitalt samfunn (Stratton mfl., 2017, s. 27). Feltet ble blant annet utviklet som en kritikk mot en manglende forståelse av sammenhengen mellom teknologi og

samfunn blant tidligere perspektiver. Dette gjelder for eksempel kriminologer som forsket på cyberkriminalitet og overså rollen teknologi spiller i utsatthet for kriminalitet, samt de bredere sosiale og digitale ulikhetene knyttet til kriminalitet (Stratton mfl., 2017, s. 23). Et tydelig uttrykk for denne kritikken finnes hos kriminologen Sheila Brown, som understreker at ”there is quite simply no such thing as a ‘technological’ crime (such as a ‘cybercrime’) as distinct from an ‘embodied’ crime” (Brown, 2006, s. 236). Hun argumenter for at kriminalitet alltid oppstår som et resultat av samspill mellom mennesker, teknologi og samfunn, der grensene mellom det biologiske og teknologiske, det naturlige og sosiale, og det menneskelige og kunstige ofte er uklare (Brown, 2006).

En sentral del av digital kriminologi er derfor å forstå hvordan digital teknologi og digitalisering påvirker kriminalitet og kontroll, både når det gjelder lovbrudd, lovbrytere og ofre (Kaufmann, 2024, s. 252). Dette gjør at begrepet sosio-teknisk («technosocial») er sentralt i digital kriminologi. Begrepet handler om at kriminalitet i det digitale samfunnet oppstår i et samspill mellom teknologiske, sosiale og mellommenneskelige faktorer (Powell, Stratton & Cameron, 2018, s. 190). Denne tilnærmingen åpner for analyser som ikke kun fokuserer på teknologiens rolle, men også på hvordan menneskelig atferd, sosiale relasjoner og analoge faktorer påvirker kriminaliteten som skjer online (Kaufmann, 2024, s. 257-258; Stratton mfl., 2017, s. 24). Digital kriminologi gir dermed verdifull innsikt i teknologiens rolle i ulike former for kriminalitet og viktimisering (Powell, Stratton & Cameron, 2018, s. 190).

I denne oppgaven vil digital kriminologi bli brukt for å belyse hvordan teknologiske og menneskelige faktorer virker sammen i svindelhendelser, og hvordan dette samspillet former hvordan slike lovbrudd skjer. Perspektivet legger et viktig grunnlag for å forstå digital svindel som et sosioteknisk fenomen, og vil gjenspeiles gjennom hele oppgaven.

3.1.2 Digital kapital og digital habitus

Begrepene «digital kapital» og «digital habitus» bygger på Pierre Bourdieus (1986) konsept om kapital, der kapital forstås som ressurser som gir fordeler og kan akkumuleres over tid (Rughinis mfl., 2024, s. 52). Bourdieu (1986) beskriver tre grunnleggende kapitalformer: økonomisk, sosial og kulturell, som er essensielle for å forstå sosiale ulikheter. Et nøkkelbegrep hos Bourdieu er også habitus, som beskriver hvordan vaner og handlinger formes gjennom livserfaring og sosialisering (Ragnedda & Ruiu, 2020, s. 10-12).

Som følge av den teknologiske utviklingen vurderte Bourdieu allerede i sitt senere arbeid å inkludere teknisk kapital som en fjerde kapitalform (Bourdieu, 2005, s. 80; Verwiebe & Hagemann, 2024, s. 2). «Digital kapital» kan sees på som en slik videreutvikling. Park (2017, s. 27) definerer digital kapital som «a predetermined set of dispositions that influences how people engage with digital technology", mens Ragnedda (2018, s. 2367) beskriver det som "the accumulation of digital competencies (information, communication, safety, content-creation and problem-solving), and digital technology". Digital kapital omfatter dermed både ferdigheter og tilgang til digitale ressurser, samt bruksmønstre på internett (Park, 2017, s. 6). Denne kapitalformen bidrar ikke bare til å forklare ulikheter i digital deltakelse, men også hvorfor noen er flinkere til å bruke teknologi enn andre (Park, 2017, s. 63-64). Begrepet belyser også hvordan motivasjon, ferdigheter og sosial kontekst påvirker teknologibruk (Park, 2017, s. 17). Som andre kapitalformer kan også digital kapital akkumuleres og transformeres til andre kapitalformer (Ragnedda & Ruiu, 2020, s. 14).

For å forstå digital kapital må man også vurdere «digital habitus», individers vaner og oppfatninger om den digitale verden, formet av deres erfaringer på nettet. Digital habitus utvikles over tid og påvirker hvordan individer bruker teknologi, vurderer risiko og responderer på trusler (Rughnis mfl., 2024; Romele, 2021, s. 497). Etter hvert som samfunnet blir mer digitalt, samvirker digital habitus og digital kapital, og påvirker hvordan individer navigerer digitale situasjoner (Rughinis mfl., 2024).

Begrepene er særlig relevante for studier av digital svindel. Rughinis mfl. (2024) viser hvordan digital kapital kan påvirke oppfatning av risiko og sårbarhet for trusler. I forbindelse med dette fant Graham & Triplett (2017) at personer med høy digital kompetanse var mindre utsatt for phishing, fordi de i større grad klarte å skille mellom falske og ekte e-poster. Begrepene er også sentrale for å forstå det andre nivået i det digitale skillet, som handler om ulikheter i hvordan internett brukes (Ragnedda & Ruiu, 2020, s. 34-35). Dette skillet er, som nevnt innledningsvis, et av utgangspunktene for problemstillingen min, og jeg vil derfor bruke det senere for å diskutere om ulik digital kapital kan føre til ulik sårbarhet for svindel. Videre kan begrepet brukes til å belyse teknologiens rolle i ulovlige aktiviteter. Bakken mfl. (2022) viser for eksempel hvordan både selgere og kjøpere i ulovlige narkotikamarkeder på nett må ha digitale ferdigheter, for eksempel må de mestre digitale verktøy, og ha riktig atferd og måte å kommunisere på, for å navigere markedene. Tilsvarende kan svindlere ha høy

digital kapital, som de bruker for å manipulere ofre, mens ofrenes digitale kapital kan utnyttes. Dette vil jeg komme nærmere inn på senere i oppgaven.

Selv om disse konseptene kan være nyttige i denne oppgaven, eksisterer det imidlertid kritikk mot å etablere digital kapital som en egen kapitalform. Noen forskere mener at det digitale aspektet ved kriminalitet allerede dekkes av Bourdieus eksisterende kulturelle og sosiale kapital. Andre argumenterer derimot for at det digitale utgjør en ny dimensjon som skaper egne former for ulikheter, som ikke fullt ut fanges opp av de eksisterende kapitalformene. De mener derfor at digital kapital bør anerkjennes som en selvstendig kapitalform, og at den kan akkumuleres, gi fordeler, og konverteres til andre kapitalformer, på samme måte som de tradisjonelle kapitalformene (Ragnedda & Ruiu, 2020, s. 15–19). Til tross for kritikken vurderer jeg at begrepene er nyttige analytiske verktøy for å belyse hvordan digital kompetanse påvirker både svindlernes muligheter og ofres sårbarhet i en digital kontekst.

3.2 Et offerperspektiv

3.2.1 Christies «ideelle offer»

Den neste teorien jeg har valgt er teorien til kriminologen Nils Christie (1986) om det «ideelle offeret». Han deler inn i fem karakteristikker som påvirker om et offer kan anses som ideelt eller ikke: 1) offeret er svakt, 2) offeret gjorde handlinger som kan anses som rimelige når hendelsen skjedde, 3) offeret var et sted vedkommende ikke kan klandres for å være, 4) gjerningspersonen var «stor og slem», og 5) gjerningspersonen var ukjent, og hadde ikke noe personlig forhold til offeret (Christie, 1986, s. 19). Hva som utgjør et ideelt offer varierer imidlertid mellom kulturer, som hver skaper sine egne stereotyper om forbrytere og ofre (Nielsen & Snare, 1998, s. 30-31). Teorien ble for eksempel opprinnelig opprettet for å forklare ideelle ofre i en norsk kontekst, og da ble det ideelle offeret beskrevet som sannsynligvis kvinne, syk, veldig ung, veldig gammel, eller funksjonshemmet, eller en kombinasjon av disse egenskapene (Christie, 1986, s. 18-19). Hvis et offer oppfyller disse kjennetegnene, blir det gjerne sett på som et ideelt offer, og får støtte og sympati fra samfunnet. Motsatt kan fravær av slike kjennetegn, og en status som «ikke-ideelt offer», føre til at offeret opplever manglende anerkjennelse (Cross, 2018a, s. 243-244).

I tidligere forskning har det blitt vist at dette særlig gjelder ofre for digital svindel, som ofte blir ansett som ikke-ideelle ofre (se for eksempel Cross mfl., 2016). For å belyse hvorfor dette skjer har Cross (2018a) avendt Christies fem karakteristikker på ofre for digital svindel. Hun finner at den første karakteristikken, at offeret ofte er svakt, er tydelig. Eldre mennesker

blir ofte blir sett på som attraktive mål på grunn av deres økonomi og sårbarhet. Den andre karakteristikken, at offerets handlinger er rimelige, er mindre tydelig. Ofre for digital svindel holdes ofte ansvarlige for sine egne handlinger, selv om de ble manipulert. Den tredje karakteristikken, stedet der hendelsen skjer, byr på utfordringer. Internettbruk anses ofte som en risikabel aktivitet, noe som kan få offerets handlinger til å fremstå som mindre rimelig, og at de dermed bryter med Christies (1986) tanke om at offeret burde ha tatt nødvendige forholdsregler for å beskytte seg selv. Den fjerde karakteristikken, at lovbryteren er «stor og slem», passer godt: svindlere identifiserer aktivt sårbarheter hos offeret for å utnytte dette til egen økonomisk fordel. Den femte karakteristikken, ukjent lovbryter, er delvis oppfylt: svindlere bruker ofte falske identiteter. Imidlertid skapes ofte en opplevd personlig relasjon, som ved kjærlighetssvindel, noe som kompliserer vurderingen (Cross, 2018a, s. 249-256).

Selv om ofre for digital svindel oppfyller noen av Christies kriterier, bryter de med bildet av det ideelle offeret gjennom egne handlinger og den digitale konteksten. De blir ofte sett på som ansvarlige, til tross for at de i mange tilfeller har blitt manipulert. Som Jansen & Leukfeldt (2018) understreker, er det lettere å bli anerkjent som et «ekte» offer dersom handlingene fremstår som uunngåelige, eller dersom det antas at vedkommende trodde de handlet på riktig måte. Når denne typen forståelse mangler, og offeret blir ansett som et «ikke-ideelt» offer, kan det få alvorlige konsekvenser. Det kan blant annet føre til at man mister tilgang til støtte og rettslig hjelp (Cross, 2018a, s. 256-257), eller at man opplever sekundærviktimisering og ytterligere belastninger, for eksempel når egne erfaringer blir bagatellisert, eller når hjelpetjenestene ikke anerkjenner og tar ofrenes behov på alvor (Cross mfl., 2016; Button mfl., 2009a; 2009b). Slike konsekvenser tyder på at det er viktig å sikre at ofre har tilgang til nødvendig formell og uformell støtte og hjelp for å komme seg videre (Cross, 2018a, s. 259).

Med bakgrunn i dette vil jeg i denne oppgaven bruker Christies teori for å vurdere om mine informanter blir sett på som ideelle eller ikke-ideelle ofre, og hvilke konsekvenser dette har for dem. Som Green (2007, s. 96) påpeker, er Christies teori nyttig for å forstå hvordan både yngre og eldre kan bli sett på som mer eller mindre ansvarlige, og hvordan dette igjen påvirker om de blir oppfattet som «ekte» ofre. I tillegg er det nødvendig å reflektere over hvorvidt Christies karakteristikker fortsatt er like relevante i dag. Digital kriminalitet utfordrer eksisterende antakelser om hva som bør regnes som viktimisering, og hvem som passer inn i rollen som «typisk offer» (Goodey, 2005, s. 218-220). Dette gjelder kanskje

spesielt kriteriene om offerets handlinger og stedet der hendelsen skjer. Tidligere ble internettbruk ofte sett på som en risikofylt atferd, men i dag er digital tilstedeværelse en nødvendig del av hverdagen, for alt fra banktjenester til kommunikasjon. Det kan dermed være problematisk å tolke internettbruk som et uttrykk for uansvarlighet. På grunn av dette vil jeg i diskusjonskapittelet se nærmere på om Christies teori bør tilpasses en digital kontekst.

3.2.2 Mestringsteori

Mens Christies teori fokuserer mer på synet på offeret, er det også viktig å inkludere et perspektiv som ser på hvordan ofre reagerer på og håndterer konsekvensene av det de har opplevd, både før, under og etter hendelsen.

Å bli utsatt for en kriminell handling kan føre til et brudd i livshistorien, en «narrative rupture», som skaper en narrativ krise der offeret må finne nye måter å forstå seg selv på (Pemberton mfl., 2019b, s. 411). Etter en slik hendelse kan det å bli sett på som et offer oppleves som en uønsket tilstand, fordi det ofte forbindes med svakhet (Rock, 2002, s. 13-14). Mange søker derfor å forbedre og håndtere situasjonen gjennom ulike mestringsstrategier (Strobl, 2010, s. 13-14). Dette gjør mestringsteorien («coping theory») til Lazarus & Folkman (1984) relevant. Ifølge Lazarus & Folkman (1984, s. 131) handler mestring om hvordan mennesker kognitivt og atferdsmessig forsøker å håndtere situasjoner som oppleves som overveldende, for eksempel en kriminell handling. Mestring er en dynamisk prosess, som starter med en primærvurdering av hvor truende, stressende og utfordrende situasjonen er, og en sekundærvurdering av hvilke ressurser man har for å håndtere dem. Mestringsstrategier deles ofte inn i problemfokusert mestring, der man forsøker å gjøre noe med selve problemet, og emosjonsfokusert mestring, der man forsøker å håndtere følelsene som oppstår, for eksempel gjennom å ta avstand, meditere eller søke støtte fra andre (Lazarus & Folkman, 1984). Emosjonsfokusert mestring endrer ikke den objektive virkeligheten, men hjelper individer til å håndtere og kontrollere følelsene sine (Green mfl., 2010). Disse strategiene utfyller hverandre, og valg av strategi avhenger av om situasjonen oppleves som mulig å kontrollere og forandre eller ikke (Lazarus & Folkman, 1984). Målet med mestringsstrategier er å gjenvinne kontroll over hverdagen, helsen og livskvaliteten (Lazarus & Folkman, 1984; Strobl, 2010, s. 13-14).

For ofre for digital svindel er de emosjonsfokuserte mestringsstrategiene spesielt viktige. Forskning viser at sosial støtte fra familie, venner eller profesjonelle kan hjelpe med å

bearbeide hendelsen gjennom å få forståelse, råd og veiledning (Jansen & Leukfeldt, 2018; Cross mfl., 2016). Å fortelle om det man har opplevd kan hjelpe med å bearbeide traumer og gi mening til det man har opplevd. Reaksjonene etter svindel kan likevel være sammensatte og til dels motstridende. Mange ofre føler for eksempel skyld selv om de rasjonelt sett vet at de ikke har gjort noe galt. I slike tilfeller blir støtte fra omgivelsene særlig viktig. En støttende respons kan bidra til bedre mestring og hjelpe offeret med å gjenoppbygge sitt selvbilde. Motsatt kan negative reaksjoner fra omgivelsene, for eksempel at man blir tillagt skyld, føre til sekundærviktimisering, som forverrer offerets opplevelse. Dette illustrerer hvordan mestring ikke skjer i et vakuum, og ikke kun er avhengig av subjektiv oppfatning og tolkning av hendelsen, men også om hvordan omgivelsene tolker situasjonen (Christie, 1986, s. 17-18; Rock, 2002, s. 13-15). I tillegg viser dette at viktimisering må oppfattes som en prosess snarere enn en isolert hendelse (Strobl, 2010, s. 13-15).

En annen viktig emosjonsfokusert mestringsstrategi, som ofte fungerer for å håndtere og kontrollere vanskelige følelser som skyld og skam, er å benytte «accounts», språklige forklaringer som gis for å rettferdiggjøre, forsvare eller forklare en uventet eller uheldig atferd. Accounts deles ofte inn i unnskyldninger («excuses») og rettferdiggjøringer («justifications»). Unnskyldninger innebærer at man erkjenner at noe var galt, men fraskriver seg ansvar. Rettferdiggjøringer, derimot, innebærer at man tar ansvar, men hevder at handlingen likevel var riktig eller nødvendig i situasjonen (Scott & Lyman, 1968, s. 46-47). Bruken av accounts er spesielt relevant når svindelofre håndterer skam eller sosial fordømmelse. Mange forsøker i slike tilfeller å forklare hvorfor de ble lurt på en måte som gjør handlingene forståelige (Scott & Lyman, 1968, s. 51). Dette kan igjen bidra til å beskytte selvbildet.

I forlengelse av dette kan en annen viktig emosjonsfokusert mestringsstrategi være å tolke hendelsen som en transformativ læringsopplevelse fremfor nederlag. Som Pemberton & Mulder (2025) påpeker, kan visse livshendelser fungere som transformative erfaringer, fordi de gir innsikt som ikke kunne vært oppnådd uten selve opplevelsen. Dette støttes også av Jansen & Leukfeldt (2018), som fant at flere svindelofre beskrev erfaringen som en verdifull læringsopplevelse. På lignende måte viser Pemberton mfl. (2019a, s. 396-398) hvordan mennesker som har blitt utsatt for kriminelle handlinger ofte bearbeider og reflekterer over det de har opplevd, for å gjenvinne kontroll og utvikle en ny selvforståelse.

Som en problemfokusert mestringsstrategi velger mange å endre atferden sin etter å ha blitt utsatt for svindel. Dette innebærer for eksempel økt forsiktighet på nett, mer oppmerksomhet rundt hvordan svindel foregår (se for eksempel Button mfl., 2014a; Ngo mfl., 2020; Reyns mfl., 2016), eller mer konkrete tiltak som å installere eller oppdatere antivirusprogramvare og sjekke kontosaldo for avvik (Lai, Li & Hsieh, 2012). I tråd med dette viser Jansen & Leukfeldt (2018) at ofre ofte iverksetter en rekke sikkerhetstiltak for å redusere risikoen for gjentatt svindel, både i form av tekniske løsninger og endret brukeratferd.

4 Metode

I dette kapittelet redegjør jeg for alle de metodiske valgene som ligger til grunn for studien. Først blir det beskrevet hvorfor jeg valgte å bruke kvalitative dybdeintervjuer for å besvare forskningsspørsmålene. Deretter beskriver jeg prosessen fra rekruttering av informantene til det endelige utvalget, utviklingen av intervjuguiden, og gjennomføringen av intervjuene. Videre presenterer jeg den analytiske fremgangsmåten, med særlig vekt på transkribering og bruk av tematisk analyse. Jeg gir også en vurdering av studiens datakvalitet, inkludert refleksjoner rundt validitet, reliabilitet og overførbarhet. Til slutt reflekterer jeg rundt sentrale forskningsetiske hensyn som har vært relevante i planleggingen og gjennomføringen av prosjektet, herunder informert samtykke, anonymitet og potensiell skade ved deltakelse.

4.1 Kvalitativ metode og dybdeintervjuer

Jeg bestemte meg tidlig i prosessen for å benytte kvalitative dybdeintervjuer for å besvare studiens forskningsspørsmål. Semistrukturerte dybdeintervjuer muliggjør en kontekstualisert og detaljert forståelse av intervjudeltakeres følelser, personlige historier og erfaringer (Hennink, Hutter & Bailey, 2020, s. 116-117), samt innsikt i hvordan enkeltindivider opplever og fortolker hendelser de selv har vært involvert i (Skilbrei, 2019, s. 65-66). Denne tilnærmingen vurderte jeg som særlig egnet for å undersøke hvordan eldre og yngre opplever å bli utsatt for svindel på internett og via telefon.

Selv om valget falt på denne metoden, reflekterte jeg også over hvilke andre metodiske tilnærminger som kunne være godt egnet for studien. Jeg vurderte blant annet å gjennomføre en digital spørreundersøkelse med åpne spørsmål, supplert med kvalitative dybdeintervjuer, eller å analysere dokumenter som politirapporter eller lover. Likevel konkluderte jeg med at kvalitative dybdeintervjuer var best egnet, ettersom de gir direkte tilgang til informantenes erfaringer, noe som var hovedmålet med mine forskningsspørsmål. I tillegg ønsket jeg, som nevnt tidligere, å bidra med kvalitative data fra en norsk kontekst, ettersom mye av den

eksisterende forskningen på feltet, spesielt nasjonalt, i stor grad bygger på kvantitative data. Utvalget og måten jeg rekrutterte dem på presenteres i det følgende.

4.2 Datainnsamling

4.2.1 Rekruttering av informanter

For å rekruttere informantene valgte jeg å gjennomføre en strategisk datainnsamling, som innebærer målrettet utvelgelse av deltakere med visse egenskaper som var viktige for studien (Hennink, Hutter & Bailey, 2020, s. 92-93). Siden målet med studien var å undersøke erfaringer med digital svindel, var det grunnleggende kriteriet for utvalget at de hadde direkte erfaring med å bli utsatt for svindel. Årsaken til at jeg ønsket å intervjue dem med direkte erfaring var at jeg anså det som best med tanke på studiens forskningsspørsmål, samt at det kunne vært vanskelig å få en fullstendig forståelse av ofrenes personlige opplevelser dersom man for eksempel hadde intervjuet noen som jobber med problematikken.

Videre reflekterte jeg en del rundt hvem informantene skulle være, og hvem som skulle utgjøre utvalget. Jeg gikk inn med en tanke om å ha et utvalg eldre ofre (65 år og eldre) og et utvalg yngre ofre (18-35 år). Allerede i begynnelsen av rekrutteringsprosessen ble det tydelig at jeg hadde vært litt «streng» med avgrensningene av de to aldersgruppene, da jeg fikk tak i flere i aldersgruppen i midten. Selv om jeg anså det som nyttig med de to innledende gruppene for å gi et godt sammenligningsgrunnlag for å undersøke forskjeller og likheter mellom eldre og yngre ofre for digital svindel, ble det også tydelig at jeg ville miste innsikten fra aldersgruppen mellom 35-65 år. Jeg valgte derfor å utvide kriteriene og endre gruppene, slik at den yngre gruppen ble i aldersgruppen 18-55 år, mens den eldre gruppen ble i aldersgruppen 55 år og eldre.

For å få tak i informantene startet jeg først med å kontakte familie og venner, som deretter fortalte om studien min til sine bekjente. Disse kunne deretter kontakte meg hvis de ønsket å være en del av studien. Dette resulterte i at jeg fikk tak i fem informanter. Etter dette la jeg ut et innlegg på min personlige Facebook-profil, hvor jeg beskrev hva jeg forsket på, hvilke svindeltyper jeg fokuserte på, og at jeg ønsket å komme i kontakt med personer som har opplevd dette. Dette innlegget ble også delt av mine venner og bekjente, men resulterte dessverre ikke i noen informanter. Jeg valgte derfor å legge ut et tilsvarende innlegg, med visse endringer, i ulike grupper på Facebook. Dette kan ses på som en slags rekruttering gjennom annonsering i sosiale medier, det Hennink, Hutter & Bailey (2020, s. 105) beskriver som rekruttering via «advertisements». Jeg la ut innlegg i til sammen seks grupper. Fire av

disse var grupper hvor svindel ble diskutert, og hvor innleggene i stor grad handlet om advarsler om pågående svindel, men også hvor folk fortalte om sine svindelopplevelser. De to siste gruppene var grupper med mange medlemmer (omtrent 50 000), og grupper jeg ble anbefalt av venner å legge ut innlegg i. Grunnen til at jeg la ut innlegg i gruppene som diskuterte svindel, var at jeg anså det som sannsynlig at minst en eller flere i disse gruppene hadde opplevd svindel. Videre var grunnen til at jeg la ut innlegg i de to andre gruppene at de hadde mange medlemmer, men også fordi folk kan legge ut innlegg både anonymt og med navn, hvor de spør om tips på ulike problemstillinger, blant annet rundt sine opplevelser med digital svindel. På forhånd var dette en av metodene for rekruttering jeg trodde ville gi flest deltakere, men det resulterte ikke i noen informanter.

Bakgrunnen for å velge Facebook som plattform for rekruttering var at jeg tenkte at det ville være nyttig for å få tak i de yngre informantene, da de ofte bruker sosiale medier mer enn eldre. For å få tak i de eldre informantene anså jeg at rekruttering gjennom familie og venner var mest nyttig, da ikke alle eldre bruker Facebook. Det viste seg likevel at rekruttering gjennom familie og venner var mest nyttig for å få tak i begge aldersgruppene. Det var generelt mye vanskeligere å få tak i yngre enn eldre, noe som også påvirket at jeg utvidet aldersspennet for den yngre gruppen. Det er vanskelig å si noe konkret om hvorfor de yngre var vanskeligere å få tak i, men det kan kanskje skyldes at eldre oftere opplever reelle svindelforsøk, og derfor i større grad identifiserer seg som ofre. Yngre kan på sin side ha høyere terskel for å fortelle om slike opplevelser fordi de er flaue eller ikke ser på opplevelsen som en betydningsfull hendelse.

På grunn av disse vanskelighetene med å få tak i informanter i starten, begynte jeg å forsøke å rekruttere på andre måter. Jeg tok kontakt med Seniornett, som er en organisasjon som jobber med å sikre digital inkludering av seniorer (Seniornett, 2024). Jeg anså dette som en relevant organisasjon, og at det var mulig at noen av de eldre de hjelper kanskje hadde opplevd svindel før de deltok på kursene deres og fikk hjelp. Jeg fikk et positivt svar fra dem, og de delte informasjon om prosjektet mitt både på nettsiden sin og i nyhetsbrevet sitt som de sender til sine 9000 medlemmer (se vedlegg 4). Denne måten å rekruttere på kan ses på som en form for rekruttering via formelle nettverk og tjenester (Hennink, Hutter & Bailey, 2020, s. 102), og resulterte i at jeg fikk tak i fire informanter.

Etter dette hadde jeg fått tak i tre yngre og seks eldre informanter. Jeg ønsket derfor å få tak i flere yngre for å få jevnere balanse. Etter å ha blitt tipset av to familiemedlemmer om to

personer som hadde stått frem med svindelhistoriene sine i aviser, valgte jeg å kontakte disse og hørte om de kunne tenke seg å delta i studien. Jeg var heldig, og begge ønsket å være med. To personer ble derfor rekruttert fra aviser. Grunnen til at jeg tenkte at det var passende å spørre dem om dette direkte, var blant annet fordi de allerede hadde valgt å stå frem med historiene sine i offentligheten, noe som tydet på at de var åpne om opplevelsene sine, men også fordi jeg ville gi dem muligheten til å fortelle enda mer om sine erfaringer. I motsetning til medias ofte korte, og noen ganger overfladiske og «sensasjonelle» fremstillinger, gir forskning mulighet til få frem dypere og mer nyanserte forståelser av folks erfaringer. Videre fikk jeg tak i ytterligere to informanter gjennom den ene informanten rekruttert fra aviser. Den ene var en person som hadde kontaktet henne fordi de hadde opplevd noe lignende, mens den andre var en yngre person (sønnen til en kollega) som også ønsket å delta. Dette kan ses på som en form for snøballutvalg, der nye informanter ble rekruttert via eksisterende deltakere (Hennink, Hutter & Bailey, 2020, s. 104-105).

Totalt endte jeg derfor opp med tretten informanter, hvorav fem var yngre og åtte var eldre. Jeg opplevde dette som et godt antall informanter, da jeg etter de siste par intervjuene fikk en følelse av at jeg hadde oppnådd såkalt metning, som vil si stadiet der det ikke lenger dukker opp ny informasjon om forskningsspørsmålet (Hennink, Hutter & Bailey, 2020, s. 106-108). Jeg opplevde for eksempel at lignende svindelteknikker, svindeltyper og konsekvenser hadde blitt diskutert av flere, samtidig som det var forskjeller i hvordan svindelen ble opplevd og håndtert. Jeg anså derfor at jeg hadde fått et variert og nyansert datamateriale.

4.2.2 Det endelige utvalget

Selv om jeg gjennomførte tretten intervjuer, besto det endelige utvalget av elleve informanter. Dette var fordi det kom frem i intervjuene med to av informantene at de hadde blitt forsøkt svindlet, og hadde klart å stoppe svindelen. De dekket derfor ikke mitt inkluderingskriterium om at man måtte ha blitt svindlet. Det er også en grense mellom å oppgi sensitiv informasjon som kontonummer og bankID-informasjon og få dette misbrukt versus å hindre at det blir misbrukt. Selv om disse to informantene hadde informasjon om svindlernes teknikker, ble de samme teknikkene beskrevet av øvrige informanter. Jeg vurderte derfor at datagrunnlaget fortsatt var tilstrekkelig, og at ingen vesentlig informasjon gikk tapt.

Med disse to informantene utelatt, fikk jeg også en jevnere balanse mellom antall yngre og antall eldre informanter. Det yngre utvalget besto av gutt 18 år, kvinne 29 år, mann 37 år, kvinne 41 år og mann 55 år, og det eldre utvalget besto av kvinne 61 år, mann 68 år, kvinne

73 år, kvinne 76 år, kvinne 82 år og kvinne 85 år. Aldersspennet i utvalget var derfor fra 18-85 år, og syv var kvinner, mens fire var menn. De fleste informantene var fra Oslo og nærliggende byområder, bortsett fra en informant som var fra Møre og Romsdal. Blant det eldre utvalget var fem av informantene pensjonister, mens en fremdeles var i arbeid. Blant det yngre utvalget var en elev på videregående skole, mens de andre var i arbeid. De var alt fra lærere og frisører til eiere av restaurant- og takewaybedrifter. Det var derfor noen ulikheter mellom informantene når det gjaldt alder og yrke.

Det var likevel viktige fellestrekk mellom alle deltakerne i utvalget, nemlig at de alle hadde blitt utsatt for svindel i løpet av de to siste årene, med unntak av en som opplevde det for 6 år siden. Alle informantene deltok direkte i intervjuene, med unntak av kvinne 41 år. På grunn av helsemessige utfordringer hadde hun ikke anledning til å delta selv. I stedet intervjuet jeg hennes ektemann, som formidlet informasjonen om hendelsen på deres vegne. Han hadde vært tett involvert i situasjonen, både som støtteperson og som en også ble berørt av hendelsen, og opplevde derfor svindelen som en felles belastning. Selv om ektemannen kunne gi inngående beskrivelser av hendelsen, er det viktig å presisere at opplysningene ble formidlet gjennom han, og ikke direkte fra kvinnen selv. Det kan derfor ikke utelukkes at fremstillingene bærer preg av hans egne tolkninger, eller at han vektla aspekter som han selv opplevde som viktige. Jeg vurderte likevel at informasjonen var relevant for studiens formål, men tar forbehold om at dataene i dette tilfellet er indirekte og kommer fra en tredjepart. I analysen omtales opplevelsen likevel som «kvinne 41 år» sin, ettersom det er hennes erfaring som beskrives. I tillegg er enkelte sitater lett språklig bearbeidet, slik at det fremstår som at kvinne 41 år selv forteller. Innholdet er ikke endret, men enkelte formuleringer er justert, for eksempel ved å bytte ut ord som «hun» med «jeg». Dette er gjort for å ivareta informantens perspektiv, og samtidig sikre en sammenhengende og leservennlig fremstilling. Slike tilpasninger er i tråd med faglige anbefalinger om å gjøre sitater mer forståelige, uten å endre innholdet eller informantenes uttrykksmåte (Kvale & Flick, 2007).

Et annet inkluderingskriterium var at informantene skulle være digitale i en eller annen grad, for eksempel eie en digital enhet, siden de ble utsatt for svindel via internett og telefon. Informantene varierte i sin digitale tilstedeværelse, både når det gjaldt hvor mye de brukte digitale enheter, hva de brukte dem til, og hvor ofte. De eldre informantene eide stort sett TV, mobiltelefon, PC og i noen tilfeller nettbrett, men bruken var begrenset. De fleste eldre brukte digitale enheter en time daglig eller mindre, i hovedsak til å sende meldinger, ringe, lese

nyheter, bruke nettbank, og til lett underholdning som å spille kabal. Enkelte, som mann 68 år og kvinne 61 år, hadde en mer aktiv digital hverdag med 6-7 timer daglig skjermtid, mens kvinne 85 år kun brukte én time per uke. Facebook var den mest brukte sosiale plattformen blant de eldre, men bruken var begrenset sammenlignet med de yngre informantene. De yngre informantene hadde en mer omfattende digital hverdag, med høyere skjermtid og flere enheter i bruk. De fleste eide mobil, PC og nettbrett, og en hadde også spillkonsoller. Bruken varierte fra tre til ti timer daglig, noe som kan henge sammen med at mange fortsatt er i jobb eller tar utdanning. Mange benyttet digitale enheter til både arbeid og fritid, med utstrakt bruk av sosiale medier som Facebook, Instagram og Snapchat, samt bank- og kommunikasjonsapper som Vipps, e-post og Teams. Det var også noen unntak. Kvinne 41 år var for eksempel mer passiv i sin digitale tilstedeværelse, selv om hun hadde flere av de andre plattformene. I tillegg brukte mann 37 år sjelden PC. Denne variasjonen i digital tilstedeværelse er relevant for den senere diskusjonen, både for å undersøke sammenhengen mellom digital tilstedeværelse og utsatthet, men også hvilke endringer informantene gjorde i etterkant av hendelsen.

4.2.3 Intervjuguide

I forkant av intervjuene utarbeidet jeg en intervjuguide (se vedlegg 3) for utvalget mitt, som skulle brukes som et hjelpemiddel underveis i intervjuene for å veilede samtalen i riktig retning (Hennink, Hutter & Bailey, 2020, s. 118-119). Jeg ønsket en naturlig samtale mellom meg og informantene, og å ikke være for låst til intervjuguiden og de planlagte spørsmålene. Intervjuguiden ble derfor brukt mer som en slags struktur for selve intervjuet, og en huskeliste for meg selv, som jeg kunne sjekke underveis i intervjuene, fremfor noe jeg fulgte slavisk (Skilbrei, 2019, s. 127). Det er flere fordeler med å lage en intervjuguide i forkant. Thagaard (2019, s. 97) trekker for eksempel frem at det hjelper med å holde spørsmålene åpne, fremfor ledende. Dette gjør at informantenes svar ikke blir begrenset, og at spørsmålene er konsentrert rundt tematikken og problemstillingen. I tillegg var det positivt å ha intervjuguiden dersom samtalen stoppet opp eller informantene gikk for langt vekk fra temaet (Skilbrei, 2019, s. 126).

Når det gjelder utformingen av intervjuguiden, tok jeg utgangspunkt i den tematiske strukturen som beskrives hos Tjora (2021, s. 169-172) og Thagaard (2019, s. 95). Intervjuguiden ble derfor delt inn i ulike hovedtemaer, der hvert tema hadde tilhørende underspørsmål for å utdype informantenes erfaringer. Spørsmålene og intervjuguiden for de

yngre og eldre informantene var like, da jeg ønsket å få et godt sammenligningsgrunnlag til den senere analysen (Skilbrei, 2019, s. 126). Videre ble noen spørsmål utarbeidet etter inspirasjon fra det teoretiske rammeverket jeg hadde tidlig i prosjektet, fordi jeg ønsket å se på tematikken fra ulike teoretiske synspunkter (Hennink, Hutter & Bailey, 2020, s. 123). Rutineaktivitetsteori ble for eksempel brukt som inspirasjon til temaet «digitale vaner - bruk og rutiner på nett» i intervjuguiden. Selv om teorien ikke inngår i det endelige teoretiske rammeverket, ettersom dette utviklet seg underveis i møte med nye funn og observasjoner, viser dette likevel hvordan teori kan fungere som et nyttig verktøy i utviklingen av intervjuguider. I tillegg til å formulere spørsmål på denne måten, var andre spørsmål inspirert av tidligere forskning, for eksempel spørsmålene om sårbarhet og konsekvenser av hendelsen. Til slutt ble noen spørsmål formulert på grunn av min faglige nysgjerrighet. Ut ifra dette ble følgende temaer inkludert i intervjuguiden: (1) digitale vaner – bruk og rutiner på nett, (2) erfaringer og opplevelser, (3) risikofaktorer og årsaker til viktimisering, og (4) konsekvenser av hendelsen og tiden etter hendelsen.

Selv om jeg hovedsakelig utformet intervjuguiden for å optimalisere intervjuene, var dette også nødvendig for å få prosjektet godkjent av SIKT, nettopp fordi eldre innbyggere, men også ofre generelt, kan anses som sårbare grupper. Det var derfor viktig å utforme spørsmålene på en slik måte at det ivaretok de etiske aspektene overfor informantene.

4.2.4 Gjennomføring av intervjuene

Etter at jeg hadde vært i kontakt med informantene og de hadde sagt seg villige til å delta i prosjektet, begynte prosessen med å planlegge og gjennomføre intervjuene. Jeg begynte alltid med å spørre alle informantene om hvor de ville gjennomføre intervjuene, da jeg ønsket at de skulle føle seg komfortable. Det var viktig at de skulle føle at de var i et trygt rom hvor de kunne si alt de ønsket å komme inn på (Hennink, Hutter & Bailey, 2020, s. 125). Etter hva de foretrekk endte det opp med at intervjuene ble gjennomført hjemme hos dem (kvinne 82 år og kvinne 85 år), på kafe (kvinne 41 år og mann 37 år), via plattformene Zoom og Teams på grunn av avstand (mann 55 år, gutt 18 år, kvinne 61 år og mann 68 år), og over telefon (kvinne 73 år). Jeg opplevde det som trygt å gjennomføre intervjuene hjemme hos kvinne 85 år og kvinne 82 år, da dette var to av informantene som ble rekruttert via familie og venner som kjenner dem.

Jeg opplevde at det var best å ha intervjuene hjemme hos informantene og via telefon, Zoom og Teams, da det ikke var noen andre til stede, og dermed lite støy og distraksjoner. I

motsetning til dette var det mer støy på kafeene, samt flere mennesker til stede. Dette var noe som påvirket lydopptaket, og dermed transkriberingen min. Selv om det var andre mennesker til stede på kafeene, opplevde jeg at dette ikke påvirket intervjudeltakerne i vesentlig grad. De fortalte åpent og ærlig om det de hadde opplevd, og det virket ikke som at de holdt noe tilbake. I tillegg kan dette skyldes at vi fant plasseringer på kafeene hvor det var mer stille og færre til stede. Telefonintervjuene fungerte også godt. Selv om jeg ikke kunne se kroppsspråket, opplevde jeg at samtalene fløt naturlig og at informantene snakket åpent. I forlengelse av dette syntes jeg også at intervjuet som ble gjennomført med mann 55 år over Zoom fungerte bra. Det eneste som var litt uheldig var at det var noe feil med kameraet hans, som førte til at dette ikke var på underveis i intervjuet. Dette kan ha påvirket dynamikken og gjort at jeg ikke fikk sett kroppsspråket hans. I tillegg var det et lite øyeblikk, cirka 30 sekunder, hvor internettilkoblingen var dårlig og lyden stoppet. Dette er kjente ulemper ved digitale intervjuer (Thunberg & Arnell, 2022, s. 761-762). Dette informerte han likevel om med en gang, og ventet med å svare på spørsmålet og fortelle videre frem til internettilkoblingen var bra igjen. Jeg opplevde derfor at dette ikke påvirket dynamikken og intervjuet noe bemerkelsesverdig, men valgte likevel i de neste digitale intervjuene å benytte Teams istedenfor Zoom, for å unngå samme problemer igjen. På disse intervjuene fungerte alt bra, og jeg fikk muligheten til å studere både verbale og ikke-verbale signaler, noe Thunberg & Arnell (2022, s. 757-758) mener er en fordel ved digitale intervjuer.

Intervjuene ble gjennomført i løpet av en periode på fem uker i september og oktober. Som tidsrommet viser, ble noen intervjuer gjennomført tett etter hverandre. Dette ble blant gjort på bakgrunn av når det passet for informantene å møtes, og på grunn av reisevei, da noen intervjuer ble gjennomført i hjembyen min, og jeg anså at det var best å ha flere intervjuer samtidig når jeg først var der. Dette opplevde jeg likevel ikke som problematisk, da jeg alltid fikk gjort forberedelsene jeg skulle mellom hvert intervju. Jeg sørget for eksempel for at jeg hadde tid til å transkribere intervjuene enten samme dag de ble gjennomført, og maks en til to dager etter. I tillegg syntes jeg det var nyttig å ha intervjuene litt tett etter hverandre da dette gjorde at «hodet mitt var på riktig plass», og jeg kunne huske ting fra det forrige intervjuet som jeg kunne ta med meg videre til det neste. Jeg ønsket også å få tak i datamaterialet tidlig i prosessen, for å kunne ha nok tid til den påfølgende analysedelen.

Alle intervjuene ble tatt opp med diktafon, både fysisk og via app på mobilen. Det gjorde at det ble mulig for meg å få med meg alt som ble sagt, samtidig som jeg kunne lytte fokusert til

det informantene fortalte (Tjora, 2021, s. 180). Det ga meg også bedre forutsetninger til å kunne stille gode oppfølgingsspørsmål og å konkretisere utydelige spørsmål dersom det var noen. Jeg skrev ut informasjonsskrivet og samtykkeskjemaet på forhånd og tok det med til alle intervjuene. I tillegg sendte jeg disse på e-post til alle informantene i forkant av intervjuene. Før intervjuet gikk jeg alltid gjennom informasjonsskrivet og alle formalitetene, blant annet formålet med prosjektet, hva deltakelse ville innebære for dem, hvordan jeg ville sikre anonymitet, hvilke rettigheter de hadde, og at intervjuet ville bli tatt opp. Deretter ba jeg dem om å signere samtykkeskjemaet. På de digitale intervjuene ble samtykke gitt digitalt før intervjuet begynte, og i noen tilfeller fikk jeg også tilsendt bilde av printet versjon av samtykkeerklæringen med underskrift. I informasjonsskrivet hadde jeg anslått for informantene at intervjuet ville vare i 45 minutter til en time. Intervjuene hadde varierende lengde, og varte alt fra 35 til 60 minutter, avhengig av hvor konkrete informantene var og hvor mye de fortalte. Jeg opplevde at noen var korte og konsise i sine svar, mens andre kom med lengre og mer detaljerte svar.

Når det gjelder selve intervjuene mer konkret, begynte jeg alltid de fysiske intervjuene med å håndhilse og ha litt småsnakk, enten om prosjektet eller andre ting, for å skape trygghet og gjøre informantene komfortable. Videre stilte jeg noen få åpningsspørsmål, generelle spørsmål som stilles for å forbedre informantene på spørsmålene som kommer senere og for å gjøre dem mer komfortable med intervjusettingen (Hennink, Hutter & Bailey, 2020, s. 119). Disse spørsmålene gikk ut på om de kunne fortelle litt om seg selv og hvilke digitale enheter de eier. Deretter gikk vi over til å snakke om selve svindelopplevelsen. Her hadde jeg flere spørsmål, men ofte ble mye besvart mens de snakket om hendelsen, altså at de kom inn på mange av tingene jeg hadde tenkt til å spørre om. Jeg valgte derfor å bare stille oppfølgingsspørsmål der det trengtes og var naturlig. Noen informanter fortalte mye, og det trengtes derfor færre oppfølgingsspørsmål. I intervjuer med andre informanter trengtes det flere oppfølgingsspørsmål. Jeg brukte også flere prober og ord som «mhm», «ja» og «aha», samt blikkontakt underveis for å vise informanten at jeg fulgte med mens de snakket og var interessert i det de snakket om (Thagaard, 2019, s. 96). Alle kom likevel inn på alt jeg hadde med i intervjuguiden, noe som ga gode sammenlignbare data til den senere analysen og diskusjonen (Skilbrei, 2019, s. 126-127). Mot slutten av intervjuene stilte jeg også alltid noen få avslutningsspørsmål, for å runde av og lette avslutningen av intervjuet. Spørsmålene lot informantene få anledning til å utdype seg dersom de ønsket det eller å komme med

tilbakemeldinger på intervjuet (Hennink, Hutter & Bailey, 2020, s. 120-122). Disse spørsmålene handlet blant annet om informantenes tips til forebygging av digital svindel.

4.3 Analytisk fremgangsmåte

4.3.1 Transkribering

Det første som ble gjort for å klargjøre intervjuene for analyse var å transkribere dem, og jeg sørget for å transkribere intervjuene fortløpende underveis i datainnsamlingsprosessen. Dette ga meg muligheten til å vurdere om jeg skulle gjøre noen endringer i intervjuguiden. Jeg gjorde ikke store endringer, som å inkludere nye temaer, men jeg fikk lagt til noen nye underspørsmål om svindleren under temaet «erfaringer og opplevelser». Jeg la til dette fordi det var noe alle informantene kom inn på i en eller annen form, når de fortalte om det de hadde opplevd. I tillegg ble det mulig å fjerne unødvendige spørsmål. Jeg fikk derfor forbedret intervjuguiden fortløpende basert på erfaringene jeg fikk fra hvert intervju (Hennink, Hutter & Bailey, 2020, s. 118). I tillegg gjorde denne prosessen at det dukket opp tanker om hvilke funn jeg hadde fått og hvilke analytiske temaer jeg kunne inkludere. Likevel valgte jeg å vente med å begynne på analysen til jeg hadde gjennomført alle intervjuene. Dette ble gjort fordi jeg ønsket et mer fullstendig datamateriale før jeg satte i gang med å analysere. Selv om det å vente med å analysere kan gjøre at man kan glemme spontane tanker man får underveis i transkriberingsprosessen, opplevde jeg ikke at dette var et problem. Jeg hadde datamaterialet i skriftlig form og kunne gå tilbake til det for å systematisere, «gjenoppdage» funn og se funnene på en ny måte og i et nytt lys siden sist.

Ettersom jeg brukte diktafon på mobilapp, kunne lydopptakene fra intervjuene sendes og lagres i Nettskjema, som er et nettbasert undersøkelsesverktøy utviklet av Universitetet i Oslo. Inne i Nettskjema blir opptakene automatisk transkribert ved hjelp av den UiO-interne tjenesten Autotekst som bruker Whisper fra OpenAi. Jeg tok derfor utgangspunkt i den automatiske transkriberingen fra Nettskjema, men gikk gjennom og hørte på alle intervjuene en til to ganger i ettertid for å rette opp i feil Autotekst kunne gi, da det er et AI-verktøy man ikke kan stole hundre prosent på. Jeg opplevde for eksempel at visse ord intervjudeltakeren sa hadde blitt feil eller at det manglet noen ord her og der. Dette gjaldt for eksempel for transkriberingen fra det ene intervjuet som ble gjennomført på kafe. Dette kan skyldes at det var en del støy i bakgrunnen, og at transkriberingen påvirkes av hvor god lyd det var på intervjuet. Dette viste hvor viktig det er å gå over og kvalitetssikre automatisk transkribering. I tillegg bidro denne prosessen til at jeg fikk nærhet til dataene. Av personvernhensyn ble alle

intervjuene transkribert på bokmål for at ikke dialekt skulle gjenkjennes. Jeg valgte videre å skrive transkripsjonene så tett opptil det som faktisk ble sagt som overhodet mulig, men jeg valgte å utelate navn, steder og andre identifiserende opplysninger, for å sikre krav til anonymisering (Hennink, Hutter & Bailey, 2020, s. 218). Dette var også viktig å gjøre for den påfølgende analyse- og kodefasen. Selv om jeg utelot gjenkjennbare opplysninger valgte jeg likevel å beholde koder for dette som jeg skrev i parenteser og kursiv underveis. Etter fullført transkribering satt jeg igjen med transkribert materiale på cirka 130 A4-sider, og hadde derfor mye empirisk materiale før den påfølgende analysen.

4.3.2 Tematisk analyse

Intervjumaterialet ble analysert gjennom tematisk analyse, som er en metode for å identifisere, analysere og rapportere mønstre (temaer) i data (Braun & Clarke, 2006, s. 79; Alvinus, Borglund & Larsson, 2023, s. 1). Målet er å utvikle temaer som samlet gir svar på forskningsspørsmålene man har (Johannessen, Rafoss & Rasmussen, 2018, s. 280). Jeg vurderte også narrativ analyse som metode, særlig fordi den legger vekt på språk, struktur og fortellermåte i enkeltfortellinger (Hennink, Hutter & Bailey, 2020, s. 209-210). Siden formålet i denne studien var å utforske innhold og identifisere sentrale tematiske mønstre på tvers av deltakernes fortellinger, snarere enn å analysere hvordan de enkelte historiene ble konstruert, ble tematisk analyse vurdert som den mest hensiktsmessige metoden. Tematisk analyse ble også valgt fordi den bidrar til å skape orden i dataene og gjør det mulig å identifisere nye sammenhenger i dem. I tillegg gir den god fleksibilitet gjennom sin teoretiske uavhengighet, og muliggjør kombinasjon med eksisterende teori (Braun & Clarke, 2006, s. 78; Johannessen, Rafoss & Rasmussen, 2018, s. 279-281). Dette anså jeg som nyttig, da jeg ønsket å se i hvilken grad de valgte teoriene mine, digital kriminologi, digital kapital, digital habitus, Christies «ideelle offer» og mestringsteori, kunne brukes for å forstå funnene (Hennink, Hutter & Bailey, 2020, s. 257-258).

Jeg fulgte de fire stegene Johannessen, Rafoss & Rasmussen (2018, s. 281) beskriver at tematisk analyse består av. Det første steget er å skaffe og få oversikt over data. Videre er de neste stegene å kode dataene, som innebærer å fremheve og sette ord på viktige poenger i data, kategorisere de kodede dataene inn i mer generelle temaer, og til slutt rapportere temaene og deres innhold. Samtidig vektla jeg en fleksibel og dynamisk tilnærming, hvor jeg beveget meg frem og tilbake mellom stegene i analysen etter hvert som nye mønstre og

innsikter oppsto, noe som er i tråd med forståelsen av tematisk analyse som en iterativ prosess (Braun & Clarke, 2006, s. 87; Johannessen, Rafoss & Rasmussen, 2018, s. 283).

Kodingen ble gjennomført digitalt i Word, der jeg brukte ulike farger for å markere og fremheve viktige poenger og aspekter som gikk igjen på tvers av intervjuer, for eksempel grønn for endringer i digitale vaner, og lysegrå for psykiske og emosjonelle reaksjoner. Selv om denne måten å kode på har blitt kritisert, mener Johannessen, Rafoss & Rasmussen (2018, s. 284) at tusjing og skriving nettopp er former for koding. Denne prosessen bidro til å skape oversikt over og tilrettelegge dataene for den påfølgende kategoriseringsfasen. Johannessen, Rafoss & Rasmussen (2018, s. 285-287) beskriver at koding ofte er en spørsmålsdrevet prosess, enten vi er det bevisst eller ikke. Jeg valgte derfor å begynne med en mer generell grovkoding, for eksempel «økonomiske konsekvenser», som deretter ble spisset til mer presise koder som «midlertidig økonomisk påvirkning» og «potensielt verre situasjon ved større tap» når nye spørsmål av interesse dukket opp. Underveis noterte jeg ned refleksjoner og ideer for å tilføre dybde til kodene.

Etter kodingen organiserte jeg dataene i overordnede kategorier som kunne bidra til å svare på forskningsspørsmålene. Johannessen, Rafoss & Rasmussen (2018, s. 294-295) beskriver at disse kategoriene også utgjør analysens temaer, og fungerer som «bokser». I boksene sorterer man data som har viktige ting til felles. Siden temaer ofte vil organiseres i overordnede og underordnede kategorier, er det også nyttig å tenke at hver boks består av ulike rom, og at hvert av disse rommene tilsvarer en underkategori eller et undertema. Derfor ble for eksempel koder for emosjonelle reaksjoner samlet under kategorien «psykiske konsekvenser». Jeg systematiserte dette videre i en tabell i Word med tre kolonner: en for informanten, en for koden og kategorien, og en for relevante tekstutdrag og sitater. Etter dette satt jeg igjen med og hadde identifisert tre hovedtemaer: svindeltyper opplevd av informantene, omstendigheter som påvirket sårbarhet, og konsekvenser av svindelen. Hvert av disse hovedtemaene inneholdt ulike undertemaer. For eksempel inneholdt hovedtemaet om sårbarhet undertemaer som «svindlernes teknikker», mens konsekvenser av svindelen inkluderte undertemaer som «økonomiske konsekvenser» og «psykiske konsekvenser». Temaene ble også revidert underveis, og jeg slo sammen overlappende temaer, samt sørget for at det var klare skiller mellom temaene jeg endte opp med.

Kodingen ble i hovedsak gjennomført induktivt, som vil si at den ble gjennomført ut ifra empiri, i motsetning til teori. Dette innebærer også at temaene oppdages underveis i analysen,

og er basert på hva som kommer frem i datamaterialet (Alvinus, Borglund & Larsson, 2023, s. 13). Samtidig er det viktig å understreke at jeg også tok utgangspunkt i intervjuguiden som hadde en noe tematisk inndeling og struktur, da jeg var kjent med relevant litteratur før analysen. Dette reflekterer en viss deduktiv tilnærming, men jeg forsøkte, som nevnt ovenfor, samtidig å benytte en induktiv, åpen og utforskende tilnærming i størst grad (Braun & Clarke, 2006, s. 87). For å gi analysen ytterligere dybde benyttet jeg strategien «sammenligning etter deduktivt bestemte undergrupper» (Hennink, Hutter & Bailey, 2020, s. 245), der jeg sammenlignet temaene på tvers av de yngre og eldre informantene.

4.4 Datakvalitet

En viktig del av forskningsprosessen i kvalitativ forskning er å vurdere kvaliteten på forskningen. I denne vurderingen er begreper som reliabilitet, intern og ekstern validitet, og overførbarhet sentrale. Reliabilitet handler om at man har skapt materialet på en pålitelig måte, og at leseren har grunn til å stole på at resultatene ikke skyldes feil eller skjevheter. Med validitet menes det at materialet man har, er relevant for den målsettingen forskningen har. Man skiller også mellom intern og ekstern validitet. Intern validitet omhandler hvorvidt forskeren har dekning i dataene sine for konklusjonene som blir gjort, mens ekstern validitet handler om hvorvidt kunnskapen som skapes i studien, er gyldig i andre sammenhenger, altså overførbar (Skilbrei, 2019, s. 87-89). I følgende del vil jeg reflektere over betydningen av disse begrepene for denne oppgaven.

4.4.1 Intern og ekstern validitet

Noe som er viktig for å styrke validiteten er å ha et kritisk blikk på analyseprosessen, presentere sitt perspektiv på temaet som er studert og vise hvordan man har motvirket selektive oppfatninger og partiske tolkninger (Kvale & Flick, 2007, s. 123). For å styrke studiens eksterne og interne validitet har jeg derfor valgt å inkludere sitater hentet ut fra mine intervjuer konsekvent gjennom hele analysen og i oppgaven for å vise til grunnlaget for tolkningene mine av dem (Tjora, 2021 s. 265; Hennink, Hutter & Bailey, 2020, s. 226). For å styrke validiteten er det også viktig å begrunne hvorfor og hvordan dataene har blitt tolket på den måten man gjør (Skilbrei, 2019, s. 41). Jeg har derfor valgt å begrunne tolkningene teoretisk og henvise til tidligere forskning som har blitt utført innenfor samme tema. Dette er med på å bygge opp under eller konfrontere de argumentene og poengene oppgaven presenterer (Tjora, 2021, s. 262). Dette bidrar også ytterligere til å styrke prosjektets gyldighet.

Når det gjelder ekstern validitet og studiens overførbarhet, er det viktig å være klar over at informantene i denne oppgaven utgjør et lite utvalg, og at funnene derfor ikke kan generaliseres til alle ofre for digital svindel. Likevel kan funnene ha overføringsverdi ved at de kan bidra med en forståelse av noen grunnleggende mekanismer i hvordan det kan oppleves å bli utsatt for svindel for en gruppe mennesker i Norge, og hvilke konsekvenser dette kan få, på et personlig plan, i relasjon til andre og i møte med hjelpetjenester som politi og bank. Gjennom å systematisere og teoretisere informantenes erfaringer, søker jeg ikke å etablere universelle sannheter, men heller å utvikle forståelse for underliggende mekanismer og mønstre. Dette innebærer det som ofte omtales som «analytisk generalisering» (Maxwell & Reybold, 2015, s. 688; Andenæs, 2000, s. 287). I motsetning til «statistisk generalisering», som er vanlig i kvantitativ forskning, handler analytisk generalisering om å bruke empiriske funn til å utdype eller utvikle teori (Yin, 2013). Slike funn kan fungere som veivisere, ikke som fasitsvar, men som mulige tolkninger som kan ha relevans i andre kontekster (Andenæs, 2000, s. 305). Ved å sette ord på erfaringer og reaksjoner som ofte ikke blir snakket om, kan studien bidra med kunnskap som også kan være nyttig for andre i lignende situasjoner. Som Polkinghorne (2007, s. 472) understreker, kan menneskers livsfortellinger gi viktig kunnskap om sider ved livet som ofte blir oversett. Derfor er hensikten ikke å trekke endelige konklusjoner, men å åpne opp for refleksjon og videre utforsking.

4.4.2 Reliabilitet

For å styrke studiens reliabilitet har jeg så konkret og utfyllende som mulig redegjort for hvordan datamaterialet i studien har blitt skapt. Dette inkluderer blant annet alle metodiske valg og fremgangsmåter jeg har benyttet både i innsamling av data, men også i etterarbeidet med datamaterialet (Thagaard, 2019, s. 188). I tillegg har jeg prøvd å sikre etterprøvbarhet i studien ved å legge ved referanser på alle studier og informasjon som er hentet ut fra disse til prosjektet både underveis i studien og til slutt i en utfyllende litteraturliste. Dette gjør det mulig for leseren å finne kildene som nevnes i oppgaven (Haugen & Skilbrei, 2021, s. 144).

Noe annet som er viktig for å styrke prosjektets reliabilitet er at man reflekterer over om man har noe til felles med informantene, eller om man har spesiell kunnskap eller erfaring som kan påvirke resultater (Tjora, 2010, s. 114; Skilbrei, 2019, s. 87). Dette henger sammen med en annen viktig del av forskningsprosessen, nemlig «refleksivitet», hvor man reflekterer over hvordan egen sosial bakgrunn, egne antagelser, posisjonering, atferd og andre aspekter kan påvirke forskningsprosessen, og hvordan studiedeltakerne reagerer på dette (Hennink, Hutter

& Bailey, 2020, s. 19). Denne oppgaven vil være preget av at jeg både har et utenfra-perspektiv og et innenfra-perspektiv. Jeg har ikke selv blitt utsatt for svindel på nett eller via telefon, og står derfor litt på utsiden av temaet. Dette gir meg en viss avstand, som gjør det lettere å gå inn i prosjektet med et åpent og nysgjerrig blikk. Samtidig har jeg noen egne erfaringer som gjør at jeg også delvis ser temaet innenfra. Jeg har blitt forsøkt svindlet på e-post, og opplevde en gang at banken sperret kortet mitt etter at noen hadde prøvd å bruke det på en taxitjeneste. Selv om jeg ikke ble direkte rammet og opplevde de negative konsekvensene dette kan medføre, gir disse hendelsene meg likevel en viss forståelse av hvordan svindel kan oppleves. Denne kombinasjonen kan påvirke hvordan jeg forstår temaet, hvilke spørsmål jeg stiller, og hvordan jeg tolker svarene. I tillegg kan min bakgrunn som kvinnelig kriminologistudent påvirke både datainnsamlingen og tolkningen, ettersom jeg kan legge merke til andre nyanser og aspekter enn forskere fra andre disipliner kanskje ville ha gjort.

Det er også viktig å reflektere over konteksten dataene har blitt utviklet innenfor, samt hvordan relasjoner til informantene kan ha hatt betydning for datautviklingen (Thagaard, 2019, s. 188). Selv om enkelte informanter ble rekruttert via familie og venner, hadde jeg ingen nær personlig tilknytning til dem. Jeg vurderer derfor at dette ikke har preget mine metodiske valg eller fortolkninger av oppgavens datamateriale i løpet av forskningsprosessen.

4.5 Forskningsetiske refleksjoner og vurderinger

Det er viktig med forskningsintegritet, som innebærer at man følger etiske prinsipper gjennom hele forskningsprosessen (Hennink, Hutter & Bailey, 2020, s. 72; Kvale & Flick, 2007, s. 29). Dette sørger også for at forskningen gjennomføres på en måte som ikke krenker sentrale samfunnsverdier, samtidig som man sikrer tillit til forskning (Skilbrei, 2019, s. 25). Jeg har derfor vært bevisst på forskningsetiske dilemmaer som kunne oppstå gjennom hele prosessen, og tatt gjennomtenkte valg underveis for å ivareta etiske hensyn og personvernet til informantene. Vurderingene jeg har tatt for å sikre at prosjektet opprettholder målet om en god forskningsetisk standard beskrives i det følgende. Jeg tar utgangspunkt i NESHs (De nasjonale forskningsetiske komiteene) forskningsetiske retningslinjer for samfunnsvitenskap og humaniora (NESH, 2021). Underveis vil det også reflekteres over hvordan «det digitale» påvirker og endrer våre forskningsmetoder og forskningsetikk. Teknologien kan for eksempel påvirke tilgang, deltakelse, interaksjoner, og hvilken informasjon man får fra informanter

(Kaufmann, 2024). Dette er relevant i min studie da jeg i tillegg til fysiske intervjuer også hadde fire digitale intervjuer og et over telefon.

4.5.1 Informert samtykke og frivillig deltakelse

Jeg startet prosessen med å søke om tilgang og godkjenning fra SIKT, og meldte prosjektet mitt til dem (se vedlegg 1). Dette var viktig fordi studien min omhandler et sensitivt tema, og fordi at jeg ved å ta opp intervjuene og samle inn informasjon fra studiedeltakerne vil behandle personopplysninger. I tillegg til å sikre etisk godkjenning fra SIKT var det viktig å sikre at informantene som deltar i prosjektet har gitt et fritt og informert samtykke (Hennink, Hutter & Bailey, 2020, s. 75-76). Det betyr at informantene skal ha kunnskap og forståelse om hva deltakelse i prosjektet innebærer for dem. For å sikre at de fikk tilstrekkelig informasjon om dette utarbeidet jeg et grundig informasjonsskriv og samtykkeskjema. Dette inneholdt blant annet informasjon om hvilken forskning de deltar i (i dette tilfellet en masteroppgave), forskningens formål, hva slags data som samles inn, hvordan dataene vil bli brukt og behandlet, og hvilke personer og institusjoner som er ansvarlige for prosjektet (Haugen & Skilbrei, 2021, s. 59). På denne måten kunne deltakerne selv vurdere om de ønsket å delta i studien. Det var også tydelig at de kunne trekke seg fra intervjuet og studien når som helst (Hennink, Hutter & Bailey, 2020, s. 75-78; Kvale & Flick, 2007, s. 33). Dette var spesielt viktig i min studie fordi kriminalitetsofre kan ses på som sårbare grupper (Richards & Cross, 2018, s. 107).

For å sikre dette gjennom hele prosessen valgte jeg å sende informasjonsskrivet til alle studiedeltakerne på e-post i forkant av intervjuene slik at de kunne lese gjennom det i ro og fred, og klargjøre eventuelle spørsmål de hadde til studien og deres personvern. Jeg gikk også gjennom hovedpunktene i informasjonsskrivet på selve intervjuet, slik at informantene fikk muligheten til å stille spørsmål, før de til slutt ga skriftlig samtykke. På de digitale intervjuene fikk jeg muntlig samtykke på opptak, istedenfor fysisk (Skilbrei, 2019, s. 153). Informasjonsskrivet og det skriftlige samtykket til å både la seg intervjue og til at intervjuet ble tatt opp, bidro til å skape en trygg ramme for datainnsamling (Haugen & Skilbrei, 2021, s. 55).

4.5.2 Anonymitet, personvern og konfidensialitet

Hensynet til anonymitet ble først og fremst ivaretatt i bearbeidingen av datamaterialet. Underveis i transkriberingen fjernet jeg all identifiserbar informasjon og anonymiserte alle

personopplysninger, slik at ingen enkeltdeltaker kunne identifiseres fra disse dokumentene (Hennink, Hutter & Bailey, 2020, s. 218). Jeg sørget derfor for å gjøre dataene anonyme før analyse og sikre etisk rapportering av de kvalitative dataene (Hennink, Hutter & Bailey, 2020, s. 83), da konsekvenser av å ikke gjøre det kan være at personvernet og sikkerheten til studiedeltakerne blir kompromittert (Hennink, Hutter & Bailey, 2020, s. 71-72). Eksempler på opplysninger jeg fjernet var navnet deres, stedsnavn, men også andre personer de nevnte når det fortalte om opplevelsen sin. I tillegg valgte jeg å henvise til informantene med kjønn og alder, en form for pseudonymer, fremfor fiktive navn (Hennink, Hutter & Bailey, 2020, s. 218). Dette anså jeg som hensiktsmessig da jeg hadde elleve informanter, og ønsket at det skulle være oversiktlig hvem som var hvem. Videre ble anonymiteten ivaretatt og sikret ved at jeg sørget for konfidensiell lagring av data (Hennink, Hutter & Bailey, 2020. 78-79). Opptakene fra intervjuene ble lagret på Universitetet i Oslo sin OneDrive (sky-tjeneste), og ble slettet fortløpende etter at jeg var ferdig med transkriberingen. Samtykkeskjemaene med underskrift fra informantene har jeg lagret i en mappe som jeg har oppbevart i mitt personlige skap på det juridiske fakultet ved Universitetet i Oslo. Jeg har ansett dette som et trygt oppbevaringssted, da skapet er låst med en personlig kode.

I forlengelse av dette var det også viktig å ivareta personvern og sikre digital sikkerhet under gjennomføringen i de digitale intervjuene. Mange av de tilgjengelige plattformene for digitale intervjuer tilbys av tredjepartsleverandører, som kan spore IP-adressen til deltakere, og overvåke eller avskjære dataoverføringer (Thunberg & Arnell, 2022, s. 764). For å redusere denne risikoen, valgte jeg å gjennomføre alle de digitale intervjuene på UiOs egne versjoner av Teams og Zoom, som har høyere personvern- og sikkerhetsnivåer sammenlignet med gratisversjoner av Zoom. UiO har også implementert sikkerhetsinnstillinger som ytterligere beskytter dataene (UiO, u.å.). Jeg sørget også for at intervjuene kun ble tatt opp som lyd med Diktafon, for å redusere risikoen for at tredjepartsaktører skulle få tilgang til sensitiv informasjon.

4.5.3 Vurdering av skade ved å delta i prosjektet

Forskning kan få konsekvenser for dem som deltar, for folk rundt dem og for gruppene de er rekruttert fra (Haugen & Skilbrei, 2021, s. 31). Det er derfor viktig at man som forsker reflekterer over den sosiale skaden som kan følge av å delta på et forskningsprosjekt (Hennink, Hutter & Bailey, 2020, s. 81).

I min studie er det først og fremst relevant å vurdere skadepotensialet rundt hvordan det ville være for informantene å fortelle om sine opplevelser, da det kan være svært vondt for den enkelte å gjenoppleve slike hendelser (Richards & Cross, 2018). Både i forkant og underveis i intervjuene vurderte jeg derfor ekstra nøye hvordan jeg skulle opptre, da jeg ikke har mye tidligere erfaring med å intervjue. Jeg bestemte meg for å vise empati og opptre på en slik måte at intervjudeltakeren følte seg ivaretatt (Hennink, Hutter & Bailey, 2020, s. 78). For å redusere skadepotensialet minnet jeg også informantene i forkant av intervjuet på at de ikke behøvde å svare på alle spørsmål, og at de måtte gi beskjed dersom det var noe de ikke forsto, eller om jeg skulle formulere et spørsmål på nytt. Det kan være en stor påkjenning å fortelle om vanskelige opplevelser og erfaringer, og man kan bli minnet på ting man kanskje aller helst vil glemme. Derfor ble det spesielt viktig fokusere på å skjerme deltakerne mest mulig, og ikke grave unødvendig mye dersom de ikke ville snakke om enkelte temaer. Jeg opplevde derimot at ingen av informantene mine ikke ønsket å svare på noen spørsmål. Alt dette bidrar også til å motvirke at ofrene føler på sekundærviktimisering, som det har blitt vist i tidligere forskning at ofre kan føle på i møtet med hjelpetjenester som for eksempel ikke tror på dem (se for eksempel Jansen & Leukfeldt, 2018; Cross mfl., 2016).

Prinsippet om at man ikke skal påføre forskningsdeltakere skade eller utsette dem for urimelige belastninger, gjelder også etter at datainnsamlingen i forskningsprosjektet er avsluttet. Det innebærer at man må vurdere hvordan forskningsdeltakerne påvirkes av valg man tar i analyse- og skrivefasene (Haugen & Skilbrei, 2021, s. 155). Jeg har derfor forsøkt å bruke et språk som viser respekt for dem man skriver om, særlig når det gjelder personer som har vært utsatt for kriminalitet. I stedet for å plassere informantene i en fast kategori som «offer», ønsket jeg å bruke et mer nyansert og personorientert språk som ivaretar deres individualitet. Dette handler ikke bare om presisjon, men også om å unngå utilsiktet stigmatisering eller å forsterke negative merkelapper. Personorientert språk, som for eksempel «person som har opplevd svindel» og «person som har blitt utsatt for svindel», bidrar til å skille individet fra hendelsen, og gir rom for flere sider av deres identitet. Å omtale noen på en måte de selv kjenner seg igjen i, er en måte å anerkjenne deres verdighet og autonomi på, og det er en viktig del av å redusere risiko for skade i forskningsprosessen (Willis & Letourneau, 2018, s. 480-482).

Selv om det er viktig å fokusere på å minimere skade for deltakerne, er det også viktig å reflektere over hvilke fordeler informantene kan få ved å delta i prosjektet (Hennink, Hutter

& Bailey, 2020, s. 82). Flere av mine informanter, selv om de opplevde hendelsen som kjip og trist, håpet likevel at historien deres kunne hjelpe andre, for eksempel ved å gi informasjon om hvordan svindel faktisk foregår i dagens moderne samfunn, slik at flere kan bli mer obs på dette. I likhet med mine intervjudeltakere ønsket også flere av informantene i Richards & Cross (2018) å delta i studien fordi de ønsket mer oppmerksomhet på svindel og ville advare andre om det. Noen ønsket også å delta fordi det ga dem en mulighet å sette ord på egne opplevelser. I slike tilfeller satte informantene pris på at forskeren var en objektiv og nøytral samtalepartner uten personlige bånd til dem (Richards & Cross, 2018, s. 104). Det samme kan gjelde i min studie, der deltakelse ikke bare gir en positiv opplevelse gjennom å bidra til å løfte frem ofrenes stemme, men også fungerer som en måte å bearbeide hendelsen på.

På samme måte som for informantene, er det også viktig at jeg som forsker heller ikke blir utsatt for skade og belastning (Hennink, Hutter & Bailey, 2020, s. 77). Man bør derfor ikke bare reflektere over potensiell skade på deltakerne i prosjektet, men også potensiell skade for forskeren selv. Siden det å bli utsatt for kriminalitet, i dette tilfellet svindel, kan ha mange negative konsekvenser for den som har opplevd det, var jeg nervøs på forhånd for hva de skulle fortelle og hvordan jeg skulle reagere. Dette skyldes at jeg til vanlig er en person som blir ganske lett rørt og preget av andre sine opplevelser. Selv om jeg var nervøs over dette og hadde intervjuer tett etter hverandre, opplevde jeg likevel at rollen som forsker gjorde noe med meg under disse intervjuene. Jeg ble mer profesjonell, og klarte å distansere meg emosjonelt fra fortellingene til informantene. Jeg tror dette også delvis skyldes at informantens konsekvenser varierte. Selv om noen hadde opplevd store belastninger, var det flere som ikke hadde opplevd de mest alvorlige eller langsiktige konsekvensene som ofte fremheves i forskning på ofrenes erfaringer. Samtidig hadde noen informanter opplevd at de var sterkt preget over tid, og det var dette som traff meg mest. Likevel opplevde jeg ikke at dette gjorde at jeg ble utsatt for skade og belastning i prosjektet.

5 Å være et offer i en digital verden: Opplevde svindeltyper og omstendigheter som påvirker sårbarhet

Dette er det første av to analysekapitler, og bygger på temaene som kom frem gjennom kodingen og etterarbeidet med intervjumaterialet. I det første analysekapittelet vil jeg beskrive hvilke svindeltyper informantene mine har opplevd. Dette bidrar til å kontekstualisere informantenes opplevelser, og gir en tydelig forståelse av den virkeligheten de befinner seg i. I tillegg bidrar det til å illustrere bredden og kompleksiteten av problemet,

og fungerer som et slags fundament for en mer detaljert og dyptgående analyse i det påfølgende analysekapitlet. Deretter vil jeg, basert på hva informantene oppga som del av sin fortelling, se på mulige omstendigheter og faktorer som de mente kunne ha påvirket deres sårbarhet og hvorfor de trodde på svindelen. Det andre analysekapitlet handler om hvilke konsekvenser hendelsen hadde for informantene, og hvordan de håndterte disse. Etter hvert analysekapittel følger en oppsummerende refleksjonsdel, hvor jeg viser hvordan funnene henger sammen og utfyller hverandre, samt belyser likheter og forskjeller mellom de yngre og eldre informantene, da dette er et av studiens overordnede interesseområder. Jeg har valgt å analysere erfaringene til eldre og yngre samlet underveis, fremfor hver for seg, ettersom mange av dem beskriver lignende erfaringer.

5.1 Svindeltyper opplevd av informantene

Informantene opplevde i hovedsak svindeltyper som phishing, identitetstyveri, familiesvindel og forbrukersvindel, hvor svindleren utga seg for å være en annen. Dette samsvarer også med hva Politiet (2023; 2024) registrerer som de mest utbredte formene for svindel i Norge. I tillegg opplevde en av informantene en svindeltype som ikke har en klar definisjon, og som kan betegnes som «ukjent». I dette underkapittelet vil jeg beskrive deres opplevelser mer i detalj.

5.1.1 Svindel med sosial manipulering og falske identiteter

Flere informanter opplevde svindel der svindleren benyttet sosial manipulering ved å utgi seg for å være en troverdig aktør eller en person de kjente. Dette er ikke uventet, da Politiet (2024) viser at sosial manipulering er en av de vanligste teknikkene i Norge.

Dette gjelder først og fremst kvinne 76 år og mann 55 år som opplevde phishing, hvor svindleren utga seg for å være en troverdig aktør som fikk dem til å oppgi sensitiv informasjon (Jakobsson & Myers, 2007, s. 16-17). Kvinne 76 år mottok en e-post fra det som fremsto som en helsetjeneste, som opplyste om at hun hadde fått et brev i sin digitale postkasse. Hun åpnet et vedlegg i e-posten og oppga bankID og personnummer. Først mistet hun ingen penger, men noen dager senere oppdaget hun at noen hadde opprettet en konto i hennes navn i Lunar Bank, og brukt den til transaksjoner på 13 000 kroner. Selv om hennes midler ikke ble direkte stjålet, oppdaget hun et trekk på 2500 kroner i skattemeldingen knyttet til denne kontoen, et beløp hun ikke fikk refundert. Hun opplevde derfor også identitetstyveri (Reep-van den Bergh & Junger, 2018, s. 2). Mann 55 år mottok en e-post fra det han trodde var rektoren på sin arbeidsplass, som ba ham om å kjøpe gavekort for 4000 kroner på Kiwi til

eksterne foredragsholdere. Det viste seg at dette ikke var rektor, og han fikk ikke refundert pengene.

Videre ble kvinne 85 år og kvinne 82 år i det eldre utvalget utsatt for vishing, som vil si phishing via telefon (Politiet, 2023, s. 25). Kvinne 85 år ble oppringt av noen som utga seg for å være fra Securitas, som advarte henne om at noen forsøkte å tømme kontoen hennes, men at de ville stoppe det. Hun oppga fødselsdatoen sin, og svindlerne tok senere opp et lån på 50 000 kroner i hennes navn. Hun opplevde derfor også påfølgende identitetstyveri (Reep-van den Bergh & Junger, 2018, s. 2). Svindlerne fikk ut 20 000 kroner, men hun avverget å miste mer penger. Kvinne 82 år ble oppringt av noen som utga seg for å være fra politiet, som sa at hun ble forsøkt svindlet og at noen hadde tatt opp lån. De fikk henne til å utføre flere handlinger på mobilen, og selv uten å oppgi sensitiv informasjon, klarte svindlerne å stjele 12 000 kroner. Dette beløpet fikk hun senere refundert etter å ha kontaktet banken.

I tillegg opplevde kvinne 73 år og kvinne 61 år i det eldre utvalget, og kvinne 41 år og gutt 18 år i det yngre utvalget familiesvindel, noen ganger kalt «hei mamma/pappa»-svindel, hvor svindleren utga seg for å være et familiemedlem (Finans Norge, 2024). Selv om begrunnelsene for betalingene varierte, var beløpene som krevdes ganske høye. Kvinne 73 år og kvinne 61 år overførte henholdsvis 23 000 og 28 000 kroner, hvorav bare kvinne 61 år fikk tilbake pengene. Kvinne 41 år betalte 50 000 kroner med ulike regninger på rundt 5000 kroner hver, som hun senere fikk tilbake. Gutt 18 år hadde en litt annerledes opplevelse. Han mottok en melding på Snapchat fra det han trodde var faren sin, med en forespørsel om å vippse 6000 kroner til en tredjepart i forbindelse med et kjøp. Begrunnelsen var at farens Vipps-konto hadde tekniske problemer. Kort tid etter å ha sendt pengene, forsto han at farens konto var blitt hacket av svindlere.

Videre opplevde mann 68 år og kvinne 29 år forbrukersvindel via Finn.no, der de betalte for varer de aldri mottok (Reep-van den Bergh & Jungher, 2018, s. 1-2), og hvor selgeren ikke var å oppdrive i etterkant av kjøpet (Politiet, 2023, s. 35). Mann 68 år skulle kjøpe en Apple Watch til 8000 kroner fra et firma via Finn.no. Han kontaktet firmaet, og ble møtt av en privatperson som fortalte at han jobbet i det firmaet, men skulle selge klokka privat. Han fikk ikke klokka, men fikk tilbake penger fra banken. Kvinne 29 år skulle kjøpe en iPhone X. Etter en tilsynelatende normal og ordentlig samtale med selgeren, samt en avtale om at hun kunne betale 2000 kroner av den fulle prisen på rundt 8-10 000 kroner på forhånd, mottok hun likevel aldri telefonen. Hun fikk imidlertid tilbake pengene fra banken.

5.1.2 Ukjent og uidentifisert svindeltype

Til slutt opplevde mann 37 år en litt annerledes type svindel enn de andre informantene, noe som illustrerer hvordan svindelmetoder stadig utvikles, at feltet er i konstant bevegelse, og at det er gråsoner mellom ulike svindeltyper. Han opplevde at 20 000 kroner ble overført fra hans konto til to privatpersoner via Vipps, mens han var på jobb. Han hadde verken gjort noe i forkant eller trykket på noe da transaksjonene fant sted, noe som gjør det utfordrende å fastslå nøyaktig hvilken type svindel det dreier seg om. Dette speiler også funn fra NorSIS (2023), hvor 2,7 prosent oppga at de ikke visste hvordan de hadde blitt svindlet, en usikkerhet som også kjennetegner opplevelsen til mann 37 år. Han spekulerer i om svindlerne bevisst retter seg mot ansatte med 9 til 4-jobber, som logger inn på systemer på morgenen. Ut ifra dette kan denne svindeltypen muligens defineres som «arbeidsdagssvindel». Det kan også minne om nettbanksvindel, der svindlere får tilgang til kontoer og overfører penger fra en persons nettbankkonto uten deres samtykke og viten (Reep-van den Bergh & Jungher, 2018, s. 2).

5.1.3 Mulige forklaringer på variasjoner i opplevde svindeltyper

Som disse funnene viser, ble de eldre informantene særlig rammet via telefon og e-post, ofte kombinert med identitetstyveri, mens yngre i større grad opplevde svindel via sosiale medier og når de gjorde kjøp på nett. Dette skiller seg fra funnene i rapporten til SODI om misbruk av elektronisk ID, hvor det ble vist at yngre aldersgrupper (19-30 år) var mer utsatt for å oppleve identitetskrenkelse enn eldre (Brataas, Stokke & Svensson, 2022, s. 23). Likevel har lignende funn blitt bekreftet i en undersøkelse gjennomført på vegne av NordVPN i 2024, som viser at unge mellom 18-34 år oftere blir utsatt via sosiale medier, mens eldre oftere blir rammet gjennom telefon eller SMS (Zieniūtė, 2024). Dette bekreftes også av Politiet (2023) som viser at svindel mot eldre ofte starter med phishing, smishing og telefonoppringninger.

Denne forskjellen kan skyldes ulikheter i deres digitale vaner. Som vist i beskrivelsen av det endelige utvalget var det tydelige forskjeller i tidsbruk og bruksområder blant de to aldersgruppene. De yngre var langt mer aktive på sosiale medier og brukte et bredere spekter av apper og plattformer både i jobb, skole og fritid. I motsetning til dette brukte de eldre informantene digitale enheter mer sporadisk, ofte til spesifikke formål som å lese nyheter eller sende meldinger. Slike forskjeller har også blitt vist i tidligere studier om det «digitale skillet» (se for eksempel Loges & Jung, 2001; Metallo & Agrifoglio, 2015). På bakgrunn av

dette er det interessant hvordan måtene de ble svindlet på i stor grad henger sammen med, og til en viss grad speiler, deres digitale vaner.

I forlengelse av dette kan disse funnene ses opp mot studiene som viser at digital atferd kan påvirke sårbarhet for svindel. Pratt mfl. (2010) og Van Wilsem (2013) finner for eksempel at tid brukt på internett og netthandel kan påvirke risikoen for å bli offer for svindel, fordi man blir mer synlig og derfor mer tilgjengelig for potensielle lovbrytere. Noe lignende kan også gjelde for kvinne 29 år og mann 68 år som opplevde forbrukersvindel. Ved å kjøpe varer på nettet via Finn.no, er det mulig at de gjorde seg mer synlige og til tilgjengelige mål for potensielle lovbrytere. Dette skiller seg fra de andre informantene som ikke hadde en atferd på internett som kunne gjøre dem mer tilgjengelige for å bli et mål for svindel. Dette bekreftes også av Kemp & Perez (2023) som viser at lavere internettbruk og lite shopping på nett kan fungere som beskyttelsesfaktor mot svindel. Dette kan indikere hvordan mine informanter som ble utsatt for phishing og familiesvindel ikke best forklares med digitale vaner, men heller andre faktorer. I det følgende vil jeg derfor rette oppmerksomheten mot hvordan andre faktorer enn digitale vaner, som livssituasjon og individuelle faktorer, kan ha større betydning for sårbarheten for digital svindel.

5.2 Omstendigheter og forhold som påvirker sårbarhet

Med bakgrunn i svindeltypene beskrevet ovenfor, vil jeg i dette underkapittelet se på hvilke faktorer informantene selv mente gjorde dem sårbarhet og bidro til at de trodde på svindelen. Dette omfatter blant annet svindlernes teknikker, personlige livshendelser, økonomisk situasjon, tillit, samt tidsmessige og kontekstuelle forhold.

5.2.1 Svindlernes manipulative teknikker

Flere av informantene nevnte at svindlernes teknikker på ulike måter gjorde at de trodde på svindelen. Dette gjelder først og fremst kvinne 85 år og kvinne 82 år, som ble ringt av svindlere som utga seg for å være fra henholdsvis Securitas og Politiet. De opplevde begge at det svindleren fortalte dem spilte en rolle for hvorfor de trodde på svindelen, som de forteller:

> Og da sier han: «det er noen som tar banken din, i dette øyeblikket». Du får jo et helt… ja, jeg tror hjerte og alt sammen. Videre sier han: «Men ta det med ro. Jeg er i den gruppen, og dette skal vi ordne». Så han begynner bare å spørre, og jeg vet at puls og alt, det bare [...] Og jeg sier jo [fødselsdato], ikke sant? […] Men noe skjer i min hjerne […] (Kvinne 85 år)

> […] Det øyeblikket der: «det er fra Securitas, det er noen som tar banken din». Den setningen der […] Og så sitter du alene. Du mister hodet. Det er lett å si at det hadde ikke jeg gjort […] Du må ha vært i situasjonen for å ... Selvfølgelig nå i dag, men jeg trodde det var DNB. (Kvinne 85 år)

> Og det var så rart, for det var akkurat som om jeg ble sånn paralysert, eller hypnotisert av et eller annet. […] Det er liksom ikke dagligdags […] Det var en slags tilstand som jeg… Helt uvirkelig, på en måte. Når du satt hele tiden og tenkte på at dette er svindel, men du ikke hadde sjanse til å få gjort noe med det, da må det jo være et eller annet som er ikke riktig […] Det er jo ikke normalt. Ja, det skjer et eller annet som man ikke har kontroll på, på et eller annet ekkelt vis […] (Kvinne 82 år)

Som sitatene viser, opplevde begge informantene en umiddelbar følelse av panikk da svindlerne tok kontakt. De var alene hjemme, og ble kastet ut i en situasjon som fremsto som akutt og truende. Dette kombinert med at svindleren utga seg for å være fra Securitas og Politiet, aktører som normalt forbindes med trygghet, kan ha gjort at informantene handlet impulsivt uten å tenke kritisk over hva som skjedde. Det å være alene kan også ha forsterket denne impulsiviteten, ettersom mangelen på noen å rådføre seg med kan svekke vurderingsevnen i pressede situasjoner (Dove, 2021, s. 77). Følelsen av at noe er akutt og haster kan forstås gjennom Mackenzies (2013) begrep om situasjonsbetinget sårbarhet. Tidligere forskning viser lignende mekanismer: Svindler skaper ofte bevisst en følelse av tidspress (Cross, 2022, s. 222), for å utløse panikk, en såkalt «visceral reaksjon», som reduserer evnen til kritisk tenkning (Cross, 2015; Dove, 2021, s. 55). I tillegg brukes autoritet som et virkemiddel for å øke etterlevelse (Dove, 2021, s. 69; Fischer mfl., 2013). Siden vi er oppdratt til å stole på og adlyde autoriteter, virker slike henvendelser mindre mistenkelige (Dove, 2021, s. 58). I forbindelse med dette viser Ross mfl. (2014) at høy tillit til andre kan øke sårbarheten, og i denne sammenhengen blir tillit til institusjoner et effektivt virkemiddel i svindelen. Det som skjer kan beskrives som følelsesdrevet godtroenhet (Greenspan, 2009), der kombinasjonen av frykt og tillit fører til at informantene handler på måter som ikke nødvendigvis gagner dem selv. Cross (2016) støtter dette og viser hvordan godtroenhet kan gjøre en mer mottakelig for svindel.

En slik mekanisme bekreftes også av mann 55 år, som opplevde at tidspresset påvirket hans beslutningsevne:

> Og så bruker de jo psykologiske virkemidler som gjør... De vil få deg til å handle veldig raskt. Før du tenker deg om […] (Mann 55 år)

At en yngre informant også reagerer på denne måten, indikerer at psykologiske virkemidler ikke bare påvirker eldre. Selv om yngre generasjoner gjerne har større digital kompetanse og er mer vant til å være kritiske til informasjon på nett (Prensky, 2001, s. 1), er stress- og panikkreaksjoner universelle. Dette antyder at det først og fremst er emosjonell manipulasjon, ikke alder, som avgjør hvor sårbar man er i slike situasjoner. En lignende svindel, tilpasset en yngre målgruppe, kunne dermed hatt tilsvarende effekt.

Men det handlet ikke bare om panikk og frykt. Flere informanter beskrev også hvordan svindlerne bygde opp tillit ved å skape et bilde av seg selv som hjelpsomme, som de forteller:

> […] han skulle hjelpe meg […] Jeg syntes nesten synd på han, vet du, stakkars mann. Han fikk jo ikke... jeg ga han jo ikke opplysningene antagelig […] (Kvinne 82 år)

> […] Han var litt frempå, men han var så hjelpsom og kunne hjelpe meg med alt […] Han er så høflig, man skal liksom ikke avbryte […]. (Kvinne 82 år)

> […] men hvert fall så prater han veldig sånn hyggelig da […] måten han pratet på virket helt ordentlig og fin på en måte, så jeg tenkte ikke noe mer over det […] for det var jo en ekte person, som satt bak tastatur eller mobil, og skrev til meg, som spilte på liksom høflighetsfraser patos i måten han formidlet meldinger […] (Kvinne 29 år)

> […] Og det var hyggelig tone. […] Det kunne vært ekte, da. Jeg var ikke mistenksom i det helt tatt […] Det er som om det er rektor som jeg snakker med […] (Mann 55 år)

Som sitatene viser, kan det virke som at svindlerne bevisst bruker språklige virkemidler, og en vennlig, imøtekommende tone for å etablere tillit og bygge relasjon. Ved å fremstå hjelpsomme, spiller de på sosiale normer knyttet til høflighet, lovlydighet og ønsket om å være samarbeidsvillig. Tonen kan minne om den man møter i kundeservice eller hverdagslige interaksjoner, der hjelpsomhet og løsningsorientering står sentralt. Dette kan skape en forventning om hvordan man bør opptre, og kan gjøre at man stoler på det som blir sagt, uten å vurdere innholdet kritisk (Dove, 2021, s. 56-58). Et viktig aspekt som trer fram i informantenes beskrivelser, er hvordan høflighet fungerer som en form for subtil kontroll. Når noen henvender seg på en vennlig måte, kan det oppstå en normbasert forpliktelse om å

svare på samme måte. Dette kan gjøre det vanskelig å bryte samtalen, selv om noe føles galt. Kvinne 82 år uttrykte til og med sympati med svindleren, noe som antyder at det kan oppstå en emosjonell tilknytning, til tross for den manipulerende hensikten. Svindlernes vennlighet fungerer dermed som en slags psykologisk barriere som hemmer skepsis og motstand.

I flere tilfeller benyttet også svindlerne profesjonalitet for å skape tillit og virke troverdige. For eksempel oppfattet kvinne 29 år og mann 68 år, som begge handlet på Finn.no, annonsene som ekte. I forbindelse med dette forteller kvinne 29 år:

> Så jeg tittet litt rundt på Finn og så fant jeg en som hadde lagt ut masse bilder, sånn at den så jo helt […] det var ikke tatt fra nettet sånn som mange gjør på Finnannonsene, så det var liksom en ekte mobil på bildene […] (Kvinne 29 år)

> […] Jeg tror han også skrev et eller annet sånn «kan du huske å legge inn navnet ditt, for jeg har overført gjennom bankoverføring og pleier så ofte å selge ting på Finn, så bare at det går opp i regnskapet mitt», ikke sant han spilte på litt sånn historieformidling sånn at det virket som alt var på plass der på en måte […] (Kvinne 29 år)

I likhet med dette virket også svindelen i mann 68 år sitt tilfelle veldig profesjonell. Han sjekket nettsiden til firmaet og ringte nummeret som var oppgitt, og kom i kontakt med en person som sa at han jobbet i firmaet, men skulle selge klokken privat. Selgeren ba om forhåndsbetaling slik at klokken skulle bli reservert han, og tilbød seg også å levere klokka dagen etter. Fordi han hadde sjekket firmaet og opplevde at alt var i orden, valgte han å sende pengene. Selgeren kom ikke som avtalt, men ba om noen dager til. Etter hvert ble mann 68 år mistenksom, og fikk derfor tilsendt ID-kortet til selgeren med personnummer. Det viste seg senere at ID-kortet var stjålet. Selv om han prøvde så godt han kunne å se om det var svindel, viste det seg at svindleren hadde kopiert firmaets nettside, og lagt inn sine egne telefonnumre. Han forteller:

> Ja, det virket troverdig […] Men det er jo nesten umulig å ikke la seg lure. Og han hadde jo også da lagt seg på et prisnivå som gjorde at det var ikke sånn latterlig billig. Det er jo ofte et tegn på at her er det noen tvilsomme greier. Men det var en sånn nogenlunde anstendig pris. Jeg tenkte jo før jeg skulle betale noe som helst at jeg skulle sjekke veldig godt da. Prøvde jeg å gjøre på alle mulige måter, men med en falsk side og med han som sendte falsk ID og alt som var, så ble jeg lurt (Mann 68 år)

Dette funnet kan ses i likhet med studien til Button mfl. (2014b), hvor det blir vist at svindel ofte lykkes når det presenteres med høy grad av legitimitet og profesjonalitet, for eksempel gjennom en nettside med profesjonelt utseende. I likhet med dette ble det vist i undersøkelsen gjennomført på vegne av NordVPN i 2024 at 56 prosent av nordmenn oppga at teknologi og psykologiske ferdigheter hos svindlerne, for eksempel i form av falske nettsider og etterligning av kjente merker og selskaper, er den primære årsaken til at man faller for svindelforsøkene (Zieniūtė, 2024).

I noen tilfeller virket også svindelen profesjonell fordi svindlerne benyttet ekte navn og ekte mailadresser. Dette gjelder først og fremst kvinne 29 år, som ikke tenkte over at det var svindel fordi hun fant personen hun hadde snakket med på Facebook, med et tilsynelatende ekte navn og en ekte profil. Videre gjelder dette kvinne 41 år, som opplevde svindelen som troverdig fordi svindleren brukte Klarna sitt system. Hun påpeker at hun ikke hadde betalt regningene hvis det ikke hadde vært Klarna. Mann 55 år mente også at troverdigheten var høy fordi svindlerne brukte rektoren sin e-post og sendte e-posten i systemet han er vant til, som han forteller:

> […] [e-posten] kom opp i mailsystemet vårt akkurat som den andre. Så det var bare god svindel. Men hadde jeg sjekket e-posten der. Jeg har to forskjellige e-poster. Jeg har en jobb-e-mail. Og så har jeg en privat e-mail. På den private kommer det alle mulige rare. Det er der de svindelhenvendelsene har kommet. Jeg har aldri opplevd at det kommer på den jobb-mailen. Derfor hadde jeg litt garden nede, antageligvis […] (Mann 55 år).

Blant det eldre utvalget opplevde også kvinne 76 år og kvinne 73 år svindelen som profesjonelt gjennomført. For kvinne 76 år var dette fordi brevet hun fikk på e-post hadde hennes navn i mailtittelen og var skrevet med god norsk. Hun mente at dette skiller seg fra tradisjonelle svindelmailer, som hun forteller:

> Og så var det et brev til meg. […] Og det sto til, fordi at alle disse luregreiene som kommer. Der står det «du venter pakke», «du har vunnet», «du har ditt og datt», men det står aldri navnet ditt. Det hender noen ganger at det også står til e-postadressen, som navn, men jeg har ikke vært borti noe der det står til navnet også (Kvinne 76 år)

Til slutt opplevde kvinne 73 år svindelen som både profesjonell og troverdig. Hun hadde på forhånd fått vite at sønnen hadde problemer med mobiltelefonen, og da hun mottok en

betalingsforespørsel med detaljer som kontonummer, navn på bank, KID-nummer og en konkret mottaker, fremsto det som en legitim henvendelse. Hun antok at sønnen hadde inngått en avtale om kjøp av en ny mobiltelefon, og ønsket å hjelpe han med betalingen.

I forlengelse av dette hadde det ikke bare betydning at man ble kontaktet av svindlere som utga seg for å være fra Politiet eller Securitas. Flere trodde også på svindelen fordi svindleren utga seg for å være noen i deres nærhet som trengte hjelp. For mann 55 år var dette rektor, for kvinne 73 år, kvinne 61 år, kvinne 41 år, og gutt 18 år var dette et familiemedlem.

Mann 55 år hadde for eksempel dårlig samvittighet fordi han var borte fra jobb, og ønsket derfor å hjelpe rektoren, som han forteller:

> […] Jeg pleier aldri å være borte, så jeg hadde litt sånn dårlig samvittighet for at jeg var hjemme på en planleggingsdag. Det er litt sånn bakgrunnen for hvorfor jeg klarte å bli lurt […]. Så får jeg en melding fra rektor om jeg kan ordne noe for henne. Og da er jeg selvfølgelig veldig på tilbudssiden […] (Mann 55 år)

Flere av informantene beskrev lignende opplevelser. Kvinne 73 år, kvinne 61 år og kvinne 41 år trodde de hadde en samtale med sønnene sine og ønsket å hjelpe dem med å betale regninger. For kvinne 73 år virket i tillegg svindelen troverdig fordi meldingene føltes helt normale, og som noe sønnen kunne ha skrevet. Kvinne 41 år ble også overbevist om at det var sønnen, da svindleren bekreftet et personlig kallenavn hun brukte i meldingen. De mener likevel at de burde ha lagt merke til varselsignalene underveis, men syntes at det var vanskelig fordi svindelen virket realistisk. Kvinne 73 år trakk også frem at svindlerne spilte på samvittigheten hennes, som hun forteller:

> Men så sier [navn på sønn] […] «At, men det er akkurat det de gjør. De spiller på samvittigheten din. Stakkar meg. Jeg sitter med en regning» og jeg stusser, jeg vet jo at [navn på sønn] er veldig opptatt av få betalt sine regninger. Og det kan skje […] Vi har jo av og til hjulpet han, litt sånn som en gjør med sine barn […] (Kvinne 73 år)

På samme måte som disse informantene trodde at det var sønnen sin, trodde gutt 18 år at han snakket med faren sin:

> Og det hadde vært lurt av meg kanskje å ringe ham først, men det gjorde jeg ikke. For jeg bare så meldingen og tenkte sånn: «ja, det er faren min». Så jeg bare sendte

> pengene over, spurte også om «blir det ikke noe vippsgebyr?». Og da skrev jo faren min, eller han jeg trodde var faren min: «ja, men det dekker jeg». Så da tenkte jeg sånn: «ok, det her er jo ikke en bot», fordi han interagerer med meg aktivt. Så jeg sendte pengene, og så to minutter senere ble jeg ringt av faren min, og han var sånn: «du, alle vennene mine sender meg melding og sier at jeg har spurt dem om 6000 kroner. Du har ikke fått den meldingen du også?» Så var jeg sånn: «jo da». Så spurte han meg om jeg har sendt de pengene, og da tenkte jeg: «oh shit, ok. Det var ikke faren min». (Gutt 18 år)

På spørsmål om han trodde på svindelen fordi svindleren utga seg for å være faren hans, svarte han:

> Ja. Definitivt. Jeg sa og i etterkant at hvis det var hvem som helst andre utenom faren min, så hadde jeg uten tvil ringt personen og sagt sånn: «hei, hva er det du spør om? Hva skjer?» Fordi han skrev jo som faren min, den personen. Så hadde det vært moren min som hadde sendt meldingen, så hadde jeg skjønt at det ikke var henne, fordi hun skriver ikke på den måten. Men det var akkurat det at det var faren min som sendte meldingen, at jeg bare ikke stilte noen spørsmål. Jeg tenkte sånn: «ja, det er jo min egen far, da bare sender du pengene» (Gutt 18 år)

Disse opplevelsene viser hvordan svindlere øker troverdigheten ved å utgi seg for å være en forelder, kollega eller et barn. De speiler språk og kommunikasjon som normalt skjer i nære relasjoner, og erstatter tilliten til autoriteter med tillit forankret i personlige bånd. Når hendelsen kommer fra noen man stoler på, aktiveres følelser som empati og ansvar, og den kritiske sansen svekkes fordi man gjerne vil hjelpe sitt familiemedlem. Svindlerne utnytter dermed sosiale normer og egenskaper som hjelpsomhet og medfølelse (Dove, 2021, s. 58).

Samlet tydeliggjør disse funnene hvordan svindlere opererer på flere nivåer samtidig for å fremstå som troverdige. De spiller på følelser som frykt, tillit og tidspress, samtidig som de benytter teknisk profesjonalitet og utgir seg for å være personer informantene har en relasjon til. Som mann 37 år uttrykte det: «De er så skarpe de som holder på med det». De kombinerer emosjonell manipulasjon med digital kompetanse, og benytter klassiske manipulasjonsteknikker for å utnytte menneskers behov for å stole på andre. Dette støtter funnene til Carter & Weber (2010) og Judges mfl. (2017), som viser at tillit alene ikke er tilstrekkelig for å forklare hvorfor svindelen lykkes.

Svindlernes metoder kan også forstås i lys av begrepet digital kapital (Park, 2017; Ragnedda, 2018). Som Bakken mfl. (2022) viser må både selgere og kjøpere i ulovlige narkotikamarkeder på nett ha gode digitale ferdigheter, for eksempel mestre digitale verktøy, og ha riktig atferd og måte å kommunisere på, for å navigere markedene. På lignende vis fremstår svindlerne her som personer med høy digital kapital, som de bruker målrettet og strategisk for å manipulere ofrene. De vet hvordan de skal fremstå troverdige, tilpasse språk og tone til konteksten, og utnytte digitale plattformer til sin fordel. Dette betyr ikke nødvendigvis at ofrene mangler digital kapital, men at svindlerne er så dyktige til å bruke teknologien i kombinasjon med emosjonelt press at det ikke faller naturlig å være kritisk i øyeblikket. Selv personer med høy digital kompetanse kan lurt i situasjoner preget av stress, tillit og emosjonell involvering. Svindlernes fremgangsmåter gjør at ofrenes handlinger, som å oppgi informasjon eller overføre penger, ofte fremstår mer som spontane reaksjoner snarere enn som bevisste og rasjonelle handlinger.

5.2.2 Tid, setting og kontekst

I tillegg til å oppleve svindelen som troverdig, var det også flere som fortalte at tidspunktet for svindelen, samt hendelser som hadde skjedd i livet deres, påvirket hvordan de reagerte og hvorfor de trodde på svindelen. Dette gjaldt spesielt for de eldre informantene, mens de yngre informantene oftere sa at det var en vanlig dag. Selv om noen informanter mente at det var mulig at svindlerne utnyttet slike tidspunkter som en slags teknikk, har jeg valgt å plassere tid, setting og kontekst i en egen del, da det at man blir utsatt for svindel også kan skyldes tilfeldigheter. Det er for eksempel ikke sikkert at svindleren vet hva som har skjedd i ens liv. Det betyr at tidspunkt og kontekst kan være viktig for informantenes personlige oppfatning av hendelsen, selv om svindleren ikke nødvendigvis vet om dette.

Først og fremst mente kvinne 85 år og kvinne 61 år at både tidspunktet og livshendelser spilte en betydelig rolle. Kvinne 85 år ble ringt opp to ganger, begge ganger på samme tidspunkt, like før Dagsrevyen var ferdig. Første gang skjønte hun at det var svindel, da hun ikke var kunde i banken svindlerne utga seg for å ringe fra. Andre gang, en uke senere, ble hun lurt, som hun forteller:

> Tenkte ikke så mye over det, skjønte jo senere at det var et lite forvarsel. De legger ut en liten snubletråd, eller hva jeg skal si. Det er det dem gjør […] (Kvinne 85 år)

> […] Det er en logikk i dette her. Og da ved halv åtte tiden, så rett før dagsrevyen er ferdig. For da sitter jo alle gamle og ser på Dagsrevyen, ikke sant?. Nei, altså det er finurlig. Så det med klokkeslettet, det er ikke tilfeldig. Det er når du sitter opptatt av noe […]. Ja, du blir tatt på sengen (Kvinne 85 år)

Men det var ikke bare tidspunktet som gjorde henne sårbar. Dagen før hadde hun fått en uventet beskjed fra legen om at hun likevel kunne få en øyeoperasjon hun tidligere hadde fått beskjed om at ikke var mulig. Dette påvirket henne sterkt, som hun beskriver:

> […] [jeg var] i en sånn euforisk tilstand. Og det var jeg lenge […] Så det henger jo litt sammen med at det var jo en sånn situasjon at jeg var ikke helt meg selv. Jeg var så lykkelig at det ble håp for meg […] Også kvelden etterpå. Så akkurat den er nok litt sånn...ja, man er menneske (Kvinne 85 år)

Kvinne 61 år hadde en lignende opplevelse. Samtidig som hun mottok meldingen fra noen som utga seg for å være sønnen hennes, var hun i søsterens leilighet for å rydde, da hun hadde gått bort i februar. Hun forteller at dette gjorde at tankene hennes var på en helt annen plass den dagen skjedde, og at hun i øyeblikket ikke tok seg god tid:

> Så de [svindlerne] er ganske gode, men klart antennene var jo ikke ute, og forsvarsverket var heller ikke på plass akkurat den dagen, så sånn gikk det jo (Kvinne 61 år)

> […] jeg vet jo om det, at når du blir kontaktet av noen du ikke kjenner, og de har det litt travelt, så man må bare ta seg god tid. Så jeg vil si at min oppmerksomhet var 95 %, og så ble jeg tatt mens jeg var i mine 5 %. (Kvinne 61 år)

Men sårbarheten handlet ikke alltid bare om at de befant seg i en situasjon hvor oppmerksomheten var svekket. For mann 55 år var det selve settingen som gjorde svindelen troverdig og logisk:

> Jeg var, ettersom det bare passet så jævlig bra med settingen, fordi jeg visste også at vi hadde eksterne foredragsholdere. Jeg visste ikke at de skulle få gavekort. Det er litt uvanlig, men det er heller ikke veldig uvanlig […] (Mann 55 år)

Han var hjemme under en planleggingsdag da han mottok henvendelsen, og påpekte i etterkant at han aldri ville ha blitt lurt dersom han var fysisk til stede på skolen:

> Jeg skjønner fortsatt ikke at jeg ble lurt, for jeg er egentlig veldig opptatt av sånne ting. Men settingen traff meg helt perfekt […] den planleggingsdagen, det at jeg var hjemme.. Det var så mange ... Hadde jeg ... Jeg skulle vært på skolen. Da hadde jeg aldri blitt lurt av det (Mann 55 år)

Også mann 37 år reflekterte over tidspunktet. Han hadde akkurat logget seg på jobbsystemer da svindelen skjedde:

> […] Og når jeg skjønte at det skjedde 5 over 9 på morgenen, så skjønte jeg kanskje at jeg hadde logget meg på et eller annet og tilrettelagt for dem [svindlerne] (Mann 37 år)

Selv uten en spesiell livshendelse i forkant, var tidspunktet, rett etter jobbstart, med på å forme hvordan han oppfattet situasjonen. Han tror for eksempel at det er mulig at svindlerne bruker et system hvor de kan få tilgang til folk som jobber og er ansatt i bedrifter.

Til slutt er det et interessant tilfelle hos kvinne 73 år. Dagen før svindelen fortalte sønnen hennes at han hadde problemer med telefonen sin og trolig måtte skaffe ny. Da hun mottok meldingen fra svindleren som utga seg for å være sønnen hennes, som fortalte at han trengte hjelp til å betale en regning, fremsto det derfor logisk:

> Men det var så rart fordi at […] hadde ikke jeg visst at han hadde hatt trøbbel med sin telefon på søndag. Så hadde jo ikke jeg reagert sånn på den meldingen. Da hadde jeg jo ringt han med en gang ikke sant […] (Kvinne 73 år)

På tvers av informantene ser man hvordan sårbarheten og mottakeligheten ble forsterket av spesifikke livssituasjoner, emosjonelle tilstander eller hverdagslige settinger. Slike situasjoner kan skape midlertidige rom for sårbarhet, der oppmerksomheten er svekket og tankene er «et annet sted». Noen ganger traff svindlerne tilfeldig på et slikt svakt punkt, andre ganger kan det se ut som at de utnyttet rutiner, som at mange eldre ser på Dagsrevyen klokken halv åtte. Dette bidro til at budskapet virket logisk og troverdig i øyeblikket. Når henvendelsen passer inn i det kjente og hverdagslige, senkes den kritiske vurderingsevnen, selv hos ellers årvåkne personer. På samme måte bekrefter tidligere forskning at negative livshendelser som dødsfall

i familien, kan svekke dømmekraften og øke sårbarheten for svindel (Voce & Morgan, 2023; Emami mfl., 2019, s. 8). Funnene illustrerer dermed Mackenzies (2013) poeng om at sårbarhet ofte er situasjonsbetinget og kontekstspesifikk. I disse tilfellene ble både tidspunkt og personlige hendelser avgjørende for hvordan informantene tolket og reagerte på svindelsituasjonen.

5.2.3 Alder, tilfeldigheter og digitale ferdigheter

I tillegg til svindlernes teknikker, og tid og kontekst, var det også flere av informantene som reflekterte over hvordan trekk ved deres alder kan ha spilt en rolle i hvorfor de ble målrettet eller trodde på svindelen.

Kvinne 85 år mente for eksempel at alderen gjorde henne til et attraktivt mål:

> Det er klart dem så at, altså gamle folk sparer, ikke sant? Det er et fint klientell å gå på. Rett og slett. (Kvinne 85 år)

For henne handlet det om at svindlerne sannsynligvis antok at eldre personer har oppsparte midler og pensjon, noe som også bekreftes i tidligere forskning (Cross, 2015). Kerley & Coopes (2002, s. 31) fant dessuten at eldre personer uten slike ressurser hadde mindre sannsynlighet for å bli svindlet. Noe som er interessant ved dette er at mann 37 år også tenkte at alder kunne ha noe å si i hans tilfelle fordi han ble utsatt mens hans var på jobb. Som nevnt tidligere kan det hende at svindlerne i dette tilfellet utnyttet at han var i yrkesalder og dermed visste at han hadde penger.

På en lignende måte lurte kvinne 76 år på om hun hadde blitt et mål på grunn av navnet sitt. Hun tenkte at det var mulig at brevet hun fikk skulle til godt voksne og pensjonister fordi det handlet om pensjon. Hun koblet opplevelsen til det som ofte omtales som «Olga-svindel», hvor svindlere bevisst retter som mot eldre ved å bruke navn som tradisjonelt forbindes med bestemte aldersgrupper (Politiet, 2023; 2024). Likevel var hun usikker på i hvor stor grad navnet spilte inn, da hun gjennom et søk på Statistisk Sentralbyrå fant ut at det var flere yngre enn eldre som hadde navnet hennes.

Men alder kom også opp på mer subtile måter. Flere reflekterte i ettertid over hvorfor de ble lurt, og knyttet dette til egen alder, naivitet eller hvordan de oppfatter seg selv i møte med slike situasjoner. Mann 68 år uttrykte for eksempel at det skjedde med han fremfor andre fordi han ifølge seg selv er «gammel og lettlurt». I dette tilfellet knyttes alder til et bilde av at

man er en person som er lettere å lure. Også kvinne 73 år tenkte i lignende baner, særlig i relasjonen til barna sine. Hun trakk frem at svindlerne kan se på eldre som lette å lure, blant annet fordi de ofte er snille med barna sine og gjør som de får beskjed om. Hun sier følgende om sønnens reaksjon i forbindelse med dette:

> […] For han reagerte sånn: «at her var det noen som var lette å lure». Vi var jo det. Ja, jeg hadde ikke et eneste flagg ute før det hadde gått noen timer (Kvinne 73 år)

Yngre informanter viste også lignende refleksjoner, men med andre ordvalg. På spørsmål om hvorfor mann 37 år trodde det skjedde, svarte han følgende:

> Ja, fordi jeg gikk rundt og var naiv. Tenkte dette skjer ikke meg. Jeg var ikke så forsiktig (Mann 37 år)

Slike utsagn bør ikke forstås som faste forestillinger om hvem informantene er, men snarere som en måte å forklare hvorfor de ikke reagerte sterkere, eller var mer skeptiske i øyeblikket. I lys av Scott &Lymans (1968, s. 46-47) begrep «accounts» kan informantenes utsagn og beskrivelser av seg selv som «lettlurt» eller «naiv», tolkes som en form for etterrasjonalisering, hvor de forsøker å redusere skam og bevare egen verdighet, og samtidig vise at svindelen kunne ha rammet hvem som helst under tilsvarende omstendigheter. Å bruke accounts kan derfor ses på som en slags emosjonsfokusert mestringsstrategi (Lazarus & Folkman, 1984), der ofrene prøver å håndtere og kontrollere følelsene sine (Green mfl., 2010).

Videre var det enkelte informanter som reflekterte over stereotypiske forventninger om hvem som blir lurt. Både kvinne 29 år og gutt 18 år ble overrasket over å selv ha gått på svindelen, da de i utgangspunktet forbandt svindel med eldre, som de forteller:

> Altså […] jeg føler jo at det er mer eldre som blir lurt, når man ser på for eksempel Åsted Norge på TV, eller leser om noen artikler på nettet, at de eldre blir litt, det går litt for raskt for dem og at de blir brukt med liksom godtroenhet og sånn. Så jeg husker jeg var jo litt sjokka over at jeg falt for det da. Men samtidig han solgte jo en iPhone X og det er jo mest yngre som ville ha det da. Så sånn sett hadde det nok noe å si med alderen min ja, at jeg var liksom en ja, student, i den alderen, ønsket ny mobil, trengte å spare litt penger, så ble jeg nok litt mer målrettet da (Kvinne 29 år)

> […] Nå er jeg i den alderen hvor jeg egentlig burde ha visst mest om å ikke gjøre sånt. […] det er da man hele tiden hører om disse svindlene, hvordan man skal unngå det, så tenker man jo alltid at det aldri kommer til å skje deg, og at hvis noen faller for det, så er det som regel kanskje de eldre folkene som ikke er så kjent med moderne teknologi da. […] som faller for det mest. Ikke for min case da, men... (Gutt 18 år)

Tilfellene til kvinne 29 år og gutt 18 år viser hvordan alder var noe de i utgangspunktet ikke trodde spilte inn, men som de i ettertid ser at kan ha hatt betydning for svindelen. Dette kan forstås i lys av tidligere forskning som viser at kognitive skjevheter, som tanker om at svindel bare skjer med noen mennesker, for eksempel folk som er mindre smarte eller fortjener det (Cross, 2015), kan gjøre at man overser faresignaler, blir mindre forsiktig, og overvurderer sin egen evne til å oppdage svindel (Dove, 2021, s. 78).

Gjennom disse fortellingene blir det tydelig at alder spiller en rolle både som en ytre kategori svindlerne forholder seg til, og som en ramme informantene selv bruker for å forstå hendelsen. Alderen kan påvirke hvem svindlerne retter seg mot, for eksempel ved å bruke navn eller økonomisk situasjon. Dette samsvarer med tidligere forskning som viser at det ikke nødvendigvis er alderen i seg selv, men enkelte faktorer ved aldringsprosessen, som redusert kognitiv kapasitet, som kan øke risikoen og gjøre eldre til mer attraktive mål (Dove, 2021, s. 76-77). Samtidig viser informantenes refleksjoner at alder også fungerer som en forklaring i etterkant. Både eldre og yngre forsøkte å forstå hvorfor nettopp de ble lurt, og pekte på trekk ved alderen deres som mulig forklaring. Slik blir alder en del av informantenes «accounts» (Scott & Lyman, 1968), en måte å plassere svindelen innenfor en forståelig ramme: at man «burde visst bedre» som ung og digital kompetent, eller ble oppfattet som et lettere mål fordi man var eldre. På denne fremstår alder ikke bare som et objektivt trekk, men som en aktiv del av informantenes meningsskaping og etterrasjonalisering. Funnene støtter dermed både forskning som viser at alder og demografiske forhold kan ha betydning for risiko (Whitty, 2019; James mfl., 2014; van Wilsem, 2013), og studier som understreker at slike sammenhenger ikke er entydige (Leukfeldt & Yar, 2016; Pratt mfl., 2010).

Selv om alder i noen tilfeller kan ha påvirket sårbarhet, var det flere som var skeptiske til betydningen av alder, og mente at det i stedet handlet om tilfeldigheter. Kvinne 73 år hadde for eksempel fått høre fra politiet at navnet hennes kunne ha gjort henne til et mål, men avviste raskt denne forklaringen da hun syntes det hørtes fiktivt ut. I tillegg hadde hun vært i kontakt med et annet svindeloffer som hadde opplevd det samme som henne, men ikke hadde

et «eldre» navn. Hun delte også refleksjoner fra en samtale med et annet svindeloffer, hvor de begge avviste ideen om at de var «dumme og lettlurte», slik de opplevde at svindlere kanskje antar, og beskrev seg heller som oppegående mennesker. Denne refleksjonen stod i kontrast til tidligere utsagn, der hun hadde uttrykt enighet i at eldre kanskje er lettere å lure, slik både svindleren og sønnen hennes hadde antydet. Over tid endret hun derfor forklaring, og kom frem til at det hele nok handlet om tilfeldigheter:

> […] fordi at det er klart at disse her folkene eller hva det nå er som driver og ringer, [.,.] de ringer veldig, veldig mange og en gang får de napp (Kvinne 73 år)

Flere andre informanter uttrykte lignende tanker, fordi svindelen hadde skjedd på en helt vanlig dag, hvor det ikke hadde skjedd noe spesielt i forkant. Dette gjaldt blant annet kvinne 82 år, kvinne 76 år, kvinne 29 år og gutt 18 år, som alle var hjemme da hendelsen skjedde. Dette er med på å understreke poenget om at det det kan skyldes tilfeldigheter, og at svindlerne ikke nødvendigvis er klar over at det har skjedd noe i offerets liv. I forlengelse av dette understreket flere, blant annet kvinne 73 år, kvinne 61 år, mann 37 år og kvinne 41 år, at det kan skje med hvem som helst, som kvinne 61 år beskriver:

> […] Men du kan jo sammenligne med at vi går til et fiskevann og slenger ut snøret. Og så er det noen fisker som svømmer forbi, og så er det noen som biter på. Og jeg er sikker på at de sender ut disse meldingene til mange, mange, mange. Og så er det noen som biter på da, akkurat i et svakt øyeblikk […] (Kvinne 61 år)

Slike oppfatninger samsvarer med funnene til Button mfl. (2014b), som viser at selv om personlige faktorer kan påvirke risikoen, blir mange ofre for digital svindel utsatt gjennom massemålretting, der svindlere sender svindelforespørsler til et stort antall personer uten selektiv utvelgelse. Dette støttes også av van't Hoff-de Goede mfl. (2021) og Leukfeldt (2014), som finner at svindel i stor grad skjer tilfeldig. Digitalisering forsterker denne dynamikken. Som Walklate (2025, s. 501-502) og Twigt (2024, s. 461-463) beskriver, er digitale plattformer utformet på en måte som gir svindlere fordeler: kommunikasjonen skjer raskt, anonymt og uavhengig av fysisk nærhet. Plattformenes sosiotekniske struktur fremmer deling og raske reaksjoner, noe som gjør at meldinger ofte besvares uten nøye vurdering. Samtidig blir individer eksponert for potensielle svindelforsøk nærmest kontinuerlig, ofte uten å være klar over det, gjennom e-post, sosiale medier og meldingsapper. Det er dermed ikke bare mengden meldinger som gjør svindel effektiv, men også om hvordan den digitale

konteksten svekker kritisk tenkning, særlig når tidspress og distraksjon kombineres med troverdige og profesjonelle meldinger. Når informantene bruker metaforer som å «slenge ut snøret i et fiskevann», beskriver de nettopp dette: i et digitalt landskap preget av konstant eksponering og raske avgjørelser, skal det bare et uoppmerksomt øyeblikk til før noen biter på.

I forlengelse av dette legger mann 55 år og mann 68 år til at alder ikke hadde så mye å si i deres tilfeller, da de har gode digitale ferdigheter når det gjelder å oppdage svindel:

> […] Jeg har jo IT-bakgrunn, […] og jeg har også undervist i det med hacking. Så jeg, i mitt tilfelle, tror jeg ikke alder hadde noe å si […] (Mann 55 år)

> Jeg regner meg som ganske erfaren på data. Jeg har jobbet med grafisk design på Mac da. Også jobbet siste 13 årene av yrkeskarrieren min med data, registrering og alt mulig rart […]. Jeg kan data godt, jeg kjenner fellene. Jeg prøvde jo så godt jeg kunne å se om dette her var svindel og bedrag (Mann 68 år)

Som disse sitatene viser kan det virke som at at mann 55 år og mann 68 år opplever at de har god digital kapital og en god digital habitus som gjør dem mer bevisste og bedre rustet til å navigere trygt i digitale situasjoner og håndtere digital trusler (Ragnedda, 2018, Rughinis mfl., 2024; Romele, 2021). Selv om de mener dette, ser man likevel at de ble lurt. Dette kan tolkes i lys av forskning som viser at selv om digital kompetanse kan redusere risikoen for å bli utsatt for digital svindel (se for eksempel Graham & Triplett, 2017), er ikke dette nødvendigvis et «vanntett» vern. Enkelte forskere påpeker for eksempel at digitale ferdigheter ikke alltid beskytter mot cyberkriminalitet (Holt, Bossler & Seigfried-Spellar, 2022, s. 508), eller at det ikke er noen sammenheng mellom å ha digitale ferdigheter og oppleve forskjellige former for cyberkriminalitet (se for eksempel Leukfeldt, 2014). Dette vil jeg komme mer tilbake i diskusjonen.

5.3 Sammenfatning av funnene og oppsummerende refleksjoner

Funnene viser at både eldre og yngre blir utsatt for svindel, men at metodene varierer. Eldre rammes oftere av telefon- og e-postbasert svindel, noen ganger kombinert med identitetstyveri, mens yngre oftere svindles via sosiale medier og netthandel, som falske annonser på Finn.no eller svindel gjennom Vipps og Snapchat. En likhet var derimot at begge aldersgruppene ble rammet av familiesvindel, der svindlere utga seg for å være et familiemedlem.

På tvers av alder var det flere fellesnevnere. Svindlerne virket troverdige, for eksempel ved å utgi seg for å være fra Politiet eller Securitas, og kombinerte teknisk profesjonalitet med mellommenneskelig manipulasjon. De fremsto hjelpsomme og pålitelige, og skapte stressende situasjoner for å utløse raske, følelsesstyrte handlinger. I begge grupper utnyttet svindlerne menneskelige mekanismer som empati, samvittighet, tillit, og ønsket om å hjelpe. Mange informanter uttrykte i ettertid både anger og reflekterte over tegn de burde ha oppdaget, som språklige avvik eller uvanlige forespørsler. Disse teknikkene illustrerer hvordan svindlerne har god digital kapital, som de bruker strategisk til å skape overbevisende situasjoner og manipulere ofrene.

Det var også forskjeller i hvordan svindelen ble oppfattet. Eldre trakk ofte frem livshendelser og økonomi som mulige årsaker til at de ble målrettet, mens yngre beskrev hvordan svindelen passet naturlig inn i deres digitale hverdag. Likevel reflekterte begge grupper over hvordan trekk ved deres alder, enten det gjaldt økonomi, livssituasjon, digitale ferdigheter, eller antatt godtroenhet, kunne ha påvirket hvorfor akkurat de ble lurt. Samtidig mente mange informanter at svindelen først og fremst var et resultat av tilfeldigheter, og at hvem som helst kunne blitt rammet. Dette ble knyttet til hvordan svindlere utnytter romløsheten, anonymitetsaspektet og tempoet som tilbys av internett, samt den sosiotekniske strukturen i sosiale medier.

Til sammen viser dette at sårbarhet for digital svindel ikke er begrenset til bestemte grupper, men kan ramme både eldre og yngre. Dette støtter funnet til Ranchordas & Beck (2025, s. 510) om at sårbarhet for cybertrusler ikke er begrenset til bestemte befolkningsgrupper. Det samsvarer også med Finemans (2010) argument om at sårbarhet er en universell og iboende egenskap ved mennesket, som ikke kan klassifiseres basert på rase, kjønn eller etnisitet, eller i dette tilfellet: alder. Informantens fortellinger viser at sårbarhet er kompleks, og formes av en rekke faktorer. For noen handlet det om alder, for andre om livssituasjon, rutiner, tillit eller tilfeldigheter. Dette er overens med poenget til Dove (2021, s. 67) om at sårbarhet oppstår i samspillet mellom personlige egenskaper, demografiske forhold, livshendelser, atferd, overbevisninger og omstendigheter. Digital svindel bør derfor forstås som et sosioteknisk fenomen, der både teknologiske strukturer og menneskelige faktorer som emosjoner og tillit virker sammen (Kaufmann, 2024, s. 257-258; Powell, Stratton & Cameron, 2018, s. 190). Selv om svindelen skjer digitalt, er det ofte menneskelige og

hverdagslige sårbarheter som gjør den mulig, og at digital svindel i prinsippet kan ramme hvem som helst.

6 Svindelens konsekvenser og ettervirkninger

I samtalene med informantene kom det tydelig frem at konsekvensene av digital svindel er sammensatte og nært sammenvevde, og at de strekker seg langt utover det økonomiske tapet. I dette kapittelet vil jeg vise hvilke konsekvenser informantene opplevde og hvordan disse utspilte seg, både underveis i hendelsen og i ettertid. Jeg vil også belyse hvordan ofrene opplevde møtet med politi, banker og nærstående, og hvordan reaksjoner fra omgivelsene påvirket dem. Til slutt rettes oppmerksomheten mot hvordan svindelen førte til endringer i deres digitale vaner. Kapittelet søker med dette å vise at konsekvensene av svindel ikke bare handler om økonomiske tap, men også om hvordan individet forsøker å forstå, bearbeide og håndtere det de har blitt utsatt for ved å bruke problemfokuserte og emosjonsfokuserte mestringsstrategier.

6.1 To sider av konsekvensene: det økonomiske versus det emosjonelle

6.1.1 Variasjoner i økonomisk påvirkning

Funnene viste at hendelsen hadde økonomiske konsekvenser for noen, men ikke for andre. Mann 68 år og kvinne 29 år, som mistet henholdsvis 8000 og 2000 kroner, opplevde for eksempel bare kortsiktige økonomiske konsekvenser, fordi de fikk tilbake penger. Mann 55 år opplevde heller ingen direkte økonomiske konsekvenser, men uttrykte frustrasjon over at han måtte bruke pengene han brukte på gavekort på noe han ikke trengte. I tillegg opplevde enkelte informanter indirekte kostnader (Barton mfl., 2013, s. 270-272). Mann 68 år brukte for eksempel mye tid på å ordne opp i saken, og kvinne 29 år opplevde at hun måtte legge inn en innsats for å for å få tilbake penger, som hun forteller:

> […] Og måtte jo liksom gjøre litt ekstra arbeid da, for å få tilbake penger, liksom ringe banken og fortelle hva som hadde skjedd (Kvinne 29 år)

Kvinne 61 år opplevde derimot noen umiddelbare økonomiske konsekvenser:

> [..] og så tapt de pengene, 28 000 er jo ganske, det var jo bufferen min da, så det hadde jo konsekvensene at mot slutten av september, da måtte jeg økonomisere litt, for bufferen var jo borte. Det var ikke krise for meg da, for jeg visste jo at jeg hadde

> penger som kom inn på konto [fra salg av den avdøde søsterens leilighet] […] (Kvinne 61 år)

Hun fikk likevel tilbake alle pengene sine, men ikke fra bankene hvor hun hadde gjort pengeoverføringene. Hun forteller at dette var et stort mysterium for henne, og at hun tror at det er svindlerne som har ført det tilbake. Hun valgte å ikke sperre noen kort, da hun ser på det hun opplevde som en engangshendelse.

På samme måte som tilbakebetaling fra banken hadde noe å si, hadde også en slags «tilbakebetaling» fra faren til gutt 18 år noe å si, som han forteller:

> Ja, altså jeg skulle jo til [land]. Jeg var i [land] nå i høstferien, og de 6000 [kronene] var jo en del av sparepengene for den turen. Altså heldigvis nok så sendte jo faren min meg 6000 [kroner] da, sånn at jeg kunne ha det i hvert fall. Så det var han som mistet pengene. Så feriemessig så fikk jeg beholdt pengene, men da mistet jo faren min 6000 [kroner] […] Det føltes veldig dårlig liksom at nå har jeg jo jobbet, spart opp de pengene og så plutselig forsvinner de (Gutt 18 år)

Selv om de økonomiske konsekvensene var lave, mente flere av informantene at konsekvensene ville vært verre ved større tap eller annen livssituasjon, i tråd med tidligere forskning (Notté mfl., 2021: Cross mfl., 2016). Dette kommer spesielt frem hos kvinne 85 år, som mistet 20 000 kroner som hun ikke fikk tilbake. I tillegg opplevde hun at svindlerne åpnet en konto i en bank som hun ikke er kunde hos, og at banken på grunn av dette sperret kortet hennes. Hun håndterte situasjonen ved å bruke kontanter hun hadde liggende, og ved å låne penger fra naboer. I ettertid reflekterte hun slik over tapet:

> Jo, det var tøft for meg med en gang […] jeg ringte jo til broren min en gang og sa at jeg hadde blitt svindlet, «men har de tatt noen penger», sier han. […] «de har fått ut 20.000». […] så sier jeg til han: «Men jeg har jo nå tenkt og tenkt, og ligget våken. Altså, jeg har de pengene, så 20.000, det er ikke all verden for meg. Altså jeg er villig til å ta de og bli ferdig» […] og det var han også enig med meg i. «Eventuelt så betaler jeg det» sa han da. Så det gjorde etter hvert at jeg roet meg ned […] (Kvinne 85 år)

Hun presiserte imidlertid at det hadde vært verre hvis hun var i en annen økonomisk situasjon. Dette er et synspunkt flere av de andre informantene også hadde:

> […] uansett så var det jo så lite beløp at det var ikke noe, hadde det vært et par millioner som var satt inn der, så hadde det vært verre […] (Kvinne 76 år)

> […] altså 23 000 det det står vi i, men for noen er dette en hel årslønn. Økonomisk så er det mye verre for mange som vi kjenner og. Som jeg sa vi lever med det, men det er fryktelig ergerlig likevel, men for noen vil det være nesten sånn: «Da har vi ikke til mat denne måneden». […] (Kvinne 73 år)

> Hvis jeg hadde måttet betale, så hadde jeg slitt veldig. For det er jo ganske tøft fra før, mange regninger og utgifter og sånt, siden vi [hun og mannen hennes] driver en egen forretning (Kvinne 41 år)

Som disse sitatene viser, var det økonomiske tapet håndterbart for noen, men kunne ha langt mer alvorlige konsekvenser for andre. Dette samsvarer med Jansen & Leukfeldt (2018), som fant at den økonomiske skaden varierer mellom ofre, avhengig av om de får penger tilbake eller ikke.

6.1.2 Bak beløpet – den usynlige belastningen

Selv om flere informanter ikke opplevde økonomiske konsekvenser, erfarte de likevel en rekke psykiske og emosjonelle konsekvenser både underveis og i ettertid av hendelsen, også i møte med hjelpetjenester.

Først og fremst viser funnene at mange fikk umiddelbare reaksjoner som en såret stolthet, frustrasjon, panikk, følelse av dumhet, og at de begynte å krisemaksimere. Slike reaksjoner samsvarer med funn fra tidligere studier, som finner at lignende reaksjoner er relativt utbredt (se for eksempel Cross mfl., 2016; Jansen & Leukfeldt, 2018). Som informantene mine forteller:

> […] Da det først skjedde, var jeg jo bare ekstremt frustrert […] veldig sånn panikk og var sånn: «shit, okei, nå er 6000 borte, hva skal jeg gjøre nå?» Så veldig mye frustrasjon, og så, ja, man føler seg jo kjempedum, spesielt når man har hatt alle disse kursene, sett på nyhetene om disse sakene, tenker sånn, det kommer aldri til å skje meg, jeg er klar over sånt, så plutselig skjer det […] (Gutt 18 år)

> […] jeg fikk jo pengene tilbake, sånn at heldigvis så ble det jo ikke noe økonomisk konsekvens, for det klarte jo banken å fikse, men det var jo alt dette her sånn

følelsesrelatert, at det ble veldig sånn stressende situasjon, at jeg ble sånn: «å nei, skjer dette med meg?» Og klarte liksom ikke å skjønne det, og ble liksom stresset og satt ut. Ja, man kjenner jo liksom på sånn flauhet, skam, dumhet, godtroenhet, naivitet, ja […] (Kvinne 29 år)

Altså, jeg tipper jeg skårer ganske høyt på stress og sånn krisemaksimering […] altså tankene mine spinner ganske lett: «Hva bruker de akkurat mine penger på?» […] Jeg blir jo på en måte lei meg og redd for at jeg kanskje bidrar til noe vondt verre, på en måte. Ja, så jeg får liksom både sånn selvfølgelig flauhet og skam, men også litt skyld, sånn: «ah, nei, jeg vil ikke være med i dette sirkuset her» (Kvinne 29 år)

[…] altså økonomisk har det ingen stor konsekvens, men moralsk og følelsesmessig har det veldig stor konsekvens, for jeg føler at jeg satt og snakket med sønnen min. Og det var det ikke. Så litt sånn innbrudd på en måte, følelse hadde jeg. Som er mye verre for oss enn kronebeløpet. Pluss at vi [hun og mannen hennes] kjenner at: «okei her gjorde vi noe veldig dumt» sånn i etterpåklokskapens navn så skulle jo vi ha sett dette lenge før. Og det gnager litt, mer enn de kronene […] Og vi var jo lette å lure. Og det er kanskje noe av det som er verst i dette. Det er ikke de pengene, for de klarer vi oss nok uten, men det at noen har gått inn i vår private sfære på en måte (Kvinne 73 år)

[…] det er ingen som er skadet, det er ingen som er død, det er bare at stoltheten er såret da […] (Kvinne 61 år)

[..] og så tapt de pengene […] Det var ikke en krise av noe slag, det var bare kraftig irritasjon […] jeg kan jo sammenligne dette her med et lite hjerteinfarkt. Bare passe på litt så jeg ikke får det store hjerteinfarktet […] (Kvinne 61 år)

I likhet med disse informantene beskrev også mann 55 år og kvinne 82 år følelser av skam og skyld. Begge har forsøkt å glemme hendelsen og uttrykker at det ikke er sunt å oppleve slikt. En annen informant, kvinne 76 år, omtalte det som å ha gjort en «dumhet». Slike reaksjoner tyder på at flere la skylden på seg selv, i motsetning til ofre for tradisjonell kriminalitet som kanskje oftere plasserer ansvaret hos gjerningspersonen. Funnene peker også på et indre oppgjør, der informantene ikke bare bearbeider økonomiske tap, men også et brudd i egen selvoppfatning, hvor de tenker at dette aldri ville skje med dem. Dette samsvarer med funnene til Cross (2015). Som påpekt av Parti & Tahir (2023) indikerer flere av

informantenes beskrivelser at de emosjonelle belastningene kan oppleves mer tyngende enn det økonomiske tapet i seg selv. Kvinne 73 år beskrev for eksempel opplevelsen som et «innbrudd» i privatlivet, og fortalte at opplevelsen ble ekstra belastende fordi den skjedde hjemme, i en privat, trygg og sårbar situasjon. Som Dove (2021, s. 40-41) påpeker, kan det å bli lurt og utnyttet for andres vinning oppleves svært belastende. Reaksjonene kan også forstås i lys av et samfunn hvor personlig ansvar står sterkt. Å bli utsatt for digital svindel kan da oppleves som et personlig nederlag, som noe man «burde» ha forhindret. Det oppstår dermed en spenning mellom å føle seg «dum» og å føle seg krenket og invadert, noe som tydeliggjør hvor sammensatte og komplekse de psykiske konsekvensene kan være.

Noen opplevde imidlertid at slike følelser avtok etter kort tid. Kvinne 85 år var for eksempel plaget av hendelsen en stund, men var glad for at det gikk så bra som det gikk. Hun opplevde sjokk da identiteten hennes ble stjålet, og tenkte, i likhet med kvinne 29 år, på verst-tenkelige utfall, for eksempel at identiteten skulle være solgt. Til tross for dette endret hun perspektiv til at hendelsen var noe hun kan lære av, som hun forteller:

> Ja, du får et sjokk på en måte. Du blir satt ut. Men likevel så er jeg nok den, jeg henter meg relativt fort inn, men jeg har ikke hatt noe enkelt liv […] Jeg har jo opplevd sterke ting og mye ting som jeg har taklet […] Ja, jeg er nok sterk. Men det er jo livet som har gjort meg sånn […] Og kanskje jeg har evne på en måte til å snu det [..] du lærer av alt, samme pokker hva det er […] Hvis du hadde levd som prinsessen på erten, hvem hadde du vært da? […] uansett hva som skjer deg, så lærer du. Du vokser på det. Så akkurat det jeg sier er viktig å ta med seg. Ikke bare være negativ, for det er positivt også på en måte (Kvinne 85 år)

Hun sammenligner evnen til å takle svindelen med hvordan hun håndterte mulig blindhet og øyeoperasjonen sin:

> […] jeg venter på en operasjon. Så øynene mine […] det er en stor gambling. […] Men jeg har ikke noe valg, jeg blir blind uansett da, kan du si. […]. Så jeg har mye som ligger i meg. Men, ja. Det blir en løsning. Jeg er veldig flink etter hvert å se at det blir en løsning. (Kvinne 85 år)

Disse sitatene viser hvordan kvinne 85 år aktivt omskriver sin egen fortelling ved å vektlegge læring og personlig vekst fremfor nederlag. Dette kan tolkes som en måte å gjenvinne kontroll på, samtidig som det bidrar til å styrke selvfølelsen. En lignende tendens ble også

identifisert hos flere av informantene i Jansen & Leukfeldt (2018), som beskrev svindelopplevelsen som en verdifull læringserfaring. Denne typen fortolkning kan forstås som et uttrykk for en transformativ endring, en livshendelse som endrer hvordan man forstår både seg selv og omverdenen (Pemberton & Mulder, 2025). Kvinne 85 år sin strategi kan dermed forstås som en slags emosjonsfokusert mestring (Lazarus & Folkman, 1984), der hun endret hvordan hun forholdt seg til situasjonen og fant ny mening i det som hadde skjedd.

I likhet med kvinne 85 år, opplevde også kvinne 76 år at man blir sterkere av alt man opplever. Det samme gjelder mann 68 år, som ikke fikk noen varige men av det han hadde opplevd, som han forteller:

> Nei, jeg fikk jo litt forhøyet blodtrykk og var jo veldig sint en stund. Først var jeg sint på han som hadde svindlet meg og så ble jeg jo veldig sint på politiet. Så begge deler fikk det til å koke litt i toppen. Men... Ja, jeg vet ikke om jeg har fått noe varige men av det, på noen vis […]. (Mann 68 år)

I likhet med mann 68 år opplevde kvinne 73 år også at det ikke gikk så mye utover henne over tid, blant annet har det ikke gått utover nattesøvnen hennes. Kvinne 41 år fikk også sterke emosjonelle reaksjoner underveis. Hun tok det særlig tungt at politiet ikke tok affære, da hun hadde brukt mye energi på saken. I tillegg fikk hun nesten ikke sove i starten. Disse følelsene gikk derimot over når betalingene ble slettet. Hun legger til at det ikke finnes en kur for å kurere det de har opplevd og at det kommer til å skje igjen, men ser samtidig på hendelsen som noe hun har lært av:

> Ja, altså jeg har bare fått livserfaring med det, nå har det skjedd, så da må jeg bare prøve å hindre at det ikke skjer igjen […] (Kvinne 41 år)

Noe av det samme som informantene over gjelder også mann 37 år, som først var i sjokk når det skjedde, men dette endret seg etterpå. Han kom tilbake til seg selv og var oppgitt over at dette hadde skjedd. I ettertid begynte han likevel å tvile på sikkerheten sin, og føle på mye usikkerhet. I tillegg begynte han, i likhet med kvinne 29 år, å krisemaksimere og tenke på verst-tenkelig utfall:

> Jeg var jo litt i sjokk da, så jeg måtte få tid til å tenke på det som hadde skjedd da, men jeg har jo alltid sagt det skjer ikke meg. Også skjedde det. Og jeg sitter der og tenker «seriøst?» […] (Mann 37 år)

> Jeg føler meg svakere […] Jeg føler meg alene på en måte. Jeg føler at jeg er overvåket. Jeg er ikke sikret der jeg skal være sikret når det kommer til digitalisering. Dessverre. (Mann 37 år)

> Usikkerheten da, Det er ikke noe hyggelig, nei. Å gå ut og ikke stole på din tilværelse inne der [peker på mobilen]. Og så har jeg jo tenkt på bilder jeg har. Sånne scenarier. Om det finnes noen bilder av meg. Det er det jeg ikke hadde før. […] alt var på stell. Jeg hadde full kontroll. Jeg har fått en usikkerhet som jeg aldri hadde. Det er ikke enkelt. Det blir vanskelig og tøft å gi bort søvnen min til dette. (Mann 37 år)

> Jeg opplevde greia, faktisk, for mottakerne kunne være hvem som helst, men da kom jeg på, hva hvis en av kollegaene mine, en i familien min, var mottakerne […]. Det syntes jeg er ekkelt. Jeg var lettet og glad for at det faktisk var noen jeg ikke kjenner […]. Jeg tenkte på hva som hadde skjedd da, og hva skjer med den relasjonen da? […] (Mann 37 år)

I likhet med mann 37 år opplevde også 25 prosent av deltakerne i undersøkelsen gjennomført på vegne av NordVPN i 2024 å få angst og redusert tillit til digitale tjenester (Zieniūtė, 2024). Også flere av informantene i Notté mfl. (2021) og Jansen & Leukfeldt (2018) opplevde angst, utrygghet online og offline, og svekket tillit både til seg selv, andre og samfunnet generelt. Selv om han opplevde svindelen som belastende, mener han samtidig at det er sunt å oppleve, og at det hadde gjort han mindre naiv. Mann 37 år sitt tilfelle illustrerer hvordan svindel kan få eksistensielle konsekvenser, og ikke er noe som bare kan ristes vekk.

Oppsummert ser man at konsekvensene var kortvarige for noen og mer langvarige for andre, spesielt for mann 37 år. Ingen rapporterte depresjon eller selvmordstendenser, i motsetning til informantene i Notté mfl. (2021) og Cross mfl. (2016). Noen, som mann 37 år og kvinne 41 år, mistet noe søvn, som det er vist at ofre kan føle på i tidligere forskning (se for eksempel Jansen & Leukfeldt, 2018; Borwell mfl., 2022), men ingen slet med det langvarig. Man ser også at noen, kvinne 82 år, kvinne 41 år og mann 37 år, mente at svindel kan skje igjen, noe som kan tyde på at de til en viss grad føler på en form for frykt for gjentatt viktimisering (Borwell mfl., 2022, s. 946)

6.2 Støtte eller stigma? – Møtet med omgivelsene etter svindelen

Erfaringene knyttet til å oppleve digital svindel handler ikke bare om selve hendelsen, men også om hvordan man blir møtt i etterkant av ulike hjelpetjenester og personer i sitt sosiale

nettverk. Det er ofte i møtet med banker, politi og andre aktører at spørsmål om skyld, støtte og tillit aktualiseres. I dette underkapittelet vil jeg se nærmere på hvordan ofrene beskrev kontakten med ulike hjelpetjenester og sitt sosiale nettverk.

6.2.1 Ofrenes møte med politi, banker og andre hjelpetjenester

Ofrenes vei etter svindelen gikk ofte via flere hjelpetjenester: banker, politi og ulike tredjeparter som Klarna og journalister. Å ta kontakt med disse hjelpetjenestene kan ses på som en form for emosjonsfokusert mestringsstrategi (Lazarus & Folkman, 1984).

For de fleste startet prosessen med å kontakte bankene sine. Det var kun kvinne 41 år og mann 55 år som ikke gjorde dette, da de følte at banken ikke var direkte involvert, for eksempel fordi bankkortet deres ikke hadde blitt misbrukt. Blant de øvrige informantene var erfaringene varierte. Noen, som kvinne 61 år, kvinne 29 år og kvinne 82 år, opplevde god hjelp og forståelse. I likhet med dette har det blitt vist i tidligere forskning at ofre for digital svindel rapporterer at det hjelper å snakke med andre for å få råd, støtte og veiledning (Jansen & Leukfeldt, 2018; Cross, 2016). Kvinne 29 år og kvinne 82 år beskrev begge møtet med banken som positivt, da de refunderte det tapte beløpet og viste empati:

> Den var veldig bra. Jeg traff ei innmari ålreit jente. Hun var […] så forståelsesfull, at det var ingen sak. […] Men det var en veldig positiv opplevelse, jeg tenkte, du verden. Jeg var sikkert heldig […] (Kvinne 82 år)

Andre, som kvinne 85 år, kvinne 76 år, mann 68 år og mann 37 år, møtte flere utfordringer og hadde mer blandede opplevelser. Kvinne 85 år opplevde for eksempel at hun måtte oppgi mye informasjon og fylle ut mange papirer. I tillegg opplevde hun utydelig veiledning og dårlig kundeservice, og trekker frem at hun blant annet ble møtt av forventninger om at hun skulle ha gjort ting på forhånd som hun ikke klarer eller visste at man måtte gjøre:

> […] men så kom jeg til banken og så sier hun [navn på ansatt i banken]: «har du sperret alt?» «Sperret alt? Hva da», sier jeg. «Ja, du må sperre sånn at ingen kan ta opp lån i de forskjellige institusjoner og banker» [sier hun]. Nei, hvordan skal jeg vite det da? Kunne ikke banken ha sagt det?. Det er jo ikke bare meg som kommer i en slik situasjon. Og det var et tastetrykk for henne […] (Kvinne 85 år)

Hun opplevde hele prosessen som lang og belastende, og vurderte på et tidspunkt å bytte bank. Senere hadde hun imidlertid en positiv opplevelse med en annen ansatt, da hennes faste

rådgiver var opptatt. Den ansatte hjalp henne med å installere ny bankaapp og bankID-app, ga tilbakemelding om at det var bra at hun snakket høyt om det hun opplevde, og møtte henne med forståelse, som hun forteller:

> […] Så jeg har sittet helt hjelpeløs […] og grått utenfor Sparebank1 […] det har vært så fortvilende for meg. «Jeg synes det er helt forferdelig å høre» sa hun. Men nå er alt i orden, så jeg er kjempefornøyd. Så det må noen greier til for at du skal komme i havn» (Kvinne 85 år)

Videre fikk kvinne 76 år god hjelp av sin egen bank, men slet med Lunar Bank, som krevde mye for at kontoen svindlerne hadde opprettet kunne bli slettet. De ba henne blant annet sende inn passkopi, noe hun ikke ønsket og opplevde som tungvint. I tillegg opplevde hun at prosessen føltes unødvendig lang og krevende, og uttrykte følgende:

> […] jeg ble jo litt sur på den banken som da ikke ville slette kontoen. Det var nå det, men, ellers så har det vært greit. Og banken min er grei […] (Kvinne 76 år)

Kvinne 73 år kontaktet også banken sin for å prøve å stoppe overføringen av pengene. De kunne ikke gjøre dette, men de sperret kontoen som pengene var sendt fra. Hun syntes dette gikk fint å få fikset, og hadde også forståelse for at hun ikke fikk tilbake pengene:

> […] altså jeg har ikke forventet å få tilbake penger fra banken […] Det var vi som gjorde den feilen, så banken kan ikke klandres […] Jeg skjønner jo at banken ikke kan betale tilbake når det er kunden selv som har overført summen. Det synes jeg at er rimelig (Kvinne 73 år)

Hun kontaktet også Nordea Bank, som var den angivelige banken svindleren var kunde hos. Hun hadde håpet at de kunne gi informasjon om hvem svindleren var, men de kunne ikke gi ut denne informasjonen fordi de har taushetsplikt. Hun opplevde derfor at de ikke var til noe hjelp, som hun forteller:

> Og der fikk vi ikke mye hjelp altså. Det var ganske sånn kroken på døra (Kvinne 73 år)

Mann 68 år hadde et lignende håp om at banken kunne spore svindleren via kontonummer og stoppe videreføring av pengene. Banken oppga navnet på eieren av kontonummeret da de mistenkte at det var mer svindel på gang, men kunne ikke stoppe videreføringen. De krevde

også politianmeldelse før de kunne refundere pengene, men han fikk til slutt tilbake pengene. Han opplevde derfor at banken var veldig imøtekommende og hadde gode rutiner på hvordan de skal håndtere slike situasjoner, men syntes også at de var litt vel «firkantet», som han forteller:

> […] Så jeg oppfattet det vel kanskje litt firkantet. De sa at de hadde en viss mistanke om at dette her var i svindel og sånt, men de måtte ha fra politiet før de kunne stoppe og sånt da i tilfelle han kom og ville ha pengene, så kunne de ikke nekte han det. (Mann 68 år)

Mann 37 år tok også kontakt med begge bankene sine og opplevde dem som samarbeidsvillige og hjelpsomme med å sperre kort og fikse nytt kort. Likevel opplevde han at det krevde litt av han for å få en løsning på situasjonen. Han måtte sende en del mailer frem og tilbake med forklaringer, samt legge inn reklamasjon før han til slutt fikk tilbake begge beløpene. I tillegg fikk han beskjed fra en av de bankansatte om at de ikke ville hjelpe han hvis det skjer igjen:

> Det eneste som jeg ikke synes var hyggelig og skummelt var at det ene stedet sa at: «nå må du passe på neste gang så hjelper ikke vi deg». Hvordan skal jeg passe på? (Mann 37 år)

Som disse sitatene viser, kan kontakt med banker være både støttende og frustrerende, og de spiller derfor en viktig rolle i hvordan svindel oppleves i etterkant, både praktisk og emosjonelt. Dette kommer særlig frem hos kvinne 85 år, som opplevde dårlig kommunikasjon og urealistiske forventninger, og mann 37 år, som følte at ansvaret for å unngå ny svindel ble lagt på ham, til tross for at bankene også har et ansvar for å beskytte kundene sine. Dette samsvarer med tidligere forskning, som viser at ofre både kan få støtte og oppleve sekundærviktimisering, for eksempel gjennom manglende empati eller ved å bli tillagt skyld (Jansen & Leukfeldt, 2018; Cross mfl., 2016),

For de fleste var det neste steget å ta kontakt med politiet, med unntak av mann 37 år, som valgte å ikke anmelde på grunn av latskap, hans useriøsitet i digitale situasjoner, og tidligere negative erfaringer med politiet. Dette samsvarer med tidligere forskning som viser at negative erfaringer med politiet kan påvirke ofres vilje til å rapportere (Reisig & Holtfreter, 2007), og at beslutningen om å anmelde påvirkes av både individuelle og kontekstuelle vurderinger (Kemp, 2020). Videre kan funnet om latskap ses i sammenheng med funnene i

Cross mfl. (2016, s. 7–8), hvor flere informanter valgte å la være å rapportere for å slippe stresset og innsatsen en strafferettslig prosess kan kreve.

Blant de som tok kontakt med politiet opplevde flere dem som lyttende og støttende. Kvinne 76 år fremhevet for eksempel møtet med politiet som veldig hyggelig, fordi de forsikret henne om at det var svindlerne sin skyld. I likhet med dette hadde også kvinne 29 år og kvinne 61 år positive opplevelser med å anmelde saken. Kvinne 29 år fikk støtte, og hadde forståelse for at saken hennes ikke kunne prioriteres:

> Jeg opplevde det egentlig som helt greit. Det var på en måte noe jeg forventet. Og så ønsker jeg at de heller kanskje prioriterer å ta noen større caser. Altså jeg hadde jo bare 2000 [kroner]. Det var litt lite, kanskje noen andre større caser heller bør prioriteres (Kvinne 29 år)

Kvinne 61 år var også fornøyd med hjelpen hun fikk av politiet, fordi de var engasjerte:

> Jeg var veldig fornøyd med politiet, fordi at han stilte spørsmål, og jeg måtte sende dokumentasjon, og han er på saken liksom […] det er fortsatt ikke henlagt. Når jeg sender han en mail med navn og telefonnummer og forskjellige opplysninger, så ja, «vi legger det inn i saken din» [svarer de da] […] (Kvinne 61 år).

Disse erfaringene kan ses i likhet med informantene i Cross (2018b) og Jansen & Leukfeldt (2018) som opplevde å bli møtt med empati, forståelse og ekspertise, noe som bidro positivt til bearbeidingen av opplevelsen.

For andre var prosessen mer utfordrende. Kvinne 85 år strevde med å få hjelp på sin lokale politistasjon, og opplevde politiet som lite tilgjengelig og lite hjelpsomme:

> […] jeg kom ikke gjennom til politiet, og da tenkte jeg: «ok, jeg kommer til å gå dukken av dette, for ikke sover jeg noen ting» […] (Kvinne 85 år)

> […] det var ikke bare å få anmeldt dette […] jeg måtte gjennom hele systemet […] Det var altså så vanskelig at det har nesten sjokkert meg (Kvinne 85 år)

Selv om hun ikke fikk hjelp på politistasjonen i hjembyen sin, satte de likevel saken hennes over til en annen politistasjon, noe hun hadde forståelse for fordi hun vet at politiet har mye å gjøre. På denne politistasjonen fikk hun mye hjelp og støtte. De noterte ned all informasjon

hun hadde, og hjalp henne også med å komme i kontakt med en annen ansatt på politistasjonen i hjembyen sin. Denne ansatte tok kontakt med firmaet svindlerne hadde brukt for å ta ut penger på hennes vegne, selv om han egentlig mente at det var noe hun kunne gjøre på egenhånd. Kvinne 85 år opplevde derimot at hun ikke ville klart dette, da hun selv sliter med teknologi, som hun forteller:

> […] Han sa at: «dette skulle jo du egentlig gjøre», men jeg kan ikke og får ikke gjort en dritt heller. Er det sånn med oss gamle at vi sitter her? [og så sa han]: «Ja, men der må du ha en sønn eller datter eller i det hele tatt». Ja, men når du ikke har det, det kan jo være flere enn meg som er alene […] Så man blir, jeg vil si, man blir konfrontert med så mye i samfunnet som er vanskelig. Det avstedkommer så mye på en måte. Du skjønner meg? (Kvinne 85 år)

Til tross for dette syntes hun at denne politibetjenten var helt enestående. Han viste stort engasjement, og tilbød seg å være tilgjengelig ved behov, som hun forteller:

> […] Så han sa: «jeg står til disposisjon, anytime». Jeg fikk privatnummer og i det hele tatt. Så jeg var så glad når jeg gikk ut fra det kammeret at jeg nesten kunne danse (Kvinne 85 år)

Kvinne 85 år sin historie illustrerer hvordan det å stå alene uten nære pårørende kan gjøre slike situasjoner ekstra krevende. Hendelsen utløste ikke bare praktiske utfordringer, men førte også med seg en rekke andre vanskeligheter, som en følelse av å være alene og å bli overveldet av samfunnets krav. Hennes erfaring illustrerer dermed hvordan svindel kan forsterke eksisterende sårbarhet og ramme hardere enn det kanskje ser ut umiddelbart.

Flere informanter, blant annet kvinne 82 år, kvinne 41 år og gutt 18 år, savnet at politiet viste mer interesse for sakene deres. Alle sakene deres ble henlagt, noe kvinne 41 år opplevdes som spesielt belastende og tungt. Dette kan ses som en form for sekundærviktimisering, hvor den opprinnelige belastningen ble forsterket i møte med hjelpeapparatet (Jansen & Leukfeldt, 2018). Samtidig uttrykte de en viss forståelse for politiets situasjon, med tanke på at slike saker kan være vanskelige å løse, tidskrevende og ressurskrevende:

> Nei, jeg skulle ønske at de gjorde noe med det. Om ikke så at jeg får tilbake pengene, så kunne de kanskje prøvd å finne ut hvordan det skjedde […] Men så vidt jeg vet, så

> gjorde de ikke noe med saken. De snakket ikke med personen som gjorde det […] (Gutt 18 år)

> Altså, nå er det jo en ganske stor greie i Norge at politiet har veldig lite ressurser, og at de som regel henlegger saker da, med mindre det er en veldig grov forbrytelse. Så hvis det er noe mildere, eller hvis det er sånn svindel, eller tyveri, så er det ganske vanlig at politiet bare henlegger saken. Og man kan ikke skylde på dem for det, for det er jo at de mangler ressurser, og at de ikke har nok sånn personal for å håndtere det (Gutt 18 år)

> Nei, både og. Jeg skjønte jo at det ikke inngår politi og at saken er liten prioritet. Og de har sikkert andre ting de skal gjøre. Og som sagt, de har ingen mistenkt person. De er sikkert maktesløse, de vet ikke hva de skal gjøre (Kvinne 41 år)

Mann 68 år beskrev en mer frustrerende prosess. Selv om politiet var imøtekommende når det gjaldt å få tilbake penger, var han svært skuffet over at saken ble henlagt raskt. Politiet mente at svindleren også kunne være et offer, men han følte at det var en feilslutning:

> Så da satt jeg og beit negler litt til politiet fikk gjort jobben sin, og pengene kom ut og tilbake igjen. Politiet var forsåvidt imøtekommende med å få pengene tilbake. Men etter det så opplevde jeg det skremmende dårlig. De henla saken på null svisj. Og mente at han karen her, han hadde igjen blitt lurt av noen i England som han skulle liksom selge klokker for. Han hadde vært litt dum muligens, men han hadde da vært et offer han også mente politiet […] men når han sender meg en falsk ID for å bevise at dette er meg og sånn. Da har han gått over en strek. Da er det ikke bare at han er blitt lurt. Så begredelig møte med politiet, må jeg si (Mann 68 år)

> […] jeg hadde jo sett for meg at han hadde blitt straffet da. En eller annen straff som gjorde at han ikke syntes det var noe moro å fortsette med svindel og bedrag […] Men sånn som det var nå, så er det jo bare for han å fortsette uten at det skjer noen ting. Og det synes jeg ikke er en rettsstat verdig (Mann 68 år)

> Så nei, jeg er ikke fryktelig imponert over politiet. Jeg ser at vi har brukt for dem. Absolutt. Men de er som noen tannløse gamle tanter til tider (Mann 68 år)

I tillegg har denne opplevelsen gjort at han nå velger å ikke si ifra til Politiet når han ser åpenbar svindel på nettet. Han har for eksempel sett at den samme svindleren fortsatte å markedsføre seg i tiden etterpå, som han forteller:

> Ja, han brukte den igjen […] og for alt jeg vet, så holder han på fremdeles. Det er jo tragisk, men nå har jeg gjort mitt, synes jeg da, og mistet jo alt initiativ til å si ifra når jeg ser åpenbar svindel på nettet. Normalt ville jeg ha varslet det som en god samfunnsborger, men med politiets respons så ser jeg ikke det som noe interessant å bruke tid på (Mann 68 år)

Mann 68 år rapporterte svindelen i håp om å oppnå rettferdighet, slik også informantene i Cross (2018b) gjorde. I tillegg ble han, i likhet med informantene i Notté mfl. (2021), frustrert over at gjerningspersonen ikke ble straffet, selv om han fortsatt var synlig aktiv på nettet.

Til slutt var det to informanter som hadde gjennomgående negative opplevelser med politiet. Kvinne 73 år opplevde at politiet viste liten interesse og følte også at hun ble avvist av en resepsjonist, som hun forteller:

> […] Men så leverte vi en ganske fyldig anmeldelse […] Det synes jeg var en veldig trist opplevelse for, for det første så måtte jeg inn en 2-3 dører, og så var det en liten luke, som det kom en ung dame inn i. Og jeg tenkte at jeg må jo forklare deg littegrann om dette selv om den skriftlige anmeldelsen var veldig utfyllende. Men jeg opplevde ikke at det var interesse i det hele tatt for det […] (Kvinne 73 år)
>
> Politiet hadde… så merkelig politi, det var jo ikke politiet, det var jo en ung resepsjonsdame (Kvinne 73 år)
>
> […] da blir jeg skuffet, men også forbanna. Jeg hadde hatt lyst til å prate med en politimann jeg. Men jeg ble avvist av en ungjente i luka […] men jeg skjønner jo deres situasjon […] (Kvinne 73 år)

Kvinne 73 år beskrev digital svindel som et «stort lite samfunnsproblem», som trenger mer oppmerksomhet. Etter hendelsen hadde hun derfor håpet på større interesse fra politiet, særlig fordi hun hadde hørt at det var ansatt flere for å håndtere økonomisk kriminalitet. I stedet fikk hun en kort beskjed om henleggelse uten forklaring, noe som førte til skuffelse. Selv om hun

ikke forventet at politiet skulle prioritere det økonomiske tapet, hadde hun, i likhet med gutt 18 år, håpet på mer interesse for det hun hadde opplevd. Samtidig uttrykte hun forståelse for politiets begrensede ressurser. Dette samsvarer med funn fra Jansen & Leukfeldt (2018), hvor ofre opplevde politiet som utilgjengelige, med lav kompetanse og lite vilje til oppfølging. Et interessant aspekt i hennes fortelling er hvordan hun omtaler resepsjonisten som «en ungjente i luka», en beskrivelse som antyder en opplevd avstand i alder, erfaring og autoritet. Det kan tolkes som en skuffelse over at forventningene om å møte en autoritetsfigur ikke ble innfridd, noe som igjen svekket tilliten og følelsen av å bli tatt på alvor. Skuffelsen hennes var derfor ikke bare rettet mot enkeltpersonen hun møtte, men mot politiet som institusjon og måten de fremsto på i møtet. Dette svekket opplevelsen av å bli anerkjent og vist respekt.

Til slutt opplevde også mann 55 år liten interesse fra politiet. Han fortalte at han hadde et pågående svindelforsøk. De spurte hvor mye penger det var snakk om, og når de fikk vite at det var 4000 kroner, så var de ikke interessert. På spørsmål om han mener Politiet burde ha reagert annerledes svarer han:

> Jeg synes absolutt det […]. Her hadde de en pågående, jeg hadde jo, om det var en person eller om det var AI på tråden, så hadde jeg en direkte linje inn. Da mener jeg at det burde være mulig å finne IP-adresser og finne litt mer ut av hvem som står bak. Jeg skjønner at det er lite penger for en enkeltperson som meg, men det er jo enorme summer som de svindlerne svindler til seg. La oss si at det er én av tusen som går på det der, og så sender de det til hundre tusen. Det er hundre ganger fire tusen, og da er det firehundre tusen som de har stjelt av folk uten at de bryr seg. Og de bryr seg virkelig ikke (Mann 55 år)

Disse funnene viser at informantene sitter på et bredt et spekter av opplevelser, fra hjelpsomhet og empati til frustrasjon og skuffelse. Dette samsvarer med tidligere studier som viser at møtet med politiet kan være både støttende og en ny belastning for ofre (Jansen & Leukfeldt, 2018; Cross, 2018b).

Ved siden av politi og bank, så flere informanter behovet for å søke hjelp hos tredjeparter. Kvinne 61 år tok for eksempel kontakt med forsikringsselskapet sitt etter å ha vært i kontakt med både politi og bank. Selv om hun fikk beskjed om at forsikringen ikke dekker tapet, fikk hun tilbud om juridisk bistand og hjelp til å legge press på bankene. I andre tilfeller ble kontakt med tredjepartsaktører avgjørende for utfallet. Kvinne 41 år tok kontakt med Klarna,

ettersom forhåndsbetalingene til svindlerne var gjort gjennom deres plattform. Til å begynne med klarte hun å stoppe regningene, fordi Klarna opererer med 30 dagers betalingsfrist. Hun dro derfor på ferie. Når hun kom tilbake, oppdaget hun at betalingene var gjenåpnet. Til tross for flere forsøk på å rydde opp ved å kontakte Klarna igjen, fikk hun beskjed om at de ikke fant en løsning. Hun forteller følgende om denne opplevelsen:

> Klarna er veldig profesjonelle, de burde finne ut dette med en gang, vi burde ikke ha jobbet så hardt for å bevise det […] (Kvinne 41 år)

I frustrasjon tok hun kontakt med en journalist, som ringte Klarna på hennes vegne, og det endte med at saken ble løst:

> […] Så det var en veldig vanskelig og tung kamp å ta selv. Men som sagt, vi bestemte oss for å gå til en journalist. Og journalistene har litt høyere stemme enn oss, så vi ble hørt (Kvinne 41 år)

Gutt 18 år erfarte det samme som flere andre informanter: å bli sendt mellom ulike aktører uten klare svar. Etter å ha sendt reklamasjon til både banken og Vipps, fikk han beskjed om at ingen av dem kunne ta ansvar, siden han selv frivillig hadde sendt pengene, noe han også hadde forståelse for. Han forteller følgende om denne opplevelsen:

> Det var litt vrient først, fordi på banken sin nettside står det at hvis det gjelder vipps-transaksjoner, så skal jeg kontakte Vipps. Men når jeg ringte Vipps, så sa de at jeg skal kontakte banken min. Så der satt jeg litt fast imellom, så vi sendte reklamasjon til begge stedene bare […]. (Gutt 18 år)

Til slutt gjelder dette kvinne 85 år, som i tillegg til å kontakte egen bank (DNB) og Norwegian Bank, også kontaktet firmaet hvor svindlerne hadde forsøkt å låne 50 000 kroner og fått ut 20 000 kr. Firmaet noterte ned alt, men det skjedde ikke noe mer. Hun ble møtt av forventninger om at hun skulle ha fikset mye selv, som hun sier:

> Ja, jeg ringte dit og presenterte meg og sa dette. Og han sa: «ja, men du må anmelde og du må gå på nett og du må hente ut». «Ja, men jeg er ikke der» sa jeg. Og du ser, 85 år og skal låne 50.000, det er vel ikke så vanlig? […]. (Kvinne 85 år)

Hun savner at bedriften stilte flere spørsmål, og mener at de burde ha tenkt mer logisk, at det ikke er så vanlig at en kvinne på 85 år skal låne så mye penger. Det var på bakgrunn av denne

manglende hjelpen at hun, som nevnt tidligere, var så takknemlig for politimannen som tok kontakt med firmaet på hennes vegne.

Samlet viser funnene at hjelpen informantene mottok, varierte betydelig. For noen ble hjelpesystemet en kilde til støtte og anerkjennelse, mens det for andre opplevdes som en ekstra belastning. Flere fortalte at de måtte legge ned mye innsats å bli hørt, blant annet ved å kontakte flere aktører, og at de i praksis sto alene i prosessen. Kvinne 41 år fikk for eksempel ikke en løsning før hun til slutt tok kontakt med en journalist. Gutt 18 år ble i sitt tilfelle sendt mellom Vipps og banken uten å få en tydelig løsning, og endte opp med å måtte sende reklamasjon til begge. Dette illustrerer det som i tidligere forskning omtales som «the merry-go-round effect» (Button mfl., 2009a; 2009b), hvor ulike aktører skyver ansvaret over på hverandre. Også kvinne 85 år opplevde noe lignende da hun måtte forholde seg til flere politistasjoner, banker og firmaet svindlerne hadde tatt opp lån hos. Som Cross (2018c, s. 4) påpeker, kan det være både krevende og komplisert å få støtte etter å ha blitt svindlet. Dette kommer også frem i mine funn, der mangel på koordinering og uklare ansvarsforhold mellom aktørene forsterket følelsen av å stå alene. Hvordan informantene ble møtt av hjelpetjenester, blir dermed en sentral del av fortellingen om hva det vil si å bli svindlet, og hva det krever å komme videre.

6.2.2 Sosial respons: reaksjoner fra familie og venner

De fleste informantene valgte å dele historien sin med familie og venner, eller andre bekjente som kollegaer eller naboer. Kvinne 85 år fortalte naboer som hjalp henne med anmeldelsen, mens kvinne 61 år delte historien sin på Facebook. Dette skiller seg fra tidligere forskning, hvor det blir vist at mange holder det de har opplevd skjult på grunn av skam og skyldfølelse (Parti & Tahir, 2023; Button mfl., 2009a), eller frykt for å bli sett på som godtroende (Dove, 2021, s. 41).

Felles for flere av informantene var at de ønsket å fortelle om opplevelsen sin for å være åpne, men også for å advare andre om at de også kan bli svindlet. Dette samsvarer med tidligere forskning som finner at ofre ofte har et altruistisk ønske å forhindre at flere blir rammet (Cross mfl., 2016; Cross, 2018b). Eksempler fra intervjuene inkluderer:

> […] Så vi forteller det til de vi vet og treffer. Og sier: «jeg er blitt lurt. Jeg har blitt svindlet, det kan du og bli. Følg med sånn og sånn». For vi har gjort en nyttig erfaring der (Kvinne 73 år)

> […] jeg fortalte dette til alle ansatte på jobben […]. Jeg synes det var en litt morsom historie, men også litt sånn til skrekk og gru, da. Her må man faktisk passe på, fordi selv om du får en mail fra de nærmeste, så må du ha garden oppe […] (Mann 55 år)

> Ja, jeg sa vel ifra til så godt som alle for å advare om hva som hadde skjedd (Mann 68 år)

Selv om flere valgte å dele historien sin, tok det noe tid for enkelte. For eksempel var kvinne 85 år i sjokk etter hendelsen og trengte tid før hun kunne sette ord på det. Kvinne 76 år valgte i utgangspunktet ikke å si så mye, og begrunnet det slik:

> Jeg føler vel kanskje at jeg ikke trenger ikke si det så veldig mye, fordi at da føler jeg at jeg må fortelle såpass mye om det. […]. Også er det det at […] jeg visste jo før jeg gjorde det, at dette skal jeg ikke gjøre […] (Kvinne 76 år)

Utsagnet peker ikke nødvendigvis på frykt for å bli oppfattet som godtroende, men heller personlige skuffelse over å ha handlet mot egen bedre viten, noe som i seg selv kan gjøre det vanskelig å være åpen. Først etter at en venninne delte at hun hadde blitt utsatt for noe lignende, åpnet også kvinne 76 år opp, noe som viser hvordan felles erfaringer kan åpne opp for gjensidig deling og fungere som døråpnere.

De fleste av informantene ble møtt med støtte, sympati og forståelse fra dem de fortalte om svindelen til, som de forteller:

> Ja, de fleste hadde vel sympati med meg. Det var ingen som mente at jeg var en lettlurt tosk. De skjønte at her var det veldig proft gjennomført. Så det jeg fikk av reaksjoner var vel om det, og at de mente at jeg kanskje ikke hadde brukt for en så dyr klokke (Mann 68 år)

> Nei, altså, familien lo litt av det hele, men jeg tror at alle har blitt enda mer bevisst, når jeg til og med ble lurt […] Det var ingen som hadde noen nega.. eller hadde noe sånne reaksjoner som at «herregud hvor dum du er som lot deg lure av det». Det var ikke det […] (Mann 55 år)

> De var jo sånn: «falt du virkelig for det [navnet til informanten]?» Så jeg var sånn: «ja, det var dumt». Og faren min sa jo at han skjønner at jeg falt for det […] Men sånn

> vennene mine da, på min egen alder, de syntes det var morsomt […] ingen ble sint på meg. Det var ikke sånn: «er du helt dum, hva er det du driver med?». Det var køddestemning. Vi syntes det bare var morsomt, så lo vi av det (Gutt 18 år)

> […] Og jeg har hatt noen som ringte meg og spurte: «hvordan har du det?». Jeg fortalte at jeg hadde blitt svindlet, og fikk som svar: «Men det hadde aldri jeg blitt». «Nei», sa jeg. Og det er mange som har sagt det og etterpå har kommet og bedt om unnskyldning […] (Kvinne 85 år)

> Aller først var det jo familie som fikk vite det med en gang. De var jo med meg da jeg satt og pratet med han karen. Så de husker jeg […] ble litt stresset med meg, og […] var bare behjelpelige og sånn. Og så er det vel mer nå i ettertid, at man liksom ler og tuller med det da (Kvinne 29 år)

Det var også eksempler på mer ambivalente reaksjoner, ikke direkte kritikk, men en undertone av undring eller skepsis. Dette gjelder for eksempel kvinne 61 år som fikk støtte av familie og venner, samtidig som noen også lurte på hva hun hadde rotet seg bort i. Hun fikk også fordømmelse fra et nettroll etter at hun delte saken sin i en avis, som hun forteller:

> […] Den eneste fordømmelsen jeg har fått, det var fra en sånn nettroll som kommenterte: «ingen som er 100% kan gå på en sånn felle som det der» […] (Kvinne 61 år)

Til slutt var det noen som også opplevde at folk var sjokkerte og bekymret:

> Nei, de var jo sjokkerte, for de har jo hørt om dette, men det rammer jo ikke oss ikke sant. Og [navn på sønn] […] han ble jo veldig skeptisk og syntes at vi skulle låse dørene (Kvinne 73 år)

> Ja, de ble overrasket over at vi hadde blitt svindlet, men samtidig, de har også blitt utsatt for svindel […] De ble litt sjokkert over at det her skjer nå […] Men skjønte at det hadde skjedd, det er jo følelsene som tok avgjørelsen (Kvinne 41 år)

Samlet viser disse funnene at det å dele erfaringen sin ikke bare handler om å formidle en hendelse, men også om å bearbeide den og skape mening. Delingen ble for flere en måte gjenvinne kontroll, advare andre og skape fellesskap. Samtidig tok det litt tid for noen før de fortalte om det, fordi det innebar å måtte forsvare egne valg og stå i egen sårbarhet. I

motsetning til tidligere forskning, som viser at skam og skyldfølelse er hovedårsaker til at man ikke sier noe (Parti & Tahir, 2023; Cross mfl., 2016; Button mfl., 2009a), viser mine funn en mer sammensatt vurdering, der også emosjonell belastning og reaksjoner fra familie og venner spiller inn. I tillegg ser man at flertallet ble møtt med støtte, forståelse og empati, noe som står i kontrast til tidligere studier, der «victim blaming» var utbredt (Notté mfl., 2021; Cross, 2016). Blant mine informanter var slike reaksjoner unntaket snarere enn regelen. Noen opplevde at folk lo og stilte spørsmål ved hvorfor de falt for det, men latter fungerte oftest som en måte å lette stemningen og normalisere situasjonen, snarere enn som kritikk eller fordømmelse. Disse funnene kan tyde på at stigmaet knyttet til å ha blitt svindlet er i endring, i hvert fall i norsk kontekst, og at ansvar i større grad plasseres hos svindleren fremfor offeret. Samlet viser funnene at det å søke støtte for mange var en vellykket emosjonsfokusert mestringsstrategi (Lazarus & Folkman, 1984), som bidro til å redusere selvbebreidelse og bygge opp selvbildet, i tråd med tidligere forskning (Jansen & Leukfeldt, 2018; Cross mfl., 2016). Dette står i kontrast til møtene med hjelpetjenestene, som i mange tilfeller ble opplevd som lite støttende.

6.3 Endringer i digitale vaner og bruk av teknologi

I tillegg til konsekvensene nevnt tidligere, fortalte flere informanter at svindelen hadde endret hvordan de forholder seg til teknologi og digitale tjenester.

Dette gjaldt først og fremst kvinne 82 år, kvinne 76 år, kvinne 61 år, mann 68 år og gutt 18 år, som fortalte at de allerede var bevisste på digital sikkerhet og hadde vært varsomme før hendelsen, men som likevel endret sine digitale vaner. Begrunnelsene for denne forkunnskapen varierte. Mann 68 år begrunnet det med at han har jobbet mye med data, mens gutt 18 år begrunnet det med at han hadde lært om det på skolen:

> Ja, jeg var helt klar over det, fordi linjene jeg går på, første året så er det jo både medieproduksjon og IT, så vi hadde jo veldig mange IT-kurs og lærte om dette, det er jo det som er ironien bak at jeg falt for det, så vi har jo lært veldig mye om det, forskjellige måter man kan svindle folk […] og hvor det skjer, og jeg har jo hørt om vippssvindel før […] Det er derfor det ble så morsomt at jeg falt for det, når vi først hadde hatt så mye om det (Gutt 18 år)

Selv med slik forkunnskap og bevissthet, beskrev de fleste informantene hvordan svindelhendelsen førte til konkrete endringer i deres digitale vaner. Mange fortalte at de

hadde blitt mer skeptiske og forsiktige i sin digitale praksis, og hadde begynt å kontrollere avsendere på e-poster og meldinger, unngå å svare på ukjente telefonnumre, og dobbeltsjekke identiteten til den som tok kontakt. I forbindelse med dette fortalte kvinne 73 år at hun hadde utviklet en strategi der hun stiller kontrollspørsmål dersom noen ringer, som kun familiemedlemmene kan svare på. Dette skyldes at hun ble fortalt av sønnen sin at svindlere kan bruke stemmeprøver av han. På lignende vis fortalte mann 68 år at han nå alltid vil ringe opp igjen og bekrefte identiteten til den som ringer dersom han blir spurt om å overføre penger. Han uttrykte også bekymring for hvordan kunstig intelligens kan endre utførelsen av svindel og mente at vi trolig vil møte trusler vi i dag ikke engang kan forestille oss.

Flere beskriv lignede tiltak i hverdagen. Kvinne 29 år fortalte at hun nå er mer forsiktig når hun kjøper ting på Finn, og at hun alltid kontrollsjekker selgere på Facebook. Det samme gjelder gutt 18 år, som en gang i høstferien fikk melding av faren sin som ba om 3000 kroner, og da valgte å ringe han og be om en selfie for å forsikre seg om at det faktisk var han. I tillegg trakk mann 55 år frem at vi ikke har full kontroll på hva som er svindel og ikke, og at han derfor har begynt å sjekke alle mailer og e-postadresser, som han forteller:

> Ja, jeg er enda mer obs nå. Jeg er litt godtroende, jeg må innrømme det. Jeg er sånn som lar meg lett lure av pranks og sånne ting som folk setter i gang. Jeg bare tror på folk, men jeg merker det. Nå er jeg mistenksom uansett. Uansett hvor det kommer mail fra nå, som ber meg om noe som helst, så sjekker jeg e-postadressen. Altså jeg går bak, ikke sant? For det kunne jeg gjort med den, for det sto jo fra rektors navn, men det er jo sånn at når du går nærmere inn og sjekker e-post, så kan du i de fleste tilfellene se om dette her er fra en annen e-post enn den utgir for å være fra (Mann 55 år)

Endringene handlet ikke bare om økt forsiktighet. Flere gjorde også økonomiske tilpasninger. Kvinne 85 år og mann 68 år sluttet for eksempel å handle på nett, eller handlet kun hos kjente, registrerte aktører. I tillegg reduserte kvinne 61 år midler på sine kontoer og vurderte å kjøpe ID-tyveriforsikring. Slike endringer samsvarer med funn fra Jansen & Leukfeldt (2018), der flere av informantene valgte å ha lite beløp på brukskonto, sjekke nettadresser, og være mer forsiktig og sjekke ordentlig hva de gjør når de handler på nett.

I noen tilfeller tok også informantene i bruk ny teknologi som et ledd i å beskytte seg. Kvinne 85 år lastet for eksempel ned mobilbankapp og BankID-app, mens kvinne 76 år tok i bruk et

spamfilter fra Telenor. Hun håpet at dette kunne luke ut noen svindelforsøk, men understreket samtidig at hun alltid må se gjennom dette, da også legitime henvendelser kunne forsvinne. Videre valgte mann 68 år å følge med på sikkerhetsmeldinger og andre oppdateringer om nye måter man kan bli svindlet på fra firmaet han har antivirusprogram fra.

Et annet sentralt område der flere endret praksis, var deling av personlig informasjon. Mann 55 år valgte for eksempel å avregistrere seg fra kundeklubber for å unngå svindelforsøk derfra, og hadde blitt langt mer kritisk til brukeravtaler og alle tjenester og steder der han må lage brukernavn og passord. Også mann 37 år beskrev hvordan han nå nøye vurderer hvor og når han gir fra seg informasjon:

> Jeg bruker absolutt tid og prøver å være seriøs og tar litt mer ansvar når jeg ser at jeg har vært raus og litt lat. Jeg glemmer ikke det her. Jeg har gjort sånn at hvis jeg logger meg inn på skatteetaten da for eksempel, og så man godkjenne. Da leser jeg veldig nøye, faktisk, før jeg trykker på noe. Jeg tar heller det ekstra sekundet enn å bare gjøre det for å gjøre det (Mann 37 år)

Grunnen til at han gjorde slike endringer, skyldes blant annet at han, som nevnt tidligere, føler seg overvåket, ikke stoler på tilværelsen sin på digitale enheter, og føler at han ikke er sikret når det kommer til digitalisering. I likhet med dette finner Button & Brooks (2009) og Dove (2021, s. 40-41) at man ofte gjør endringer fordi man har mistet troen på andre eller har endret sin oppfatning av verden.

Samlet sett samsvarer disse endringene med funnene til Button & Brooks (2009), Ngo mfl. (2020), Reyns mfl. (2016), og Jansen & Leukfeldt (2018), som viser at ofre ofte er mer forsiktige på nett etter hendelsen. Endringene kan forstås som en form for problemfokusert mestring (Lazarus & Folkman, 1984), der informantene forsøker å gjenvinne kontroll gjennom konkrete tiltak som skal redusere risiko og beskytte dem mot nye svindelforsøk. Samtidig kan endringene tolkes som et uttrykk for en økning i digital kapital (Park, 2017). Dette handler ikke bare om digitale ferdigheter, men om evnen til å navigere mer reflektert, kritisk og strategisk i et digitalt landskap preget av økt kompleksitet og usikkerhet.

Likevel må det understrekes at slike endringer ikke nødvendigvis er varige. Enkelte informanter, som kvinne 76 år og kvinne 85 år, fortalte at de i en periode etter svindelen ble mer forsiktige, men at de gradvis vendte tilbake til gamle rutiner, selv om de opplevde å ha blitt mer bevisste. Kvinne 61 år uttrykte at hun ikke hadde gjort konkrete endringer, men at

hun var mer oppmerksom i møte med digitale henvendelser. Gutt 18 år fortalte også at han er mer obs, men at det i praksis ikke har påvirket hvordan han bruker digitale tjenester. Dette samsvarer med funnene til Jansen & Leukfeldt (2018), hvor mange innførte endringer rett etter hendelsen, men over tid falt tilbake til tidligere praksis. Endringene fremstår dermed som delvis midlertidige og situasjonsbetingede, et uttrykk for en reaksjon mer enn en varig transformasjon.

6.4 Sammenfatning av funnene og oppsummerende refleksjoner

Funnene viser at konsekvensene var sammensatte og berørte flere sider av livet, både praktiske, psykiske, emosjonelle, sosiale og digitale, og at det var mange likheter mellom informantene når det gjelder hvordan de opplevde disse. Både eldre og yngre informanter opplevde ekstraarbeid knyttet til å få tilbake pengene de hadde mistet, og understreket hvor viktig det var å få tilbake pengene, og hvordan dette reduserte de økonomiske konsekvensene på lang sikt. De fleste mente at situasjonen ville vært verre hvis de hadde hatt en svakere økonomisk situasjon. En forskjell var at eldre generelt mistet større beløp (20 000-50 000 kroner), mens yngre informanter ofte mistet mindre summer (2000-8000 kroner).

Samtidig ble det tydelig at det økonomiske tapet i seg selv sjelden ble opplevd som den største belastningen. Det var oftest de emosjonelle reaksjonene som ble stående sterkest i etterkant: følelsen av å ha blitt lurt, skam, og en usikkerhet knyttet til egen dømmekraft. Dette gjaldt begge aldersgrupper. En forskjell var likevel at yngre i større grad mistet tilliten til digitale tjenester, mens eldre oftere aksepterte hendelsen og betraktet den som en erfaring de kunne lære av. Svindel ble dermed ikke bare opplevd som et økonomisk tap, men som en personlig krise som berørte tillit og selvforståelse.

Møtet med omgivelsene var en sentral del av mestringsprosessen for alle informantene. Både eldre og yngre uttrykte et behov for å bli hørt, trodd og tatt på alvor, både av hjelpetjenester og nærstående. Noen opplevde god støtte, spesielt fra familie og venner, mens andre følte seg alene og måtte kjempe for å bli tatt seriøst, særlig i møte med politi og banker. Eldre informanter beskrev større utfordringer med digitale løsninger, følte seg mer hjelpeløse og var mer avhengig av personlig oppmøte og bistand fra banken. Yngre håndterte systemene lettere, tok raskt i bruk digitale løsninger, og tok i større grad ansvar selv. Samtidig hadde eldre høyere forventninger til støtte fra institusjonene, og uttrykte oftere misnøye, særlig overfor politiet, mens yngre i større grad viste forståelse for begrensede ressurser. Ulike

forventninger til hjelp og ulik teknologisk kompetanse kan derfor delvis forklare forskjellene i hvordan de ulike aldersgruppene håndterte situasjonen.

Etter hendelsen fikk både eldre og yngre en økt bevissthet rundt digital risiko, og ble mer skeptiske og forsiktige i møte med digitale tjenester. Eldre gjennomførte oftere konkrete tiltak som å sperre kort, redusere midler på konto eller stenge for lån og kreditt. Yngre fokuserte i større grad på digitale vaner, som å være mer kritiske til registreringer og gjennomgå vilkår og brukeravtaler mer grundig.

Samlet viser funnene at det å bli utsatt for svindel utløste en kompleks mestringsprosess, der informantene benyttet en kombinasjon av problemfokuserte og emosjonsfokuserte mestringsstrategier (Lazarus & Folkman, 1984). Denne prosessen innebar både praktiske tiltak, emosjonell bearbeiding, atferdsendringer, og en fortolkende, narrativ bearbeiding av hendelsen. Til sammen viser dette at det å bli svindlet ikke bare handler om et enkelt svik i et digitalt møte, men om en hendelse som setter i gang en rekke reaksjoner, handlinger og refleksjoner. Informantenes fortellinger vitner om motstandskraft, læring, og en sterk vilje til å gjenvinne kontroll og ta grep i egen situasjon.

7 Diskusjon og implikasjoner

I dette kapittelet vil jeg trekke fram noen av analysens hovedfunn og diskutere disse i lys av de valgte teoretiske perspektivene og tidligere forskning. Dette bidrar til å se på teorienes anvendbarhet i konteksten av mine data, altså hvordan funnene mine støtter eller utfordrer disse teoriene. Først diskuterer jeg hvordan det å bli utsatt for digital svindel kan skape en spesiell offeropplevelse som går utover økonomiske tap, og som berører eksistensielle dimensjoner som tillit, selvbilde og kontroll. Jeg ser videre på hvordan slike erfaringer ofte overses eller bagatelliseres av hjelpetjenester. Med utgangspunkt i Christies teori om det «ideelle offeret» diskuterer jeg hvordan ofre for digital svindel ofte faller utenfor samfunnets oppfatninger av hvem som fortjener sympati og anerkjennelse. Deretter belyser jeg hvordan informantene utfordrer stereotype oppfatninger om hvem som er sårbare for digital svindel, og hvordan dagens digitale kontekst gjør at det er behov for en videreutvikling av Christies teori. Til slutt retter jeg blikket fremover og diskuterer behovet for bedre håndtering og forebygging av digital svindel, og hvem sitt ansvar det er, særlig i møte med nye utfordringer knyttet til teknologisk utvikling og fremveksten av kunstig intelligens.

7.1 En annerledes offeropplevelse?

Som vist i analysen, opplevde informantene en rekke konsekvenser som følge av svindelen. Dette inkluderte alt fra økonomiske tap og sterke emosjonelle reaksjoner, til endringer i bruk av digitale enheter. Av disse var det særlig de psykiske og emosjonelle konsekvensene som påvirket dem mest. De beskrev hvordan det ikke bare handlet om å føle seg dum eller lettlurt, men at det hadde mer eksistensielle konsekvenser som at man mistet tillit til andre, at de fikk et negativt syn på seg selv og følte at de hadde mistet kontroll. Flere ble også svindlet hjemme, hvor de var avslappet og ikke hadde «garden oppe». I motsetning til dette har man ofte garden mer oppe ute på gata, fordi man har forventninger om at for eksempel lommeboken kan bli stjålet. Når man er hjemme, i en privat, trygg ramme har man ikke nødvendigvis de samme forventningene, og kan derfor oppleve å bli «tatt på senga» i dobbelt forstand. Kvinne 73 år illustrerte dette ved å beskrive det som skjedde som et slags innbrudd i hennes private sfære. Informantenes erfaringer viser dermed hvordan det å bli utsatt for digital svindel kan ha dyptgripende personlige konsekvenser, som er langt mer alvorlige og omfattende enn det ser ut som ved første øyekast.

Flere av informantenes beskrivelser kan forstås som et uttrykk for at svindelen utgjorde et slags brudd i livsfortellingen deres, en «narrative rupture», som krevde en aktiv prosess for å gjenopprette mening og selvforståelse (Pemberton mfl., 2019b, s. 411). Flere benyttet derfor en rekke emosjonsfokuserte og problemfokuserte mestringsstrategier (Lazarus & Folkman, 1984) for å håndtere det de opplevde. Av disse var det særlig de emosjonsfokuserte mestringsstrategiene som var mest fremtredende. De tok blant annet kontakt med flere hjelpetjenester, men også familie og venner. Mens de mottok støttende og medfølende reaksjoner fra familie og venner, var reaksjonene fra hjelpetjenestene de kontaktet annerledes. Selv om noen, som kvinne 61 år, kvinne 29 år og kvinne 82 år, fikk støtte og hjelp, var det likevel flere som opplevde liten interesse, mangel på anerkjennelse og å ikke bli tatt på alvor. Kvinne 41 år opplevde for eksempel at hun måtte jobbe hardt for å bli hørt, mens mann 37 år fikk vite at hvis det skjedde igjen ville de ikke hjelpe han. Slike reaksjoner kan ha ført til sekundærviktimisering for informantene, noe som også har blitt vist i tidligere forskning (se for eksempel Cross mfl., 2016).

Ser man på disse erfaringene i lys av Christies teori om det «ideelle offeret», kan en mulig forklaring på hvorfor flere informanter opplevde slike reaksjoner, være at ofre for digital svindel ofte ikke passer inn i samfunnets forestilling om hvem som fortjener sympati. Ifølge

Christie (1986) kjennetegnes det ideelle offeret av å være uskyldig, moralsk uklanderlig og ute av stand til å gjøre noe annerledes i situasjonen. I motsetning til dette blir ofre for digital svindel ofte sett på som delvis ansvarlig, nettopp fordi de har utført en handling, for eksempel oppgitt informasjon, klikket på en lenke eller godkjent en transaksjon. Selv om disse handlingene skjer under manipulasjon og press, bryter de med ideen om offeret som helt passivt. Dette skiller dem fra ofre for mer tradisjonelle kriminalitetstyper som vold, overgrep eller tyveri, hvor ansvaret i større grad umiddelbart plasseres hos gjerningspersonen, og hvor offeret sjeldnere blir stilt spørsmål ved. Man stiller for eksempel sjelden spørsmål ved offerstatusen til noen som har blitt frastjålet verdier fra et ulåst hus, selv om de kunne ha låst døren. I digitale kontekster oppleves derimot tilsvarende handlinger, som å trykke på en lenke eller dele informasjon, ofte som bevis på at man selv har skylden. Det er dermed ikke nødvendigvis de faktiske konsekvensene man opplever som avgjør om en person blir møtt med støtte, men i hvilken grad samfunnet oppfatter at offeret «kunne ha unngått» situasjonen. Dette ble også tydelig i Cross (2018a), hvor flere informanter, til tross for at de passet til noen av Christies karakteristikker om hva som utgjør et ideelt offer, ble møtt med skepsis fordi deres egne handlinger, og stedet lovbruddet skjedde, gjorde at de brøt med idealbildet. På grunn av dette hadde de også negative opplevelser i møte med hjelpetjenestene.

Videre reflekterte flere av mine informanter også selvkritisk over sin egen rolle i svindelen. Noen, som kvinne 29 år, mann 55 år og mann 68 år, beskrev seg som godtroende og lettlurte. De følte på skyld for å ha blitt lurt, og plasserte til en viss grad ansvaret hos seg selv, til tross for at svindelen var svært sofistikert gjennomført. Dette kan forstås i lys av en utbredt samfunnsholdning om at digital svindel er noe man burde klare å unngå, særlig i en tid der informasjon om svindelmetoder er allment tilgjengelig. Det å bli lurt digitalt fremstår dermed ikke bare som et tegn på å ha blitt utsatt for kriminalitet, men også som et uttrykk for manglende dømmekraft, kritisk sans eller teknologisk forståelse. Denne indre dialogen var særlig tydelig hos kvinne 29 år og gutt 18 år, som begge uttrykte undring over hvordan de kunne «la det skje». Her ser man hvordan den ytre mistroen mange ofre for digital svindel ofte møtes med, også kan bli internalisert. Dette skaper en form for selvbebreidelse som skiller seg fra det som ofte preger ofre for tradisjonell kriminalitet, hvor offerrollen kanskje i større grad anerkjennes uten at det reises spørsmål ved egen rolle. Noen av informantene hadde også vansker med å se seg selv som «ekte» ofre, nettopp fordi de selv hadde vært involvert i deler av forløpet. Samtidig ble dette delvis dempet av støttende reaksjoner fra familie og venner, som forsto at svindlerne hadde brukt svært profesjonelle metoder og

understreket at informantene hadde handlet i god tro. Slike reaksjoner fra omgivelsene kan bidra til å styrke følelsen av uskyld hos dem som er rammet, og gjøre det lettere å forstå dem som «ekte» ofre, selv om situasjonen deres ikke fullt ut passer inn i Christies idealbilde.

7.1.1 Når virkeligheten utfordrer bildet av det «ideelle» offeret

Som vist ovenfor, hadde flere informanter en slags indre kamp med skyldfølelse og tvil om egen offerstatus. Det som likevel er interessant, er at mange samtidig aktivt utfordret stereotypier om hvem som blir svindlet, og hvordan. Dette gjaldt for eksempel kvinne 73 år som over tid tok tydelig avstand fra ideen om at hun var lettlurt. Hun mente at svindleren trolig hadde bygget på et feilaktig, stereotypisk samfunnsbilde av den «typiske eldre», som ensom, lite teknologisk kompetent og dermed lett å lure. Dette var et bilde hun ikke kjente seg igjen i og ønsket å utfordre. I lys av Scott & Lymans (1968) begrep «accounts», kan dette sees som en måte å gjenvinne kontroll og beskytte selvbildet etter en belastende opplevelse.

Også flere yngre informanter, som kvinne 29 år og gutt 18 år, reflekterte over slike stereotypier. De hadde selv hatt et bilde av eldre som typiske ofre for digital svindel, nettopp fordi de ofte hadde hørt at slike hendelser rammet personer med lav digital kompetanse. Samtidig viser informantens erfaringer at dette bildet ikke alltid stemmer. Selv om yngre forventes å ha høy digital kapital som skal beskytte dem mot svindel, ble de likevel rammet. Dette utfordrer ideen om at teknologisk kompetanse automatisk gir beskyttelse. Ser man disse funnene opp mot det digitale skillet, er det interessant hvordan både kvinne 73 år og disse to yngre informantene på en måte «møter seg selv i døra» hele tiden. De erfarte at virkeligheten ikke stemte overens med egne eller andres forventninger. Det oppstår med andre ord et interessant spenn mellom samfunnets forestillinger om hvem som er mest sårbare, og det som faktisk skjer.

I tråd med dette fremhevet flere informanter, både yngre og eldre, at de hadde tatt forholdsregler, vært kritiske og vurdert situasjonene nøye, men likevel blitt svindlet. Dette gjaldt blant annet mann 55 år, kvinne 61 år, mann 68 år, og kvinne 76 år. Deres erfaringer nyanserer forestillingen om at digital sårbarhet først og fremst handler om alder. Funnene viser at det ikke nødvendigvis er noen klar sammenheng mellom alder og digital kompetanse, da både yngre og eldre med god digital kompetanse kan bli lurt. Dette peker mot et mer komplekst bilde av hvem som faktisk er mest utsatt. Det er ikke slik at eldre automatisk er mer sårbare, eller at yngre nødvendigvis er beskyttet. Hva som gjør noen mottakelige for

svindel handler i større grad om den konkrete situasjonen de befinner seg i, for eksempel et øyeblikk preget av tillit eller lav årvåkenhet. Det er altså ikke hvem man er, men når og hvordan man møtes av svindelen, som avgjør hvor sårbar man er.

Disse nyansene i hvem som faktisk rammes, står i kontrast til samfunnets forventninger om hvem som burde være sårbare. Nettopp fordi teknologisk kompetanse er så tett knyttet til alder, kan det oppleves mer overraskende når en ung og digitalt erfaren person, som kvinne 29 år, blir utsatt for svindel. Når yngre ofre, som gutt 18 år og kvinne 29 år, ikke passer inn i forestillingen om det «ideelle» offeret, kan de også oppleve mindre sympati og forståelse. Et tydelig eksempel på dette var forskjellen i hvordan mann 37 år og kvinne 85 år ble møtt av hjelpetjenestene. Mann 37 år fikk beskjed om at dersom noe lignende skjedde igjen, ville han ikke få hjelp. Kvinne 85 år, derimot, ble møtt med forståelse og bekreftelse på at det ikke var hennes feil. Denne kontrasten illustrerer hvordan kulturelle ideer om hvem som fortjener sympati, og hvem som burde «visst bedre», fortsatt preger hvordan svindelofre blir møtt. Dette samsvarer også med Christies (1986) poeng om at offerstatus ikke bare er noe man har, men noe man må tilkjennes, og det skjer ofte i lys av samfunnets normer og forventninger (Nielsen & Snare, 1998, s. 30-31).

7.1.2 Det ideelle offeret i en digital tid

Funnene som er presentert og diskutert over viser, som påpekt av Dove (2021, s. 67), at sårbarhet for digital svindel ikke kan forstås utelukkende gjennom alder, men heller bør sees som et samspill mellom flere faktorer, som livssituasjon, emosjonell tilstand og digital atferd. Denne innsikten støttes også av nyere forskning, som viser at cybertrusler, som digital svindel, ikke er begrenset til bestemte aldersgrupper (Ranchordas & Beck, 2025, s. 510).

Denne bredden i hvem som rammes henger tett sammen med hvordan hverdagen har blitt stadig mer digitalisert. I dag foregår en stor del av dagliglivet på nett, alt fra å betale regninger til å kommunisere med offentlige instanser og holde kontakt med familie og venner. Mobilen er alltid med, og skillet mellom jobb og fritid, privat og offentlig, er i stor grad visket ut. Det forventes at man er tilgjengelig og handler raskt, og digitale henvendelser fremstår ofte som troverdige. I dette landskapet har det vokst frem en ny type sårbarhet, en som ikke handler om fysisk svakhet, men om å være tilgjengelig i feil øyeblikk. Den digitale hverdagen gjør at risikoen for svindel er konstant til stede, og det å bli «tatt på senga» har fått en ny betydning. Selv om svindel ikke er nytt, har den digitale infrastrukturen gjort

spredningen langt større og mer uforutsigbar enn før, og det er lettere å treffe noen som er distraherte eller i visse øyeblikk har «garden nede», slik man også så hos flere av mine informanter.

Disse endringene i hvordan og hvorfor folk svindles, utfordrer ikke bare etablerte forestillinger om hvem som er «typiske ofre», men avdekker også teoretiske begrensninger ved Christies (1986) teori om det «ideelle offeret». Ifølge Christie (1986) kjennetegnes det ideelle offeret av å være svakt, uskyldig og moralsk uklanderlig, og å ha blitt utsatt for kriminalitet av en sterk og ond gjerningsperson. Det legges også vekt på at offeret ikke kunne ha gjort noe annerledes. Dette bildet harmonerer dårlig med virkeligheten til mine informanter. Mange av dem ble riktignok manipulert på en aggressiv og kynisk måte, men i motsetning til Christies idealbilde, fantes det ofte en viss grad av medvirkning, for eksempel at de selv hadde oppgitt informasjon. I et digitalt landskap, hvor svindel forutsetter at offeret handler, for eksempel klikker, svarer eller overfører, er det vanskeligere å oppfylle kravet om moralsk uklanderlighet.

Selv om teorien fortsatt har analytisk verdi, fremstår det i lys av funnene som nødvendig å videreutvikle Christies teori for at den skal kunne anvendes på digitale kontekster og digital kriminalitet. Hva som regnes som et ideelt offer er ikke statisk, men historisk og kontekstuelt betinget. Det er derfor viktig at ideelle offeret alltid speiler samtiden. I dagens digitale samfunn innebærer dette at forståelsen av både sårbarhet og ansvar må speile en virkelighet preget av teknologisk utvikling. I dag handler sårbarhet i mindre grad om fysisk svakhet, og mer om digital kapital, tillit og evne til å navigere komplekse nettmiljøer. Svindlere opererer i grenselandet mellom det tekniske og det sosiale: De bruker avanserte digitale verktøy, samtidig som de bygger tillit ved å etterligne kjente aktører. Det er nettopp denne kombinasjonen av teknologisk og mellommenneskelig kompetanse som gjør dem så effektive, og ofrene så sårbare.

Basert på dette bør følgende punkter tas med i vurderingen av hvem som utgjør et ideelt offer i en digital tid: 1) Digital situasjonell sårbarhet: Offeret blir svindlet i en digital hverdagssituasjon der det er naturlig å være tillitsfull og handle raskt, for eksempel når man mottar en e-post eller melding fra det som fremstår som banken, myndigheter eller noen man kjenner. Det handler ikke om alder, men om øyeblikk hvor garden er nede. 2) Svindlerens doble kompetanse: Svindleren kombinerer teknisk kunnskap med sosial forståelse. Ved å mestre både digitale og sosiale mellommenneskelige koder klarer de å fremstå som

troverdige, noe som gjør det vanskelig for offeret å forstå at noe er galt før det er for sent. 3) Fravær av skyld i lys av digitale vaner: Offeret har handlet i tråd med normale og aksepterte digitale vaner. Å åpne en e-post fra en tilsynelatende legitim aktør er ikke uaktsomt, og offeret bør derfor ikke holdes ansvarlig for å ha blitt lurt. Gjennom disse punktene blir det tydelig hvordan det ikke nødvendigvis er mangel på digitale ferdigheter som gjør noen sårbare. Det er fullt mulig å være digitalt kompetent og likevel bli utsatt i visse situasjoner.

I tillegg til en teoretisk videreutvikling av Christies teori, peker funnene i denne oppgaven på et behov for en bredere forståelse av selve offerbegrepet i møte med digital kriminalitet. Samfunnet, medier og hjelpetjenester må forholde seg til en langt mer mangfoldig gruppe ofre enn det stereotypiene tilsier, og være bevisste på hvordan de møter personer som har blitt svindlet. Dersom offeret møtes med mistro, ansvarliggjøring eller mangel på forståelse, kan det forsterke følelser av skam og selvbebreidelse, og i verste fall hindre både gjenoppretting og forebygging.

I forlengelse av dette oppstår det et viktig spørsmål: Hvem har egentlig makten til å definere hva et «ekte» offer er? Det handler ikke bare om hva loven sier, men også om kulturelle forestillinger og hvordan ulike institusjoner operer i praksis. Når politiet eller banker vurderer at noen «burde ha visst bedre», flyttes ansvaret tilbake til den som er rammet. På den måten oppstår en form for institusjonalisert mistillit, der aktører med definisjonsmakt avgjør hvem som fortjener sympati, støtte og rettigheter. Anerkjennelsen av offerstatus blir dermed ikke bare et individuelt spørsmål, men uttrykk for en form for symbolsk maktutøvelse. Dette viser behovet for et mer nyansert språk når man snakker om ofre for digital kriminalitet. I stedet for å vurdere dem ut ifra forenklede forestillinger om hva de «burde ha forstått» eller «unngått», må man i større grad ta hensyn til intensjonene bak handlingene, situasjonen de var i, og hvordan sårbarhet kan oppstå i bestemte øyeblikk. Det å bli anerkjent som offer bør ikke være noe man må kjempe for, da det er viktig å bli anerkjent for å få nødvendig støtte og hjelp til å komme seg videre (Cross, 2018a, s. 259).

7.2 Bedre håndtering av digital svindel – et delt ansvar?

Flere av informantene mine hadde negative opplevelser med politi og banker. De opplevde at sakene deres ble henlagt eller at det ble vist liten interesse for situasjonen deres. Selv om noen, som gutt 18 år og kvinne 41 år, hadde forståelse for dette, fordi de var klar over at politiet har begrensede ressurser til å bruke på slike saker, mente de likevel at de burde ha vært mer interessert og fått flere ressurser for å bekjempe svindel. Det samme har blitt vist

blant ofre i andre land. Cross (2018c, s. 10-11) viser for eksempel at ofre for digital svindel i Australia etterlyser bedre støtteordninger og mer åpenhet rundt hvordan sakene deres håndteres, for å unngå gjentatt viktimisering. Dette kan skyldes at politiet i Australia, som i Norge, ofte prioriterer tradisjonelle kriminalitetstyper fremfor cyberkriminalitet på grunn av lav rapportering, og manglende ressurser og kompetanse til å etterforske svindel (Cross, 2019, s. 121-123).

Som en respons på slike utfordringer har det i flere land blitt etablert sentraliserte rapporterings- og støtteordninger for svindelofre. Eksempler inkluderer Actionfraud i Storbritannia, ScamWatch og ACORN (Australian Cybercrime Online Reporting Network) i Australia og The Canadian Anti-Fraud Centre i Canada (Cross, 2019, s. 121-123). Disse forenkler rapporteringsprosesser, forbedrer informasjonsdelingen mellom ofre, politi og andre relevante aktører, og forenkler problemer knyttet til jurisdiksjon (Cross, 2018c, s. 2). Internasjonalt blir det vist at slike sentraliserte rapporteringsaktører kan gjøre det lettere for ofre å få hjelp (Cross, 2020b, s. 371-373). Likevel må det påpekes at slike aktører ikke alltid har myndighet til å gjøre det ofre forventer, noe som i seg selv kan skape nye frustrasjoner (Cross, 2018c, s. 5-6; Cross 2020b, s. 358)

Også i Norge har det de senere årene blitt igangsatt tiltak. I 2023 etablerte Nasjonal kommunikasjonsmyndighet (NKOM) og Økokrim en nasjonal ekspertgruppe for å forhindre svindel. Initiativet har fått internasjonal oppmerksomhet og ledet til opprettelsen av GIRAF (Global Informal Regulatory Antifraud Forum), hvor 21 land nå deltar (NKOM, 2024). Et annet eksempel er ID-juristen, et rettshjelptiltak som ble opprettet som en del av forskningsprosjektet SODI (Samfunnssikkerhet og digitale identiteter), med mål om å gi gratis juridisk hjelp til personer som har opplevd svindel. Tiltaket ble opprettet som en respons på at svindelofre, særlig i saker med misbruk av BankID, opplevde at banker avviste erstatningskrav basert på små endringer i svindelmetodene. Dette synliggjør hvordan rettslige gråsoner utnyttes, og hvordan svindel ofte utvikler seg raskere enn lovverket (Pileberg, 2024). ID-juristen er imidlertid nå avviklet, noe som igjen synliggjør behovet for varige og stabile hjelpetjenester.

I tillegg til slike formelle tiltak, spiller også mediene en viktig rolle i arbeidet med å forebygge digital svindel. Oppslag om svindel kan gjøre folk oppmerksomme på at slike hendelser skjer, og dermed fungere både som advarsel og som informasjon. Flere informanter, som kvinne 61 år og dame 29 år, fortalte at de hadde lært mye om svindel og

hvordan det foregår gjennom medieoppslag. Mediene har derfor et stort potensiale som folkeopplysende aktør, ved å spre kunnskap på en tilgjengelig og virkelighetsnær måte. De kan for eksempel bidra til å synliggjøre hjelpetjenester som Forbrukerrådet, som har utviklet digitale guider og verktøy for å hjelpe folk med å forstå og håndtere ulike typer digital svindel (Forbrukerrådet, u.å.). Et interessant funn i denne sammenhengen var nemlig at ingen av mine informanter hadde benyttet slike selvhjelpsressurser. Dette kan tyde på at flere ikke vet hvor man kan henvende seg for å få hjelp. I slike tilfeller kan mediene bidra til å bygge bro mellom personlige erfaringer og eksisterende støtteapparater, samtidig som økt synlighet kan senke terskelen for å søke hjelp, fordi svindel kan oppleves som mindre tabubelagt når det snakkes åpent om. Junger mfl. (2023, s. 1) bekrefter også at det trengs en mer proaktiv tilnærming for å informere offentligheten om svindel og svindelmetoder, slik at potensielle ofre har kunnskap om svindel før de møter på det, og for eksempel forstår at seriøse aktører aldri etterspør passord eller BankID over telefon.

Til tross for at flere tiltak er på plass, er det også viktig å sikre at de allerede eksisterende hjelpetjenestene, som politi og banker, som ofte er de første ofre tar kontakt med, styrkes, for eksempel ved å omprioritere ressurser for å forbedre håndteringen av digital svindel. Cross (2019, s. 121-123) påpeker at økt opplæring og støtte til politiet er avgjørende for å integrere etterforskning av digital svindel som en naturlig del av politiarbeidet. Mann 55 år og gutt 18 år uttrykte et tydelig ønske om at politiet burde vise større interesse og faktisk prøve å finne ut hvem som står bak. Mann 55 år la til at selv om det kan dreie seg om småbeløp for enkeltpersoner, kan summene bli betydelige når svindlere sender ut tusenvis av svindelforsøk. Dette illustrerer hvordan digital svindel samlet sett kan få store samfunnsøkonomiske konsekvenser, og hvorfor det er i både offentlige og private institusjoners interesse å forebygge slike hendelser, også når det gjelder enkeltsaker.

I forlengelse av dette bør det også rettes oppmerksomhet mot forebyggende tiltak i forkant av svindelen. Allerede i 2015 påpekte Politidirektoratet (2015, s. 119) behovet for sikre løsninger for elektronisk ID, og en tydeligere regulering av hvordan digital identitet utstedes, verifiseres og eventuelt oppheves. Siden den gang har Norge innført flere grep, blant annet gjennom implementeringen av eIDAS-forordningen, som er forkortelsen for forordning om «elektronisk identifisering og tillitstjenester for elektroniske transaksjoner i det indre marked». Formålet med eIDAS-forordningen er å sikre et velfungerende marked og oppnå et passende sikkerhetsnivå for elektronisk identifikasjon og tillitstjenester (Nkom, 2020). I

tillegg har det blitt etablert ulike eID-løsninger som BankID, Buypass og MinID, som gjør det mulig å bekrefte identitet på en sikker måte i digitale tjenester (Nkom, 2025). Likevel viser funnene i denne studien at slike tiltak ikke alltid gir tilstrekkelig beskyttelse i praksis. Kvinne 85 år uttrykte for eksempel frustrasjon over at det hadde vært mulig å ta opp et stort lån i hennes navn, uten at banken reagerte. Hun mente at det burde ha vært systemer på plass som fanget opp slike uvanligheter, som at eldre personer sjelden tar opp så store lån. Dette illustrerer at selv om regelverket er på plass, kan manglende oppfølging og risikovurdering i praksis føre til at slike hendelser likevel skjer. Det peker på et behov for å styrke både de tekniske systemene og institusjonelle rutinene, særlig for å beskytte de mest sårbare.

Selv om institusjoner har et klart ansvar, er det også relevant å diskutere hvorvidt enkeltindivider har et ansvar i møte med digital svindel. NorSIS (2023) understreker for eksempel at alle bør ta visse grunnleggende forholdsregler, som å bruke sterke passord og totrinnspålogging, oppdatere programvare jevnlig, sikkerhetskopiere data, og være skeptiske til lenker og uventede henvendelser. Likevel må man ikke glemme at det kan være vanskelig for visse grupper å etterleve slike anbefalinger i praksis. Kvinne 61 år og mann 68 år påpekte at mange eldre, spesielt de med kognitiv svikt eller lav digital kompetanse, kan ha utfordringer med å forstå og anvende slike råd i hverdagen. Dermed blir det tydelig at ansvarsfordelingen ikke er så enkel som ofte fremstilt. Når tiltakene forutsetter et visst nivå av digital kompetanse, risikerer man å skyve ansvaret over på dem som allerede er mest utsatt. Dette skaper et dilemma: Hvordan kan man stille krav om individuell årvåkenhet, uten samtidig å overse de strukturelle ulikhetene i befolkningens evne til å følge slike råd? Dove (2021, s. 120) nyanserer bildet ytterligere ved å understreke at svindlere som regel vil være smartere og mer utspekulerte enn det kan man forestille seg, og at selv digitale brukere med høy kompetanse kan bli lurt.

Til sammen understreker dette behovet for en felles innsats for å forebygge svindel, der både offentlige institusjoner, medier og enkeltpersoner har en viktig rolle. Det krever tydeligere strukturelle tiltak, mer tilpasset informasjon, og individuell årvåkenhet, men også et støtteapparat som tar høyde for ulikheter i digital kompetanse og livssituasjoner.

7.2.1 Svindel med kunstig intelligens: en voksende utfordring

Selv om flere av mine informanter uttrykte et tydelig behov for bedre håndtering og forebygging av digital svindel, understreket de samtidig at dette kan bli mer utfordrende i fremtiden. Mann 68 år uttrykte for eksempel at det er vanskelig å forutsi fremtidig svindel, og

at vi trolig vil møte nye trusler, som kunstig intelligens, samt ting vi i dag ikke engang kan forestille oss. Mann 55 år uttrykte lignende bekymringer, og mente at det kan bli vanskelig å ha full kontroll på hva som er svindel og ikke. I forbindelse med dette trakk sønnen til kvinne 73 år frem at det kan være vanskelig å oppdage svindel, fordi svindlere for eksempel kan bruke stemmeprøver for å etterligne andre. Dette understrekes også i tidligere forskning hvor det blir vist at svindel vil fortsette å endre seg etter hvert som teknologier fortsetter å utvikle seg (Wall, 2007, s. 155). I tillegg påpeker Finanstilsynet (2024) at ny teknologi, særlig kunstig intelligens, har utvidet handlingsrommet for kriminelle, som nå kontinuerlig utvikler, forbedrer og automatiserer svindelmetodene sine i høyt tempo. Svindlere gjør innholdet stadig mer overbevisende, blant annet gjennom forbedret språk, stemmeforfalskning (NSM, 2023), og bruk av deepfake-teknologi til å lage realistiske videoer og lydopptak som etterligner personer man har tillit til (Akademikerne Pluss, u.å.). Denne utviklingen øker risikoen for at også kritiske og årvåkne personer kan bli lurt i et svakt øyeblikk. Samtidig muliggjør kunstig intelligens at kriminelle kan gjennomføre et stort antall svindelforsøk samtidig, ved hjelp av KI-drevne chatboter som simulerer menneskelige samtaler og tilpasser seg offerets svar. KI brukes også til å analysere store datamengder for å skreddersy phishing-angrep retter mot enkeltpersoner, samt til å opprette falske nettbutikker som ser svært troverdige ut (Akademikerne Pluss, u.å).

Denne utviklingen illustrer hvordan digital svindel blir enda mer profesjonalisert, og NSM (2024, s. 30) advarer derfor om at rekkevidden av KI-verktøy er vanskelig å overskue og ha kontroll på. I tråd med dette påpeker Politiet (2025, s. 48-49) at KI fungerer som en forsterkende aktør som effektiviserer sosial manipulering, og gjør det vanskeligere å oppdage og forhindre svindel, både på individnivå og samfunnsnivå. På bakgrunn av dette har Finanstilsynet (2024) understreket behovet for tettere samarbeid mellom banker, ulike tjenestetilbydere, foretak og myndigheter for å møte utfordringen. For å imøtekomme dette behovet har flere myndigheter, inkludert Nasjonal kommunikasjonsmyndighet, Økokrim og Finans Norge, som nevnt tidligere, etablert GIRAF, en nasjonal ekspertgruppe for å forhindre svindel, særlig via telefon og SMS (Nkom, 2024).

I tillegg til at kunstig intelligens kan skape utfordringer og vanskeligheter for rettshåndhevende aktører, skaper det også utfordringer at svindel skjer på nett, fordi svindleren får en rekke fordeler (Yar & Steinmetz, 2019, s. 142). Selv når en svindel har blitt oppdaget, kan det være svært vanskelig å identifisere den eller de ansvarlige. Sporene kan for

eksempel føre til en uskyldig tredjepart med en stjålet identitet, eller det kan være umulig å spore opp svindleren bak aliaser og falske identiteter. I tillegg bruker svindlere i økende grad krypterte nettverk for å utføre svindel og distribuere stjålet informasjon (Yar & Steinmetz, 2019, s. 143; Button & Cross, 2017, s. 85). I lys av dette kan det stilles spørsmål ved om politiets arbeid i større grad bør preges av fleksibilitet og evne til å tenke utenfor etablerte rammer, særlig fordi svindelmetoder stadig utvikler seg, og utfordrer tradisjonelle måter å forstå og etterforske kriminalitet.

Til tross for slike utfordringer kan kunstig intelligens, særlig i form av maskinlæring, også brukes til forebygging. Maskinlæring kan oppdage unormal atferd, identifisere mønstre og forutsi svindel med høy nøyaktighet (Financial Crime Academy, 2025; Bello & Olufemi, 2024, s. 1505-1506). Som understreket av det australske teknologiselskapet Niux, innebærer dette at svindel kan identifiseres gjennom analyse av historiske data og oppdagelse av avvik fra etablerte mønstre. Denne evnen er avgjørende for å gjenkjenne nye trusler og tilpasse seg nye metoder for svindel (Niux, u.å.).

8 Avslutning

I denne oppgaven har jeg undersøkt hvilke typer digital svindel eldre og yngre innbyggere i Norge har opplevd, og hvilke likheter og forskjeller det finnes i hvordan de forstår, forklarer og reagerer på slike hendelser. Funnene viser at aldersgruppene utsettes for ulike typer svindel. Mens eldre oftest ble svindlet via telefon og e-post, noen ganger kombinert med identitetstyveri, ble yngre derimot oftere utsatt via sosiale medier eller når de gjorde kjøp på nett. Disse variasjonene ble knyttet til deres digitale vaner og teknologibruk. Likevel ble begge grupper rammet av familiesvindel, noe som illustrerer at enkelte svindeltyper går på tvers av alder.

Videre ble sårbarhet for svindel forklart som et samspill mellom individuelle, sosiale og teknologiske forhold. Informantene trakk særlig frem svindlernes digitale kapital i form av evne til å skape tillit og manipulere som avgjørende. I tillegg la eldre ofte vekt på livshendelser og økonomi som risikofaktorer, mens yngre vektla hvordan svindelen passet perfekt inn i deres digitale hverdag. Samtidig uttrykte begge grupper at det også handlet om tilfeldigheter, og at svindel i prinsippet kan ramme alle. Dette peker mot en forståelse av sårbarhet som situasjonsbetinget og kontekstavhengig, og noe som ikke er begrenset til alder alene. Det illustrerer også hvordan digital svindel bør forstås som et sosioteknisk fenomen,

der både teknologiske strukturer og menneskelige faktorer som emosjonell tilstand, tillit og digitale ferdigheter virker sammen og skaper rom for manipulering og risiko.

Konsekvensene av svindelen strakte seg langt utover økonomiske tap. Både eldre og yngre rapporterte emosjonelle og psykiske reaksjoner som skam, skyldfølelse og svekket selvbilde. Enkelte beskrev også en dyp følelse av mistillit og tap av kontroll. For å håndtere slike konsekvenser og selve hendelsen brukte informantene ulike emosjonsfokuserte og problemfokuserte mestringsstrategier. Disse inkluderte alt fra praktiske tiltak som å sperre kort eller endre digitale vaner, til emosjonell bearbeiding, refleksjon og søken etter sosial støtte. Den sosiale støtten de opplevde var varierende. Selv om mange fikk støtte fra familie og venner, hadde flere negative erfaringer med hjelpetjenester, særlig politi og banker. Her kom også aldersforskjeller til uttrykk: Eldre hadde høyere forventninger til bistand og uttrykte større frustrasjon over mange oppfølging fra hjelpetjenestene, mens yngre i større grad tok ansvar selv og viste forståelse for hjelpetjenestenes begrensninger.

Alt i alt viser funnene at det å bli utsatt for digital svindel kan få dype emosjonelle og eksistensielle følger, særlig når ofrene opplever å ikke bli tatt på alvor. Mange opplevde manglende anerkjennelse som ofre, særlig i møte med hjelpesystemet. Det ble vist at dette kan forstås i lys av Christies teori om det «ideelle offeret», som fortsatt former samfunnets og institusjoners oppfatninger av hvem som fortjener sympati. Ofre for digital svindel passer ofte ikke inn i dette idealet, og nettopp derfor argumenteres det for en videreutvikling av Christies teori for å bedre fange opp hva som kjennetegner ofre i en digital tidsalder. I en digital tid bør følgende punkter tas med i vurderingen av hvem som utgjør et ideelt offer: 1) digital situasjonell sårbarhet, der offeret rammes i en hverdagssituasjon der det er naturlig å være tillitsfull og handle raskt, 2) svindlerens doble kompetanse, som kombinerer teknologisk dyktighet med sosial manipulering, og gjør det vanskelig for ofre å oppdage svindelen, og 3) fravær av skyld hos offeret, som har handlet i tråd med vanlige digitale praksiser og derfor ikke kan klandres for å ha blitt lurt. Dette innebærer at både eldre og yngre kan være sårbare, ikke på grunn av manglende digitale ferdigheter eller alder, men på grunn av situasjoner der tillit og oppmerksomhet utnyttes.

Til slutt peker oppgaven på behovet for et delt ansvar i møtet med digital svindel. Individer må rustes til å håndtere risiko, for eksempel bli mer bevisste og endre sine digitale vaner. Samtidig har institusjoner også et tydelig ansvar for forebygging, støtte og oppfølging, samt å sikre bedre informasjonstilgang for hele befolkningen. Når svindelmetodene blir stadig mer

avanserte og sofistikerte, ofte drevet av kunstig intelligens, blir digital svindel ikke bare en teknologisk og juridisk utfordring, men et komplekst sosioteknisk fenomen som krever nytenkning rundt etablerte forestillinger om tillit, ansvar og hvem som kan regnes som et «ekte» offer.

8.1 Anbefalinger for videre forskning

Funnene i denne oppgaven peker på behovet for videre forskning som fokuserer på forebygging av digital svindel. Dette kan omfatte studier av hvordan hjelpetjenester forstår og håndterer slike saker, og hvordan deres praksis påvirkes av forestillinger om det «ideelle offeret». En slik tilnærming kan supplere perspektivet i denne oppgaven, som primært bygger på ofrenes perspektiv, ved å gi innsikt i hvorfor noen ofre ikke føler seg ivaretatt, samt bidra til forbedringer i praksis. Komparative analyser av rapporterings- og oppfølgingssystemer i ulike land, som ScamWatch i Australia og ActionFraud i Storbritannia, kan gi verdifulle perspektiver på hvordan norske støttesystemer kan styrkes. I lys av teknologisk utvikling er det også behov for forskning på hvordan kunstig intelligens, som deepfakes, stemmekloning og avanserte chatboter, endrer svindelens karakter og utfordrer eksisterende forebyggingsstrategier. Det bør også undersøkes hvordan ulike grupper opplever sin egen sårbarhet, og om kjønn eller andre demografiske faktorer påvirker risikoen for å bli rammet. En bredere forståelse av hva som gjør ulike grupper sårbare, kan bidra til mer målrettede og effektive forebyggende tiltak.

Samlet peker disse forskningsbehovene på at digital svindel må forstås som et komplekst, sammensatt og alvorlig samfunnsproblem, som krever tverrfaglig innsats.

Litteraturliste

Akademikerne Pluss (u.å.) *Svindel – Akademikere i økende grad utsatt.* Tilgjengelig fra: https://akademikernepluss.no/aktuelt/akademikere-utsatt-for-svindel/ (Hentet: 13.04.2025)

Akdemir, N. & Lawless, C. J. (2020) Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach, *Internet research*. 30(6), s. 1665-1687. DOI: 10.1108/INTR-10-2019-0400

Alvinus, A., Borglund, A. & Larsson, G. (2023) *Tematisk analys: din handbok till fascinerande vetenskap*. 1.utg. Lund: Studentlitteratur

Andenæs, A. (2000) Generalisering. Om ringvirkninger og gjenbruk av resultater fra en kvalitativ undersøkelse. i Haavind, H. (red.), *Kjønn og fortolkende metode: Metodiske muligheter i kvalitativ forskning.* Oslo: Gyldendal Akademisk

Bakken, S. A., Oksanen, A. & Demant, J. (2022) Capital in illegal online drug markets: How digital capital changes the cultural environment of drug dealing, *Theoretical criminology*, 27(3), s. 421-438. DOI: 10.1177/13624806221143365

Barton, C., Anderson, R., Levi, M., Böhme, R., van Eeten, M., Moore, T., Savage, S., & Clayton, R. (2013) Measuring the cost of cybercrime, i Böhme, R. (red.) *The economics of information security and privacy.* Heidelberg, Tyskland: Springer, s. 265-300. DOI 10.1007/978-3-642-39498-0 2013

Bello, O. A., & Olufemi, K. (2024) Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities, *Computer science & IT research journal*, *5*(6), 1505-1520. DOI: 10.51594/csitrj.v5i6.1252

Bigset, J. (2023) 18-åring svindlet for 48.000: - Jeg ble livredd, *Nettavisen*, 8.desember. Tilgjengelig fra: https://www.nettavisen.no/nyheter/18-aring-svindlet-for-48-000-jeg-ble-livredd/s/5-95-1507172 (Hentet: 16.02.2025)

Borwell, J., Jansen, J. & Stol, W. (2021) Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions, *Journal of digital social research*, 3(3), s. 85-110. DOI: 10.33621/jdsr.v3i3.66

Borwell, J., Jansen, J. & Stol, W. (2022) The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered Assumptions Theory, *Social science computer review*, 40(4), s. 933-954. DOI: 10.1177/0894439320983828

Bourdieu, P. (1986) The forms of capital, i Richardson, J. G. (red.) *Handbook of theory and research for the sociology of education*, s. 241-258. New York: Greenwood

Bourdieu, P. (2005) Principles of economic anthropology, i Smelser, N. J. & Swedberg, R. (red.) *The handbook of economic sociology*, 2.utg., s. 75–89. New York: Princeton University Press

Brataas, E. B., Stokke, M. S., & Svensson, A. (2022) *Rapport om misbruk av eID.* Tilgjengelig fra: https://www.jus.uio.no/ifp/forskning/prosjekter/sodi/publikasjoner/rapporter-mv/sodi-rapport-1-2022.pdf (Hentet: 11.01.2025)

Braun, V. & Clarke, V. (2006) Using thematic analysis in psychology, *Qualitative Research in Psychology*, 3(2), s. 77-101. DOI: 10.1191/1478088706qp063oa

Brown, S. (2006) The criminology of hybrids: Rethinking crime and law in technosocial networks, *Theoretical Criminology*, 10(2), s. 223-244. DOI: 10.1177/1362480606063140

Burton, A., Cooper, C., Dar, A., Mathews, L. & Tripathi, K. (2022) Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review, *Experimental gerontology*, vol. 1159. DOI: 10.1016/j.exger.2021.111678

Butler, R. P. (2013) Victims of cybercrime, i Davis, R. C., Lurigio, A. J. & Herman, S. (red.) *Victims of crime.* 4.utg. Los Angeles: Sage, s. 449-469.

Button, M. & Brooks, G. (2009) 'Mind the gap', progress towards developing anti-fraud culture strategies in UK central government bodies, *Journal of Financial Crime*. 16(3), s. 229–244. DOI: 10.1108/13590790910971784

Button, M. & Cross, C. (2017) *Cyber frauds, scams and their victims*. Abingdon, Oxon: Routledge

Button, M., Lewis, C. & Tapley, J. (2014a) Not a victimless crime: The impact of fraud on individual victims and their families, *Security Journal*, 27(1), s. 36–54. DOI: 10.1057/sj.2012.11

Button, M., Lewis, C., & Tapley, J. (2009a) *A better deal for fraud victims: research into victims' needs and experiences*. London: National Fraud Authority.

Button, M., Lewis, C., & Tapley, J. (2009b) *Support for the victims of fraud: an assessment of the current infrastructure in England and Wales*. London: National Fraud Authority.

Button, M., Nicholls, C. M., Kerr, J. & Owen. R. (2014b) Online frauds: learning from victims why they fall for these scams, *Australian & New Zealand journal of criminology*, 47(3), s. 391–408. DOI: 10.1177/0004865814521224

Button, M., Tapley, J. & Lewis, C. (2012) The 'fraud justice network' and the infrastructure of support for individual fraud victims in England and Wales, C*riminology and Criminal Justice*. 13(1) s. 37-61 DOI: 10.1177/1748895812448085

Carter, N. L., & Weber, J. M. (2010) Not pollyannas: Higher generalized trust predicts lie detection ability, *Social psychological & personality science*, 1(3), s. 274–279. DOI: 10.1177/1948550609360261

Christie, N. (1986) The Ideal Victim, i Fattah, E. A. (red.) *From Crime Policy to Victim Policy*. London: Palgrave Macmillan UK, s. 17–30. DOI: 10.1007/978-1-349-08305-3_2

Cross, C. (2015) No laughing matter: Blaming the victim of online fraud, *International review of victimology*, 21(2), s. 187-204 DOI: 10.1177/0269758015571471

Cross, C. (2016) 'They're very lonely': understanding the fraud victimisation of seniors, *International journal for crime, justice and social democracy*, 5(4), s. 60–75. DOI: 10.5204/ijcjsd.v5i4.268

Cross, C. (2018a) Denying victim status to online fraud victims: the challenges of being a 'non-ideal victim', i Duggan, M. (red.) *Revisiting the "Ideal Victim": Developments in Critical Victimology*. Storbritannia: Bristol University Press, s. 243–262. DOI: 10.51952/9781447339151.ch013

Cross, C. (2018b) Victims' motivations for reporting to the 'fraud justice network', *Police practice & research*, 19(6), s. 550–564. DOI: 10.1080/15614263.2018.1507891

Cross, C. (2018c) Expectations vs reality: Responding to online fraud across the fraud justice network, *International Journal of Law, Crime and Justice*, vol 55, s. 1–12. DOI: 10.1016/j.ijlcj.2018.08.001

Cross, C. (2019) Is online fraud just fraud? Examining the efficacy of the digital divide, *Journal of Criminological Research, Policy and Practice*, 5(2), s. 120–131. DOI: 10.1108/JCRPP-01-2019-0008

Cross, C. (2020a) Responding to individual fraud – perspectives of the fraud justice network, i Leukfeldt, E. R. & Holt, T. J. (red.) *The Human factor of cybercrime.* 1.utg. Abingdon, Oxon: Routledge, s. 359-388. DOI: 10.4324/9780429460593-16

Cross, C. (2020b) 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims, *Criminology & criminal justice*, 20(3), s. 358–375. DOI: 10.1177/1748895819835910

Cross, C. (2022) Meeting the Challenges of Fraud in a Digital World, i Gill, M. (red.) *The handbook of security*. Cham: Springer International Publishing, s. 217-238. DOI: 10.1007/978-3-030-91735-7_11

Cross, C., Richards, K. M. & Smith, R. (2016) The reporting experiences and support needs of victims of online fraud, *Trends and issues in crime and criminal justice*, (518), s. 1–14.

Daigle, L. E. & Muftic, L. R. (2016) *Victimology*. Los Angeles: Sage.

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L & Hardyns, W. (2020) Help, I need somebody: Examining the antecedents of social support seeking among

cybercrime victims, *Computers in human behavior*, vol. 108, s. 1-11. DOI: 10.1016/j.chb.2020.106310

Digitaliserings- og forvaltningsdepartementet (2024) *Fremtidens digitale Norge – Nasjonal digitaliseringsstrategi 2024-2030.* Tilgjengelig fra: https://www.regjeringen.no/no/tema/statlig-forvaltning/it-politikk/ny-nasjonal-digitaliseringsstrategi/id2982892/ (Hentet: 09.01.2025)

Dove, M. (2021) *The Psychology of Fraud, Persuasion and Scam Techniques: Understanding What Makes Us Vulnerable*. 1.utg. Oxford: Routledge. DOI: 10.4324/9781003015994

Eliassen, H. Ø. (2023) Agnete (20) ble svindlet for nærmere 170.000 kroner: - Svindlere opptrer stadig mer profesjonelt, *VG,* 19.august. Tilgjengelig fra: https://www.vg.no/nyheter/i/8J1KQW/oekning-i-svindelforsoek-i-norge-agnete-20-fra-frastjaalet-160-000-kroner (Hentet: 16.02.2025)

Emami, C., Smith, R. G., & Jorna, P. (2019) *Online fraud victimisation in Australia: Risks and protective factors.* AIC research Report 16. Canberra: Australian Institute of Criminology.

Europol (2023) *Online fraud schemes: a web of deceit.* Tilgjengelig fra: https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf (Hentet: 30.04.2025)

Financial Crime Academy (2025) *The future of fraud detection: trends and challenges.* Tilgjengelig fra: https://financialcrimeacademy.org/the-future-of-fraud-detection/ (Hentet: 30.04.2025)

Finans Norge (2024) *«Hei mamma/pappa»-svindel.* Tilgjengelig fra: https://www.svindel.no/selvforsvar/svindelmetoder/hei-mamma-pappa-svindel/ (Hentet: 30.04.2024)

Finanstilsynet (2024) *Risiko- og sårbarhetsanalyse (ROS) 2024*. Tilgjengelig fra: https://www.finanstilsynet.no/publikasjoner-og-analyser/risiko--og-sarbarhetsanalyse/2024/ros-2024/risiko--og-sarbarhetsanalyse-ros-2024/#2-finansiell-infrastruktur (Hentet: 02.04.2025)

Fineman, M. A. (2008) The vulnerable subject: Anchoring equality in the human condition, *Yale Journal of Law & Feminism*, 20(1), s. 1–23.

Fineman, M. A. (2010) The vulnerable subject and the responsive state, *Emory Law Journal*, 60(2), s. 251–267.

Fineman, M. A. (2019) Vulnerability in Law and Bioethics, *Journal of health care for the poor and underserved*, 30(5), s. 52–61. DOI: 10.1353/hpu.2019.0115

Fischer, P., Lea, S. E. G. & Evans, K. M. (2013) Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance, *Journal of Applied Social Psychology*, 43(10), s. 2060–2072. DOI: 10.1111/jasp.12158

Fjellengen, S. (2024) *«Digitalt sårbar i en digital verden» En kvalitativ analyse av politiet og andre aktørers håndtering av bedrageri av eldre personer*. Masteroppgave. Universitetet i Oslo.

Fonseca, C., Moreira, S. & Guedes, I. (2022) Online Consumer Fraud Victimization and Reporting: A Quantitative Study of the Predictors and Motives, *Victims & offenders*, 17(5), s. 756–780. DOI: 10.1080/15564886.2021.2015031

Forbrukerrådet (u.å.) *Svindel.* Tilgjengelig fra: https://www.forbrukerradet.no/forside/okonomi-og-betaling/svindel/ (Hentet: 15.05.2025)

Furnell, S. & Dowling, S. (2019) Cybercrime: a portrait of the landscape. *Journal of Criminological Research, Policy and Practice*, 5(1), s. 13–26. DOI: 10.1108/JCRPP-07-2018-0021

Gillespie, A. A. & Magor, S. (2020) Tackling online fraud. *ERA-Forum*, 20(3), s. 439–454. DOI: 10.1007/s12027-019-00580-y

Goodey, J. (2005) *Victims and victimology research, policy and practice*. Harlow: Pearson Longman.

Grabosky, P. N. (2001) Virtual Criminality: Old Wine in New Bottles?, *Social & legal studies*, 10(2), s. 243-249. DOI: 10.1177/a017405

Graham, R. & Triplett, R. (2017) Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization, *Deviant behavior*, 38(12), s. 1371–1382. DOI: 10.1080/01639625.2016.1254980

Green, D. L., Choi, J. J. & Kane, M. N. (2010) Coping strategies for victims of crime: Effects of the use of emotion-focused, problem-focused, and avoidance-oriented coping, *Journal of Human Behavior in the Social Environment*, 20(6), s. 732–743. DOI: 10.1080/10911351003749128

Green, S. (2007) Crime, victimisation and vulnerability i Walklate, S. (red.) *Handbook of Victims and Victimology*. Cullompton: Willan, s. 91-117.

Greenspan, S. (2009) *Annals of Gullibility: Why We Get Duped and How to Avoid It.* USA: Bloomsbury Publishing

Gundersen, M., Husebye, J. M., Gustavsen, Ø, Vikan, J. A. & Schaubert, V. (2025) *Svindelsentralen.* Tilgjengelig fra: https://www.nrk.no/dokumentar/xl/svindelsentralen-1.17333817 (Hentet: 11.05.2025)

Halder, D. (2022) *Cyber victimology: decoding cyber-crime victimisation*. New York: Routledge

Haugen, H. Ø. & Skilbrei, M. L. (2021) *Håndbok i forskningsetikk og databehandling.* 1.utg. Bergen: Fagbokforlaget

Hawdon, J. (2021) Cybercrime: Victimization, Perpetration, and Techniques, *American journal of criminal justice*, 46(6), s. 837-842. DOI: 10.1007/s12103-021-09652-7

Hennink, M., Hutter, I. & Bailey, A. (2020) *Qualitative research methods*. 2.utg. London: SAGE Publications.

Holt, T. J. & Holt, K. M. (2025) Cybercrime, i Kaufmann, M. & Lomell, H. M. (red.) *De Gruyter Handbook of Digital Criminology.* 1.utg. vol 6. Berlin/Boston: Walter de Gruyter GmbH, s. 149-156. DOI: https://doi.org/10.1515/9783111062037

Holt, T. J., Bossler, A. M. & Seigfried-Spellar, K. C. (2022) *Cybercrime and digital forensics: an introduction*. 3.utg. London: Routledge

Jakobsson, M. & Myers, S. (2007) *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. Hoboken, New Jersey: Wiley-Interscience

James, B. D., Boyle, P. A., & Bennett, D. A. (2014) Correlates of susceptibility to scams in older adults without dementia, *Journal of elder abuse & neglect*, 26(2), s. 107–122. DOI: 10.1080/08946566.2013.821809

Jansen, J. & Leukfeldt, R. (2018) Coping with cybercrime victimization: An exploratory study into impact and change, *Journal of Qualitative Criminal Justice and Criminology*, 6(2), s. 205-228. DOI: 10.21428/88de04a1.976bcaf6

Jewkes, Y. & Yar, M. (2010) *Handbook of internet crime*. Cullompton: Willan

Johannessen, L. E. F., Rafoss, T. W. & Rasmussen, E. B. (2018) *Hvordan bruke teori?: nyttige verktøy i kvalitativ analyse.* Oslo: Universitetsforlaget

Judges, R. A., Gallant, S. N., Yang, L., & Lee, K. (2017) The role of cognition, personality, and trust in fraud victimization in older adults, *Frontiers in psychology*, vol 8, s. 1-10. DOI: 10.3389/fpsyg.2017.00588

Junger, M., Koning, L., Hartel, P. & Veldkamp, B. (2023) In their own words: deception detection by victims and near victims of fraud, *Frontiers in psychology*, vol 14, s. 1-20. DOI: 10.3389/fpsyg.2023.1135369

Kaufmann, M. & Lomell, H. M. (2025) An introduction to digital criminology, i Kaufmann, M. & Lomell, H. M. (red.) *De Gruyter Handbook of Digital Criminology.* 1.utg. vol 6. Berlin/Boston: Walter de Gruyter GmbH, s. 1-19. DOI: https://doi.org/10.1515/9783111062037

Kaufmann, M. (2024) Digital kriminologi, i Lomell, H. M. & Skilbrei, M. L. (red.) *Kriminologi.* 2.utg. s. 252-267.

Kemp, S. & Perez, N. E. (2023) Consumer fraud against older adults in digital society: examining victimization and its impact, *International journal of environmental research and public health*, 20(7), s. 1-17. DOI: 10.3390/ijerph20075404

Kemp, S. (2020) Fraud reporting in Catalonia in the Internet era: Determinants and motives, *European Journal of Criminology*, 19(5), s. 994-1015. DOI: 10.1177/1477370820941405

Kerley, K. R., & Copes, H. (2002) Personal fraud victims and their official responses to victimization, *Journal of Police and Criminal Psychology*, 17(1), 19–35. DOI: 10.1007/BF02802859

Kvale, S. & Flick, U. (2007) *Doing interviews.* London: Sage.

Kaariainen, J. & Siren, R. (2011) Trust in the police, generalized trust and reporting crime, *European journal of criminology*, 8(1), s. 65–81. DOI: 10.1177/1477370810376562

Lai, F., Li, D. & Hsieh, C-T. (2012) Fighting identity theft: The coping perspective, *Decision Support Systems*, 52(2), s. 353–363. DOI: 10.1016/j.dss.2011.09.002

Langford, M., Svensson, A. & Wærstad, T. (2025) Identity theft, i Kaufmann, M. & Lomell, H. M. (red.) *De Gruyter Handbook of Digital Criminology.* 1.utg. vol 6. Berlin/Boston: Walter de Gruyter GmbH, s. 269-277. DOI: https://doi.org/10.1515/9783111062037

Lazarus, R. S. & Folkman, S. (1984) *Stress, appraisal, and coping*. New York: Springer Publishing Company

Lerner, M. J., & Miller, D. T. (1978) Just world research and the attribution process: Looking back and ahead, *Psychological Bulletin*, 85(5), s. 1030–1051. DOI: 10.1037/0033-2909.85.5.1030

Leukfeldt, E. R. & Yar, M. (2016) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis, *Deviant behavior*, 37(3), s. 263–280. DOI: 10.1080/01639625.2015.1012409

Leukfeldt, E. R. (2014) Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization, *Cyberpsychology, behavior and social networking*, 17(8), s. 551–555. DOI: 10.1089/cyber.2014.0008

Loges, W. E. & Jung, J. Y. (2001) Exploring the digital divide – Internet connectedness and age, *Communication research*, 28(4), s. 536-562. DOI: 10.1177/009365001028004007

Mackenzie, C. (2013) The Importance of Relational Autonomy and Capabilities for an Ethics of Vulnerability, i Mackenzie, C., Rogers, W. & Dodds, S. (red.) *Vulnerability.* New York: Oxford University Press, s. 33-59. DOI: 10.1093/acprof:oso/9780199316649.001.0001

Maxwell, J. A. & Reybold, L. E. (2015) Qualitative Research, i Wrigt, J. D. (red.) *International Encyclopedia of the Social & Behavioral Sciences*. 2.utg. Elsevier Ltd. s. 685–689. DOI: 10.1016/B978-0-08-097086-8.10558-6

Mesch, G. S. & Dodel, M. (2018) Low Self-Control, Information Disclosure, and the Risk of Online Fraud, *The American behavioral scientist (Beverly Hills)*, 62(10), s. 1356–1371. DOI: 10.1177/0002764218787854

Metallo, C. & Agrifoglio, R. (2015) The effects of generational differences on use continuance of Twitter: an investigation of digital natives and digital immigrants, *Behaviour & information technology*, 34(9), s. 869-881. DOI: 10.1080/0144929X.2015.1046928

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, L., Sirola, A., Zych, I. & Paek, H-J. (2020) Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context, *International journal of offender therapy and comparative criminology*, 68(5), s. 449-467. DOI: 10.1177/0306624X20981041

NESH – De nasjonale forskningsetiske komiteene (2021) *Forskningsetiske retningslinjer for samfunnsvitenskap og humaniora.* Tilgjengelig fra: https://www.forskningsetikk.no/retningslinjer/hum-sam/forskningsetiske-retningslinjer-for-samfunnsvitenskap-og-humaniora/ (Hentet: 22.04.2025)

Ngo, F. T., Piquero, A. R., LaPrade, J. & Duong, B. (2020) Is it how long we spend online, what we do online, or what we post online?, *Criminal Justice Review*, 45(4), s. 430–451. DOI: 10.1177/0734016820934175

Nielsen, B. G. & Snare, A. (1998) *Viktimologi: om forbrydelsens ofre: teori og praksis*. Århus: Aarhus Universitetsforlag

Niux (u.å.) *Future trends in fraud detection and investigation.* Tilgjengelig fra: https://www.nuix.com/resources/future-trends-fraud-detection-and-investigation (Hentet: 30.04.2025)

Nkom – Nasjonal kommunikasjonsmyndighet (2020) *Om regelverket – eIDAS-forordningen.* Tilgjengelig fra: https://nkom.no/internett/elektronisk-id-og-tillitstjenester/eidas-forordningen (Hentet: 18.05.2025)

Nkom – Nasjonal kommunikasjonsmyndighet (2025) *Elektronisk identifikasjon (eID)* Tilgjengelig fra: https://nkom.no/internett/elektronisk-id-og-tillitstjenester/elektronisk-identifikasjon-eid?utm_source=chatgpt.com#eid_bidrar_til_et_tryggere_internett (Hentet: 18.05.2025)

Nkom –Nasjonal kommunikasjonsmyndighet (2024) *Norge skal lede global kamp mot digital svindel.* Tilgjengelig fra: https://nkom.no/aktuelt/norge-skal-lede-global-kamp-mot-digital-svindel (Hentet: 30.04.2025)

NorSIS – Norsk senter for informasjonssikring (2023) *Nordmenn og digital sikkerhetskultur 2023*. Tilgjengelig fra: https://norsis.no/sikkerhetskultur2023/sikkerhetspraksis/ (Hentet: 13.04.2025)

Notté, R., Leukfeldt, E. R. & Malsch, M. (2021) Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands, *International review of victimology*, 27(3), s. 272-294. DOI: 10.1177/02697580211010692

NSM – Nasjonal sikkerhetsmyndighet (2023) *Nasjonalt digitalt risikobilde 2023.* Tilgjengelig fra: https://nsm.no/getfile.php/1313382-1719434559/NSM/Filer/Dokumenter/Rapporter/Nasjonalt%20digitalt%20risikobilde%202023.pdf (Hentet: 02.04.2025)

NSM – Nasjonal sikkerhetsmyndighet (2024) *Risiko 2024.* Tilgjengelig fra: https://nsm.no/getfile.php/1313477-

1719434219/NSM/Filer/Dokumenter/Rapporter/Risiko%202024.pdf (Hentet: 02.04.2025)

Näsi, M., Danielsson, P. & Kaakinen, M. (2023) Cybercrime Victimisation and Polyvictimisation in Finland—Prevalence and Risk Factors, *European journal on criminal policy and research*, 29(2), s. 283-301. DOI: 10.1007/s10610-021-09497-0

Oksanen, A. & Keipi, T. (2013) Young people as victims of crime on the internet: A population-based study in Finland, *Vulnerable children and youth studies*, 8(4), s. 298–309. DOI: 10.1080/17450128.2012.752119

Park, S. (2017) *Digital Capital*. London: Palgrave Macmillan.

Parti, K. & Tahir, F. (2023) "If We Don't Listen to Them, We Make Them Lose More than Money:" Exploring Reasons for Underreporting and the Needs of Older Scam Victims, *Social sciences (Basel)*, 12(5), s. 264-281. DOI: 10.3390/socsci12050264

Parti, K. (2023) What is a capable guardian to older fraud victims? Comparison of younger and older victims characteristics of online fraud utilizing routine activity theory, *Frontiers in psychology*, vol. 14, s. 1-16. DOI: 10.3389/fpsyg.2023.1118741

Partin, R. D., Meldrum, R. C., Lehmann, P. S., Back, S. & Trucco, E. M. (2022) Low Self-Control and Cybercrime Victimization: An Examination of Indirect Effects Through Risky Online Behavior, *Crime and delinquency*, 68(1314), s. 2476-2502. DOI: 10.1177/00111287211061728

Pemberton, A. & Mulder, E. (2025) Victimization as transformative experience: A phenomenological perspective, *Theoretical criminology*, 29(2), s. 214-230. DOI: 10.1177/13624806241271764.

Pemberton, A., Mulder, E., & Aarten, P. G. M. (2019a) Stories of injustice: Towards a narrative victimology, *European Journal of Criminology*, 16(4), s. 391-412. DOI: 10.1177/1477370818770843

Pemberton, A., Aarten, P. G., & Mulder, E. (2019b) Stories as property: Narrative ownership as a key concept in victims' experiences with criminal justice, *Criminology & Criminal Justice*, 19(4), s. 404-420. DOI: 10.1177/1748895818778320

Pileberg, S. (2024) *Forskere mener at svindelofre må hjelp av staten.* Tilgjengelig fra: https://www.jus.uio.no/ifp/forskning/aktuelle-saker/2024/svindelofre-ma-fa-hjelp-av-staten.html (Hentet: 11.05.2025)

Politidirektoratet (2015) *Datakrimstrategien.* Tilgjengelig fra: https://www.regjeringen.no/contentassets/4d2ba37bf2ae4cc9ac39afdf20a2f41b/datakrimstrategi_2015.pdf (Hentet: 28.04.2025)

Politiet (2023) *Cyberkriminalitet 2023.* Tilgjengelig fra: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf (Hentet: 06.03.2025)

Politiet (2024) *Cyberkriminalitet 2024.* Tilgjengelig fra: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf (Hentet: 06.03.2024)

Politiet (2025) *Cyberkriminalitet 2025.* Tilgjengelig fra: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2025.pdf (Hentet: 06.04.2024)

Polkinghorne, D. E. (2007) Validity Issues in Narrative Research, *Qualitative inquiry*, 13(4), s. 471–486. DOI: 10.1177/1077800406297670

Powell, A., Stratton, G. & Cameron, R. (2018) *Digital Criminology: Crime and Justice in Digital Society*. New York & London: Routledge

Pratt, T. C., Holtfreter, K. & Reisig, M. D. (2010) Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory, *The journal of research in crime and delinquency*, 47(3), s. 267–296. DOI: 10.1177/0022427810365903

Prensky, M. (2001) Digital Natives, Digital Immigrants, *On the horizon*, 9(5), s. 1–6. DOI: 10.1108/10748120110424816

Ragnedda, M. & Ruiu, M. L. (2020) *Digital Capital: A Bourdieusian Perspective on the Digital Divide*. 1.utg. Bingley: Emerald Publishing Limited. DOI: 10.1108/9781839095504

Ragnedda, M. (2018) Conceptualising digital capital, *Telematics and Informatics*, 35(8), s. 2366–2375. DOI: 10.1016/j.tele.2018.10.006

Ranchordas, S. & Beck, M. (2025) Vulnerability, i Kaufmann, M. & Lomell, H. M. (red.) *De Gruyter Handbook of Digital Criminology.* 1.utg. vol 6. Berlin/Boston: Walter de Gruyter GmbH, s. 509-517. DOI: https://doi.org/10.1515/9783111062037

Reep-van den Bergh, C. M. M. & Junger, M. (2018) Victims of cybercrime in Europe: a review of victim surveys, *Crime science*, 7(1), s. 1-15. DOI: 10.1186/s40163-018-0079-3

Regjeringen (2024b) *Fremtidens digitale Norge – Nasjonal digitaliseringsstrategi 2024-2030.* Tilgjengelig fra: https://www.regjeringen.no/no/tema/statlig-forvaltning/it-politikk/ny-nasjonal-digitaliseringsstrategi/id2982892/ (Hentet: 09.01.2025)

Reisig, M., & Holtfreter, K. (2007) Fraud victimization and confidence in Florida's legal authorities, *Journal of Financial Crime*, 14(2), s. 113–125. DOI: 10.1007/s10610-016-9310-5

Reyns, B. W., Randa, R. & Henson, B. (2016) Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis, *Crime Prevention and Community Safety*, 18(1), s. 38–59. DOI: 10.1057/cpcs.2015.21

Richards, K. & Cross, C. (2018) Online fraud victims' experiences of participating in qualitative interviews, *Criminal justice studies*, 31(1), s. 95-111 DOI: 10.1080/1478601X.2017.1396217

Roaldseth, S. L. & Landsverk, H. (2024) Kristin ble svindlet og mistet grendehuset sine penger: - Du føler deg lite lur, *NRK*, 22.desember. Tilgjengelig fra: https://www.nrk.no/mr/kristin-grebstad-ble-svindlet-for-over-100.000-da-hun-trodde-hun-solgte-sko-med-helthjem-pa-facebook-1.17171222 (Hentet: 16.02.2025)

Rock, P. (2002) On becoming a victim, i Hoyle, C. & Young, R. (red.) *New Visions of Crime Victims*. Oxford: Hart Publishing, s. 1-22.

Romele, A. (2021) Technological Capital: Bourdieu, Postphenomenology, and the Philosophy of Technology Beyond the Empirical Turn, *Philosophy & technology*, 34(3), s. 483–505. DOI: 10.1007/s13347-020-00398-4

Ross, M., Grossmann, I., & Schryer, E. (2014) Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud, *Perspectives on psychological science*, 9(4), s. 427–442. DOI: 10.1177/1745691614535935

Rughinis, R., Bran, E., Staiculescu, A. & Radovici, A. (2024) From cybercrime to digital balance: How human development shapes digital risk cultures, *Information (Basel)*, 15(1), s. 50-67. DOI: 10.3390/info15010050

Sandberg, S (2010) What can 'lies' tell us about life? Notes towards a framework of narrative criminology, *Journal of criminal justice education*, 21(4), s. 447–465. DOI: 10.1080/10511253.2010.516564

Scott, M. B. & Lyman, S. M. (1968) Accounts, *American sociological review*, 33(1), s. 46–61.

Seniornett (2024) *Om oss.* Tilgjengelig fra: https://www.seniornett.no/om-oss/ (Hentet: 22.04.2025)

Skilbrei, M-L. (2019) *Kvalitative metoder: Planlegging, gjennomføring, og etisk refleksjon.* Bergen: Fagbokforlaget.

St.meld. nr. 27 (2015-2016). *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet.*

Straffeloven (2005). Lov om straff (LOV-2005-05-20-28). Lovdata. https://lovdata.no/dokument/NL/lov/2005-05-20-28

Stratton, G., Powell, A. & Cameron, R. (2017) Crime and justice in digital society: towards a 'digital criminology'?, *International journal for crime, justice and social democracy*, 6(2), s. 17–33. DOI: 10.5204/ijcjsd.v6i2.355

Strobl, R. (2010) Becoming a victim, i Shoham, S. G, Knepper, P., & Kett, M. (red.) *International handbook of victimology*. CRC Press Taylor and Francis Group: Boca Raton, Florida, s. 3-25.

Sur, A., Deliema, M., & Brown, E. (2021) Contextual and social predictors of scam susceptibility and fraud victimization, *SSRN Electronic Journal*, s. 1-42. DOI: 10.2139/ssrn.4053903

Thagaard, T. (2019) *Systematikk og innlevelse: en innføring i kvalitative metode*. 5.utg. Bergen: Fagbokforlaget.

Thunberg, S. & Arnell, L. (2022) Pioneering the use of technologies in qualitative research – A research review of the use of digital interviews, *International Journal of Social Research Methodology*, 25(6), s. 757-768. DOI: 10.1080/13645579.2021.1935565

Tjora, A. H. (2021) *Kvalitative forskningsmetoder i praksis.* 4.utg. Oslo: Gyldendal

Trøen, M. I. N. & Strande, O. B. (2020) Lillian vart svindla for over 300.000 – må pantsette huset, *NRK*, 2.juni. Tilgjengelig fra: https://www.nrk.no/innlandet/lillian-vart-svindla-for-300.000-kroner-og-synest-banken-har-vore-lite-hjelpsame-1.15037264 (Hentet: 16.02.2025)

Twigt, M. A. (2025) Social media, i Kaufmann, M. & Lomell, H. M. (red.) *De Gruyter Handbook of Digital Criminology.* 1.utg. vol 6. Berlin/Boston: Walter de Gruyter GmbH, s. 461-468. DOI: https://doi.org/10.1515/9783111062037

UiO (u.å) *Hjelp og veiledninger for Zoom på UiO*. Tilgjengelig fra: https://www.uio.no/tjenester/it/telefoni-sanntid/videokonf/zoom/hjelp/ (Hentet: 04.05.2025)

van Wilsem, J. (2013) 'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization', *European sociological review*, 29(2), s. 168–178. DOI: 10.1093/esr/jcr053

van't Hoff-de Goede, S. M., Leukfeldt, E. R., van der Kleij, R. & van de Weijer, S. (2021) The online behaviour and victimization study: the development of an experimental research instrument for measuring and explaining online behaviour and cybercrime

victimization, i Weulen Kranenbarg, M. & Leukfeldt, R. (red.) *Cybercrime in context. The human factor in victimization, offending and policing.* Sveits: Springer, s. 21-41. DOI: 10.1007/978-3-030-60527-8_3

Verwiebe, R. & Hagemann, S. (2024) Bourdieu revisited: new forms of digital capital – emergence, reproduction, inequality of distribution, *Information, communication & society*, s. 1–23. DOI: 10.1080/1369118X.2024.2358170

Voce, I. & Morgan, A. (2023) Online behaviour, life stressors and profit-motivated cybercrime victimisation, *Trends and issues in crime and criminal justice*, (675), s. 1-18. DOI: 10.52922/ti77062

Walklate, S. (2011) Reframing criminal victimization: Finding a place for vulnerability and resilience, *Theoretical criminology,* 15(2), s. 179-194. DOI: 10.1177/1362480610383452

Walklate, S. (2025) Victimization, i Kaufmann, M. & Lomell, H. M. (red.) *De Gruyter Handbook of Digital Criminology.* 1.utg. vol 6. Berlin/Boston: Walter de Gruyter GmbH, s. 501-508. DOI: https://doi.org/10.1515/9783111062037

Walklate, S., Maher, J., McCulloc, J., Fitz-Gibbon, K. & Beavis, K. (2019) Victim stories and victim policy: Is there a case for a narrative victimology?, *Crime, media, culture*. 15(2), s. 199–215. DOI: 10.1177/1741659018760105

Wall, D. S. (2007) *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press

Wang, Q., Myers, M. D. & Sundaram, D. (2013) Digital natives and digital immigrants – towards a model of digital fluency, *Business & information systems engineering*, 5(6), s. 409-419 DOI: 10.1007/s12599-013-0296-y

Whitty, M. T. (2019) Predicting susceptibility to cyber-fraud victimhood, *Journal of Financial Crime*, 26(1), s. 277–292. DOI: 10.1108/JFC-10-2017-0095

Willis, G. M. & Letourneau, E. J. (2018) Promoting Accurate and Respectful Language to Describe Individuals and Groups, *Sexual abuse*, 30(5), s. 480–483. DOI: 10.1177/1079063218783799

Yar, M. & Steinmetz, K. F. (2019) *Cybercrime and Society.* 3.utg. Thousand Oaks, California: Sage Publications

Yin, R. K. (2013) Validity and generalization in future case study evalutations, *Evalutation (London, England, 1995),* 19(3), s. 321-332. DOI: 10.1177/1356389013497081

Zieniūtė, U. (2024) *Ny studie viser at over 70 % nordmenn har blitt utsatt for cyberangrep*. Tilgjengelig fra: https://nordvpn.com/no/blog/studie-nettsvindel-norge/ (Hentet: 03.05.2025)

Økokrim (2023) *Bedrageri – et samfunnsproblem.* Tilgjengelig fra: https://img8.custompublish.com/getfile.php/5180722.2528.qaamznluipnjsl/Bedrageri%2B-%2Bet%2Bsamfunnsproblem.pdf?return=www.okokrim.no (Hentet: 02.04.2025)

Økokrim (2024) *Årsrapport 2023.* Tilgjengelig fra: https://img8.custompublish.com/getfile.php/5295597.2528.7bqmlmtiqjmkwk/%C3%98kokrim%2B%E2%80%93%2Ba%CC%8Arsrapport%2B2023-nett.pdf?return=www.okokrim.no (Hentet: 02.04.2025)

Vedlegg

Vedlegg 1: Godkjenning fra SIKT

Sikt

Vurdering av behandling av personopplysninger

Referansenummer	Vurderingstype	Dato
737656	Standard	12.06.2024

Tittel
Nettkriminalitet i Norge - Eldre og yngre innbyggere sine erfaringer med å bli utsatt for svindel og bedragerier på nett

Behandlingsansvarlig institusjon
Universitetet i Oslo / Det juridiske fakultet / Institutt for kriminologi og rettssosiologi

Prosjektansvarlig
Silje Anderdal Bakken

Student
Lotte Josefine Vollmerhaus Føyn

Prosjektperiode
10.06.2024 - 30.11.2025

Kategorier personopplysninger
Alminnelige
Særlige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)
Uttrykkelig samtykke (Personvernforordningen art. 9 nr. 2 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 30.11.2025.

Meldeskjema

Kommentar
OM VURDERINGEN
Sikt har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket.

TYPE PERSONOPPLYSNINGER
Prosjektet vil behandle særlige kategorier personopplysninger om helse (Utvalg 1 og Utvalg 2).

FØLG DIN INSTITUSJONS RETNINGSLINJER
Vi har vurdert at du har lovlig grunnlag til å behandle personopplysningene, men husk at det er institusjonen du er ansatt/student ved som avgjør hvilke databehandlere du kan bruke og hvordan du må lagre og sikre data i ditt prosjekt. Husk å bruke leverandører som din institusjon har avtale med (f.eks. ved skylagring, nettspørreskjema, videosamtale el.).

Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Se våre nettsider om hvilke endringer du må melde: https://sikt.no/melde-endringar-i-meldeskjema

OPPFØLGING AV PROSJEKTET
Vi vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Vedlegg 2: Informasjonsskriv og samtykkeskjema

Vil du delta i forskningsprosjektet

"Nettkriminalitet i Norge – Eldre og yngre innbyggere sine erfaringer med å ha blitt utsatt for svindel og bedragerier på nett»?

Dette prosjektet er en masteroppgave som skrives ved Institutt for kriminologi og rettssosiologi (IKRS) ved Universitetet i Oslo. I dette prosjektet ønsker jeg å kartlegge eldre og yngre innbyggere i Norge sine erfaringer og opplevelser med å bli utsatt for svindel og bedragerier på nett. I dette skrivet vil du få informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Formålet med denne masteroppgaven er å gjennomføre intervjuer for å fange opp hvilke erfaringer eldre og yngre innbyggere i Norge har med å bli utsatt for svindel og bedragerier på nett. Jeg ønsker å få vite mer om hvilke typer svindel og bedragerier de blir utsatt for, hvordan de opplevde hendelsen, og hvilke mulige konsekvenser hendelsen har hatt for dem. Oppgavens problemstilling vil derfor være som følger; *«Hvilke erfaringer har eldre og yngre innbyggere i Norge med å bli utsatt for svindel og bedragerier på nett, og er det en forskjell i hva de opplever, samt hvordan de opplever dette?»*.

Hvem er ansvarlig for forskningsprosjektet?

Institutt for kriminologi og rettssosiologi ved Universitetet i Oslo er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Utvalget er trukket på bakgrunn av utvalgskriterier knyttet til alder og at man har blitt utsatt for svindel og bedragerier på nett. Du blir altså spurt om å delta fordi du har opplevd svindel og bedrageri på nett, og befinner deg i en av aldersgruppene som er sentrale i prosjektet.

Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet, innebærer det at du stiller til et dybdeintervju, som vil ta deg cirka 45 til 60 minutter. Intervjuet vil inneholde spørsmål om hva slags type svindel og bedrageri du har opplevd, hvordan du opplevde hendelsen, og hvilke konsekvenser hendelsen har hatt for deg. For å ivareta ditt og andres personvern, ønsker jeg at du ikke opplyser noens navn eller andre identifiserbare karakteristikker dersom du oppgir sensitive opplysninger. Ved eget samtykke, vil intervjuet tas opp med lydopptaker lånt fra Universitet i Oslo og notert av meg. Dette er for å sikre at dine utsagn blir korrekte, slik at det ikke blir tatt ut av kontekst. Lydopptaket vil transkriberes i løpet av svært kort tid etter intervjuet, hvor all informasjon vil anonymiseres fortløpende.

Frivillig deltakelse

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet og ingen deler av intervjuet vil bli brukt i oppgaven. Jeg understreker også at det ikke vil ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan jeg oppbevarer og bruker dine opplysninger

Jeg vil kun bruke opplysningene om deg til formålene jeg har fortalt om i dette skrivet. Jeg behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Det vil kun være jeg som gjennomfører masterprosjektet, og som dermed vil ha tilgang til dine opplysninger og datamaterialet. Navnet ditt og kontaktopplysningene dine vil bli erstattet med en kode som lagres på egen navneliste adskilt fra øvrige data. Dataene vil oppbevares på UiOs brukersystem bak lukket tilgang ved hjelp av en innloggingsfunksjon, samt en kryptert harddisk dersom det må fraktes. Jeg vil ikke skrive om eller publisere informasjon der du eller andre deltakere vil kunne gjenkjennes. Opplysning om alderen din kan dukke opp, men ingenting mer spesifikt vil nevnes (f.eks navn).

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?

Prosjektet vil etter planen avsluttes innen mai 2025. Dataene som blir anvendt i prosjektet vil bli slettet når masteroppgaven er levert, og den seneste sluttdatoen for prosjektet vil være utgangen av november 2025. De anonymiserte opplysningene vil ikke gjenbrukes for videre forskning etter prosjektslutt.

Hva gir meg rett til å behandle personopplysninger om deg?

Jeg behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Oslo har Sikt – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger jeg behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvor kan jeg finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

Meg: Lotte Føyn (mail: l.j.v.foyn@student.jus.uio.no, telefon: 947 88 232)
Prosjektansvarlig: Silje Anderdal Bakken (s.a.bakken@jus.uio.no) ved Universitetet i Oslo, IKRS.
Vårt personvernombud: Roger Markgraf-Bye, personvernombud@uio.no

Hvis du har spørsmål knyttet til SIKT sin vurdering av prosjektet, kan du ta kontakt med: SIKT – Kunnskapssektorens tjenesteleverandør på e-post (personverntjenester@sikt.no) eller på telefon: 73 98 40 40.

Med vennlig hilsen

Silje Anderdal Bakken
(Forsker/veileder)

Lotte Føyn
(Student)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *«Nettkriminalitet i Norge – Eldre og yngre innbyggere sine erfaringer med å bli utsatt for svindel og bedragerier på nett»,* og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju
- ☐ at intervjuet blir tatt opp med lydopptaker
- ☐ at mine opplysninger behandles frem til prosjektet er avsluttet
- ☐ å delta til intervju, men at navn og kontaktopplysninger ikke skrives ned noe sted under behandling (navn vil aldri skrives ned i selve oppgaven)

(Signert av prosjektdeltaker, dato)

Vedlegg 3: Intervjuguide

Intervjuguide

«Nettkriminalitet i Norge – eldre og yngre innbyggere sine erfaringer med å ha blitt utsatt for svindel og bedragerier på nett»

Introduksjon – informasjon om prosjektet og problemstilling

1. Informere om bakgrunn og formål for samtalen
   - Undersøke og kartlegge hvilke erfaringer eldre og yngre innbyggere har med å bli utsatt for svindel og bedragerier på nett
2. Forklare hva intervjuet skal brukes til
   - Ønsker å benytte intervjuer for å få en kvalitativ forståelse av fenomenet nettkriminalitet i norsk kontekst
3. Informere om anonymitet og taushetsplikt
   - Gjennomgå informasjonsskrivet og samtykkeskjema
   - Gi informasjon om lyd- og båndopptak og forsikre om at begge parter har skrevet under samtykkeskjema før start
4. Avklar om intervjudeltakeren har spørsmål, og informer om følgende: Dersom du ikke ønsker å svare på noen av spørsmålene er det bare å si ifra, og spør dersom noe er uklart.

// Start lydopptak

Innledende spørsmål:

Bakgrunn og kontekst – Om intervjudeltakeren

- Vil du fortelle litt om deg selv? (alder, utdanning, bosted etc.)

Digitale vaner – Bruk og rutiner på nett

- Hvilke digitale enheter eier du? (f.eks pc, mobil, tv, nettbrett, etc.)
- Kan du beskrive eller vise meg hva du typisk bruker mobilen og de digitale enhetene dine til?
  - Oppfølgingsspørsmål:
    Hvilke digitale plattformer og apper bruker du i din hverdag? (f.eks Snapchat, Facebook, LinkedIn, Instagram, apper med banktjenester som f.eks BankID, Paypal, Vipps etc.)
    Hvilke nettsider bruker du?
    Hvilke aktiviteter gjør du på nett?

- Hvor mye tid vil du si at du bruker på pc, mobil, skjerm generelt i løpet av en dag/uke?

Sentrale spørsmål/nøkkelspørsmål:

Erfaringer og opplevelser

- Kan du fortelle meg om når du ble utsatt for svindel og bedrageri på nett, og hvordan du opplevde denne hendelsen?
  - Oppfølgingsspørsmål:
    Hva ledet opp til situasjonen?
    Hvordan oppsto situasjonen?
    Hvor var du når det skjedde?
    Hvilken aktivitet gjorde du på nett når dette skjedde?
    Hadde det skjedd noe i livet ditt når du ble utsatt for dette?
    Hvordan opplevde du avsenderen, altså den som «gjorde» svindelen mot deg?
- Hva slags type svindel og bedrageri vil du si at du opplevde?

Risikofaktorer og årsaker til viktimisering

- Hvorfor tror du at det skjedde med deg fremfor andre?
- Tror du at din alder har påvirket din opplevelse av nettkriminalitet?
- Hvordan vil du beskrive din kunnskap om internett og digital sikkerhet, samt dine teknologiske ferdigheter når det gjelder å oppdage og unngå nettsvindel?

Konsekvenser av hendelsen og tiden etter hendelsen (både kortsiktige og langsiktige konsekvenser)

- Vil du fortelle meg om hvordan det var for deg etter at du ble utsatt for svindel og bedrageri på nett?
- Hvilke konsekvenser hadde situasjonen for deg og hvordan håndterte du situasjonen?
  Oppfølgingsspørsmål
  - Økonomiske konsekvenser
    - Hvordan påvirket nettkriminalitet din økonomiske situasjon og livsstil? (f.eks tap av penger)
  - Sosiale konsekvenser

- Informerte du ditt sosiale nettverk (familie, venner og kollegaer) om hendelsen; Hvis ja, hvordan opplevde du dette? Fikk du negative eller positive reaksjoner, i så fall hvilke? Hvis nei, hvorfor ikke?
- Har hendelsen ført til noen endringer i dine sosiale relasjoner eller tillitsforhold til andre?
- Tok du kontakt med noen andre enn familie og venner i ettertid av hendelsen, f.eks hjelpetjenester, støttesystemer, banken, i så fall hvordan opplevde du dette? Og hvis ikke, hvorfor tok du ikke kontakt med noen?
  Oppfølgingsspørsmål:
  Rapporterte du hendelsen til politiet, hvis ja, hvorfor, hvis nei, hvorfor ikke?
  Hva var din opplevelse med dette?

➢ Psykiske konsekvenser

- Har hendelsen gått utover deg psykisk? (f.eks få angst eller depresjon, bli mer usikker, påvirket selvfølelse eller selvtillit etc.)
  Hvis ja, hvordan har du håndtert dette? (f.eks fått profesjonell hjelp etc.)

➢ Digitale konsekvenser

- Endret du noen av dine digitale vaner i ettertid av hendelsen? I så fall hva endret du? Og hvis du ikke endret noe og levde videre som før, hvorfor det?
- Har hendelsen påvirket din bruk av teknologi generelt? (for eksempel skru av mobilen oftere, ikke gå inn på visse apper, ikke svare på telefon hvis man blir ringt med skjult nummer etc., laste ned programvarer som identifiserer utrygge nettsider etc?)
- Har du oppsøkt noe informasjon i ettertid av hendelsen? (for eksempel sett noen vider om digital sikkerhet, tatt kurs eller opplæring for å forbedre digital sikkerhet etc.)
- Har hendelsen gjort deg mer bevisst på risikoene ved digital teknologi? I så fall, hvordan har dette påvirket dine digitale vaner?

Avslutning:

- Forebygging og tiltak
  ➢ Har du noen råd eller anbefalinger til hvordan andre kan unngå å oppleve nettkriminalitet? Eventuelt om det er noe samfunnet kan gjøre bedre for å støtte ofre for nettkriminalitet?
- Er det noe som er uklart?

- Er det noe du vil spørre meg om?
- Er det noe du vil tilføye eller legge til?

// Stopp lydopptak

Vedlegg 4: Nyhetsbrev – Seniornett

AKTUELT

Vil du delta i et forskningsprosjekt om nettkriminalitet?

Publisert 19.09.2024 Oppdatert 19.09.2024 SKRIV UT

"Nettkriminalitet i Norge – Eldre og yngre innbyggere sine erfaringer med å ha blitt utsatt for svindel og bedragerier på nett»? er en masteroppgave som skrives ved Institutt for kriminologi og rettssosiologi (IKRS) ved Universitetet i Oslo. I dette prosjektet skal eldre og yngre innbyggere i Norge sine erfaringer og opplevelser med å bli utsatt for svindel og bedragerier på nett undersøkes.

Det skal gjennomføres intervjuer for å fange opp hvilke typer svindel og bedragerier de blir utsatt for, hvordan de opplevde hendelsen, og hvilke mulige konsekvenser hendelsen har hatt for dem.

Kunne du tenkt deg å være med på et slikt intervju?

Hvis du velger å delta i prosjektet, innebærer det at du stiller til et dybdeintervju, som vil ta deg cirka 45 til 60 minutter. Intervjuet vil inneholde spørsmål om hva slags type svindel og bedrageri du har opplevd, hvordan du opplevde hendelsen, og hvilke konsekvenser hendelsen har hatt for deg.

Alle personopplysninger vil bli behandlet konfidensielt.

Du kan lese mer om prosjektet her: Informasjonsskriv

Om du kunne tenkte deg å være med på dette, eller ønsker å vite mer om prosjektet, kan du kontakte:

Lotte Føyn

E-post: l.j.v.foyn@student.jus.uio.no, eller telefon: 947 88 232.