Identitetstyveri og identitetssvindel: konsekvenser i offentlig sektor

av

Dejan Ljusic

Master's thesis

Master of Science in Information Security

30 ECTS

Department of Computer Science and Media Technology

Gjøvik University College, 2011

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Foreord

Denne oppgaven er en avsluttende del i masterprogrammet innen Informasjonssikkerhet ved
Høyskolen i Gjøvik.

Denne oppgaven har gitt meg verdifull kunnskap og innsikt i problematikken omkring
D nummer rekvirering som er identifikator for personer som har ikke norsk fødsels og personnummer i Norge. Oppgavens tema har vært interessant og det har bidratt til en prosess som har vært motiverende.

Jeg vil takke min faglige veileder Finn Olav Sveen fra HiG. Han har bidratt med både konstruktiv og lærerik veiledning.

Jeg vil videre takke Hilde Ingebrigtsen og hennes ID – gruppen i NAV Kontroll øst for at de tok seg tid til intervju og bidra med informasjon i henhold til rutiner ved rekvirering av D nummer i NAV.

Jeg vil videre takke Ann Kristin Roheim, Hilde Marianne Henriksen og Lise Abelsnes fra Skatteetaten for at de tok seg tid til intervju og bidra med informasjon i henhold til rutiner ved rekvirering av D nummer i Skatteetaen og informasjon om folkeregister data.

Jeg vil videre takke Jan Daniel Juniszewski fra FNO for at han tok seg tid til intervju og bidra med informasjon i henhold til rutiner ved rekvirering av D nummer og informasjon om finansnærings synspunkt om problemet ved rekvirering av D nummer

Jeg vil videre takke Anita Wikran Hartviksen fra Brønnøysundregistrene for at hun tok seg tid til intervju og bidra med informasjon i henhold til rutiner ved rekvirering av D nummer i Brønnøysundregistret

En stor takk til Christian Meyer fra Norsk Senter for Informasjonssikring for å ta seg tid til og svare på spørsmål.

Mine kollegaer fra jobben, Ørjan, Asbjørn og Joel som har med sitt engasjement bidratt med sine tanker og ideer samtidig prøvde å rette alle skrivefeilene i oppgaven, noe jeg er veldig takknemlig for.

Tilslutt vil jeg takke familien for deres moralske støtte under skriveprosessen og tålmodighet.

Oversikt over figurer:

Oversikt over tabeller

1. Innlending

Identitetsstyveri er i dag en av de sterkest voksende formene for kriminalitet i verden. I USA utsettes omslag 9 millioner mennesker for ID tyveri hvert år FTC[1][1]. Leif T Aanensen fra Datatilsynet[2] hevder at hver nordmann kan bli utsatt for forsøk på identitetstyveri to til tre ganger i løpet av livet. Identitetstyvene bruker forskjellige metoder for å skaffe nødvendige opplysninger, eksempelvis sosiale nettverk og phishing. De utnytter svakheter som finnes i datasystemer, vår sosiale infrastruktur og ikke minst vår mangel på kunnskap om problemet.

Det koster penger og tid til å rette opp sakker ved ID-Tyveri. Noen problemer kan løses ganske kjapt men noen kan koste flere tusen kroner og mange dager arbeid for å rette alt. I noen tilfelle det er veldig vanskelig å finne ut at person var utsett for Id tyveri før det er ganske sent.

Det er ikke alltid snakk om tyveri av andres identitet. Noen ganger opprettes fiktive identiteter for å utnytte systemene. Ved å benytte en falsk identitet kan en person skaffe forskjellige ytelser fra NAV, opprette egen bedrift etc. NAV, Brønnøysundregistrene og Skatteetaten er bare en del av offentlig sektor som har utfordringer på dette område.

1.1. Nøkkelord

Identitetstyveri, identitetssvindel, identitetskontroll, dokumentkontroll, falsk identitet, fiktiv identitet identifikator i Norge, D nummer rekvirenter.

1.2. Problembeskrivelse

Per i dag må vi i Norge basere oss på antagelser om problemets omfang, da statistisk tallmaterialet ikke finnes. Denne oppgaven har som mål å definere konsekvenser ved rekvirering av D nummer og hva identitetstyveri betyr for offentlig sektor i Norge.

[1] Federal Trade Commission

Informasjon fra NAV[2] viser at i 2010 klarte de å slette 42 fiktive identiteter, åtte personer er dømt og stønader for millioner av kroner er stoppet. De største anmeldelsene gjelder mistanke om fiktive identiteter[3].

Vi skal undersøke hvordan de føringer som ligger i lovverket får konsekvenser for hvordan offentlig og privat sektor rekvirerer D-nummer[3], og om begrensninger i lovverket medfører økt risiko for identitetstyveri eller forfalskning. Forskjellige etater har per i dag mulighet til å rekvirere D nummer. De må gjøre rekvirering av D nummer for å tjene offentlig og private sektors behov i deres oppgaveløsning.

For å opprette bedrift i Norge man må ha person som har personnummer eller D nummer fra Norge som skal levere oppgavene til offentlig etater i Norge. Ved opprettelse av arbeidstillatelse i Norge person får tildelt personnummer eller D nummer. Hvis person vil opprette en bankkonto i norsk bank eller å ha førekort i Norge det er nødvendig og ha personnummer eller D nummer i Norge. Alle folketrygdrettighetene er knyttet mot personer som har gyldig personnummer eller D nummer. Vi ser at behov for å beskyte dokumentene med personlig opplysningene er stor fordi konsekvenser ved misbruk av disse opplysningene kan vare stor.

Hvem har ansvar for å beskytte vår identitet? Er det bare vi som er ansvarlige, eller har også næringslivet og myndighetene ansvar? Hvordan beskytter norsk lov og rett oss når det gjelder identitetstyveri, og hvilke konsekvenser får det for tildeling og rekvirering av D-nummer? Foreløpig finnes det ikke egen lovbestemmelse for identitetstyveri.

En av offentlig etater som kan bli utsatt for ID tyveri er NAV. Magne Flatby direktør for NAV kontroll og innkreving opplyser i pressmelding[4] at i 2009 anmeldte NAV 1435 personer for svindel av totalt 159 millioner kroner og det er cirka 10 % mer en i 2008. Utarbeidelse av en fiktiv ident er også en type av svindel som er i bruk i verden og som er ganske synlig her i Norge. I følge Magne Flatby som er direktor i NAV Kontroll bare en svindel sak som var basert på svindel

[2] Arbeids- og velferdsetaten

[3] D-nummer er en midlertidig identifikasjon – som brukes isteden for fødselsnummer - for personer som oppholder seg i Norge på midlertidig basis

ved bruk av fiktive identitet[5] kostet NAV 13 millioner kroner. Han også påpeker at kontrollarbeidet i NAV bare tatt toppen av isfjellet.

1.3.Forskningsspørsmålene

1. Hvordan foregår ID svindel?
2. Hvilke metoder kriminellmiljøer bruker mest for anskaffelse av personopplysninger.
3. Hvordan NAV kan svindles?

1.4.Målet med oppgaven

Oppgaven har som mål å utarbeide oversikt over rutinene ved rekvirering av D nummer samtidig å vurdere kan de rutinene som finnes i offentlig etater og private aktører som kan rekvirere D nummer kan øke risiko for misbruk. Målet med oppgaven er også å viser frem sårbare områder som kan utnytes av kriminelle miljøer.

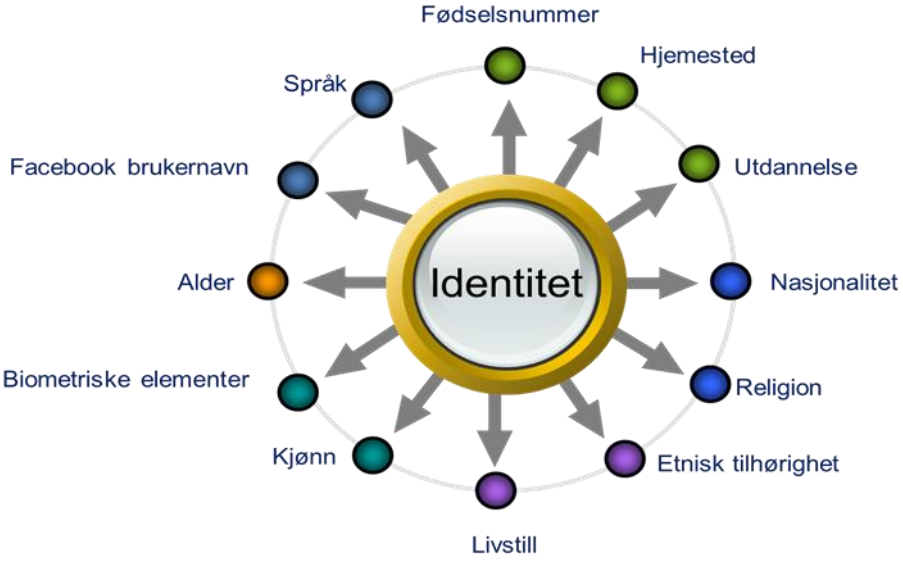
I slutten av oppgaven skal det utarbeides et oversikt over kritiske momenter som vi har fant hos rekvirenter slik at det kan utarbeiddes videre forskning spørsmål som kan undersøkes i videre arbeid

Vi skal også viser frem eksempler fra virkeligheten som kan gi oss forklaring hvordan de utforer kriminelle handlinger.

2. **Hva er identitet**

Det er veldig vanskelig å definere egentlig begrepet ”Identitetstyveri” og det er flere årsaker for det. Men før vi begynner å se på selve problemet det er nødvendig å forstå begrepet identitet. Vi må finne ut hva egentlig er identitet slik at vi kan forstå hva de kriminellere vil stjele fra oss.

Enn definisjon som fleste kan definere som riktig begrep er at identitet er noe som forklarer hvem vi er. Men hvis vi begynner å bruke denne definisjon faller vi ført i enn enda mer komplisert tema – Hvem er jeg?



Figur 2-1 Filosofiks aspekt av identitetet

Før ’70 tallet dette spørsmål var knyttet mot den filosofiske aspekten og enkelt svar at ”identitet er det som man ser når man ser seg i speilet” (Thomas Hylland Eriksen[6]).

”Identity is a person’s self-definition as a separate and distinct individual, including behaviors, beliefes, and attitudes”(Gardiner &Kosmitzki 2008:154).

Her ser vi at selv definisjon som var brukt av Gardiner og Kosmitzki(2008) skiller egne oppførsler, tro og holdninger som er knyttet mot individsidentitet. Som vi har nevnt tidligere identitetsbegrepet kan defineres på forskjellige måter fra ulike synsvinkler. Innen sosiologi identitetsbegrepet brukes også i forhold til rekke aspekter og egenskaper som: alder, kjønn, mote, livsstil, yrke, klasse, nasjonalisme, rase og etniske relasjoner (Korsnes, Olav, Anersen, Heine og Brante, Thomas (1997: 123,124).

Langt tilbake som i 1993 Peter Steinar[7] har publisert karikaturer i The New Yorker magasin som viser to hunder å snakke sammen, og en sier til en annen *"På internett vet ingen at du er en hund."* På dette enkel karikatur Peter viste hvor lett det er,på internett,å vises i et annet lys.

Vi kan se at det er veldig vanskelig å finne riktig definisjon av begrepet identitet og denne oppgaven legger til grunn en forståelse av identitet som er summen av attributter som viser noe hvem vi er.

Vi kan si at identitet er en gruppe av personlig attributter som skiller en person fra et sett av personer for eksempler fødselsnummer blant alle mennesker i Norge. Typiske attributter for en identitet er navn, størrelse, adferd, kontaktdata, fødselsdato, etc.

Men med eksistensen av flere attributter som bestemmer vår identitet, åpner det oppende større risiko for at en tyv eller svindel kommer lettere til noen av disse attributter og kombinasjoner av noen av dem kan øke risiko for oppretting en falsk identitet som kan misbrukes via offentlig eller privat sektor.

3. **Hva er identitetstyveri**

Historien om identitetstyveri viser at kriminaliteten har økt i forekomst med utviklingen av kommunikasjonsteknologi, og er selv nå anerkjent for å være den raskest voksende kriminalitet i verden[8].

Uansett at vi alle har mening om hva egentlig betyr ord identitetstyveri det finnes flere ulike definisjoner av identitetstyveri begrepet i verden. Vi skal nevne noen som er i bruk i utlandet før vi beskriver hvordan vi i Norge definerer dette. Vi viser definisjon som fines hos OECD[4][9]:

"ID theft occurs when a party acquires transfers, possesses, or uses personal information of a natural or legal person in an unauthorized manner, with the intent to commit, or in connection with, fraud or other crimes."

Her ser vi at de har regnet identitetstyveri slik at hvis man har fått andre sine personlige opplysninger på en uautorisert måte med hensikt om å begå svindel, eller med hensikt om å gjøre andre ulovligheter.

Federal Trade Commission som er en av de viktigste aktorene i verden når det gjelder statistikk om identitetstyveri som finnes i USA definerer identitestyveri som:

"Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes"

Her ser vi at FTC var mer konkrete i definisjon hvilke ulike typer av personlig opplysningen kan misbrukes. De nevner konkrete identifikatorene som kan misbrukes. Det viktigst identifikatorene i USA er Social Security Number som er ekvivalnet til norsk fødsels og personnummer.

Kruize[10] i sitt rapport om identitetstyveri skriver at Den Danske rådet for IT sikkerhet definerer identitetstyveri som :

[4] OECD- Organisasjonen for økonomisk samarbeid og utvikling

"Identitetstyveri skjer, når personer tilegner sig andres personoplysninger og udgiver sig for at være disse personer. Det kan skje elektronisk ved brug af bankoplysninger, cpr-numre eller kodeord eller ved at bruge den andens identitetspapirer (sygsikringsbevis, kørekort, m.m). Det er også tale om identitetstyveri, når en person køber produkter, fx over internettet, ved hjælp af en andens person- og kontooplysninger".

Her vi ser at Kruitz har gått litt dypere og ta i definisjon bruk av falske identitet på internett. I ovennevnte definisjoner ser vi tendensen til at identitetstyveri er basert på de hendelser som fører til tap av penger eller en annen kriminellhandling.

Definisjon som er representert i Norge som finnes i Datatilsynet rapport om Identitetstyveri[11] gir bredere mening til definisjonen.

"Identitetstyveri: Innsamling, besittelse, overføring, reproduksjon eller annen manipulering av en annen persons personlige informasjon med den hensikt å skade andres omdømme, begå svindel eller annen kriminell handling"

Her ser vi at bortsett fra å tape penger, kan identitetstyveri bli vurdert som en forbrytelse hvis resultatet er tap av omdømme. Det er ganske stor forskjell i definisjon som brukes her i Norge og i andre land. I Norge definisjon av identitetstyveri går et skritt videre og viser at offer som var utsatt for identitetstyveri trenger ikke å være bare økonomisk skadet men også dårlig omdømme kan forårsake tapt av kunder, brukers tillit til offentlig eller privat sektor.

Vi ser at definisjon som kan definere en tydelig definisjon av begrepet ID tyveri finnes ikke. Det omfates på forskjellige måter hos flere aktører i verden og vi ser mulighet at selve definisjon vil endres i tid framover

4. **Omfang av identitetstyveri**

Historien om identitetstyveri viser at kriminaliteten har økt i forekomst med utviklingen av kommunikasjonsteknologi, og er selv nå anerkjent for å være den raskest voksende kriminalitet i verden.

"*Identitetstyveri er verdens hurtigst voksende kriminelle aktivitet og har passert narkotika i omsetning*[12]"

opplyser Petter Danielsen fra Security Valley på Gjøvik som er prosjektleder som har støtte fra blant annet Nav, Posten Norge, Sparebankforeningen, Sparebank1, Kripos, Politidirektoratet, DnB, Nordea og Næringslivets sikkerhetsorganisasjon FNH. De har også med Datatilsynet, Forbrukerrådet og FAD (Fornyelses og administrasjonsdepartementet).

Ubehag er ikke bare til stede ved identitetstyveri opplevelse. Selv om vi er i de fleste tilfeller, forsikret og dekkes av forsikring svindel koste mye.

Undersøkelse i USA viser tallene[5].

- Det trenges 14 måneder for oppdagelse av identitesttyveri
- 10 millioner amerikanere ble utsatt for ID tyveri i 2006
- 40 timer arbeid kreves for å rydde opp i identitesttyveri
- Stjålet bankkort koster fra 1-12 dollar på internett.

Her i Norge vi følger trend. Knut Erik Clausen i AffinionInternational sier at Vi kan konkludere at Norge er paradis for ID tyvene når det gjelder identitetstyveri.

Magne Flatby direktør for NAV kontroll og innkreving opplyser i pressmelding[13] at i 2009 anmeldte NAV 1435 personer for svindel av totalt 159 millioner kroner og det er cirka 10 % mer en i 2008.

Statistikk fra NAV[14] viser utvikling, beløp og anmeldelser 2008-2010.

[5] Identitetstyveri konferanse (Oslo 2010)

Tabell 4-1 Tapt hos NAV (NAV 2011)

	2008	2009	2010
I alt	155 273 450	158 847 929	133 931 418
Attføringsytelser*	26 812 992	37 752 003	13 484 521
Barnetrygd	1 149 766	2 386 648	4 535 978
Bidragsforskudd	438 850	0	2 034 263
Dagpenger	51 960 675	53 716 979	46 136 773
Enslig forsørger stønad	9 749 884	10 398 861	20 237 539
Foreldrepenger/engangsstønad	1 433 477	2 670 560	2 234 311
Rehabiliteringspenger*	11 577 298	5 040 894	5 741 620
Sykepenger	21 911 167	17 441 212	14 899 729
Uførepensjon	26 339 637	26 348 714	21 564 719
Ventelønn	1 587 138	1 520 894	0
Annet	2 312 566	1 571 164	3 061 965

Selvfølgelig vi kan ikke påstå at alt som står i tabellen skilles identitetstyveri men vi ser at beløp som viser NAV sin statistikk er ganske stor uansett at trenden viser nedgang. Bare fakta at i 2010 NAV Kontroll klarte å slette 42 fiktive identiteter viser at ID tyveri og ID svindel er en reel problem for offentlig sektor.

"En felles statistikk finnes ikke i Norge per i dag og det er stor behov for etablering en felles statistikk som skal vise trend i Identitetstyveri." sier Christian Meyer som leder Id Tyveri prosjekt[6].

[6] Christian Meyer, ID Tyveri konferanse, Oslo 2010

5. **Metoder for anskaffelse av personalopplysninger**

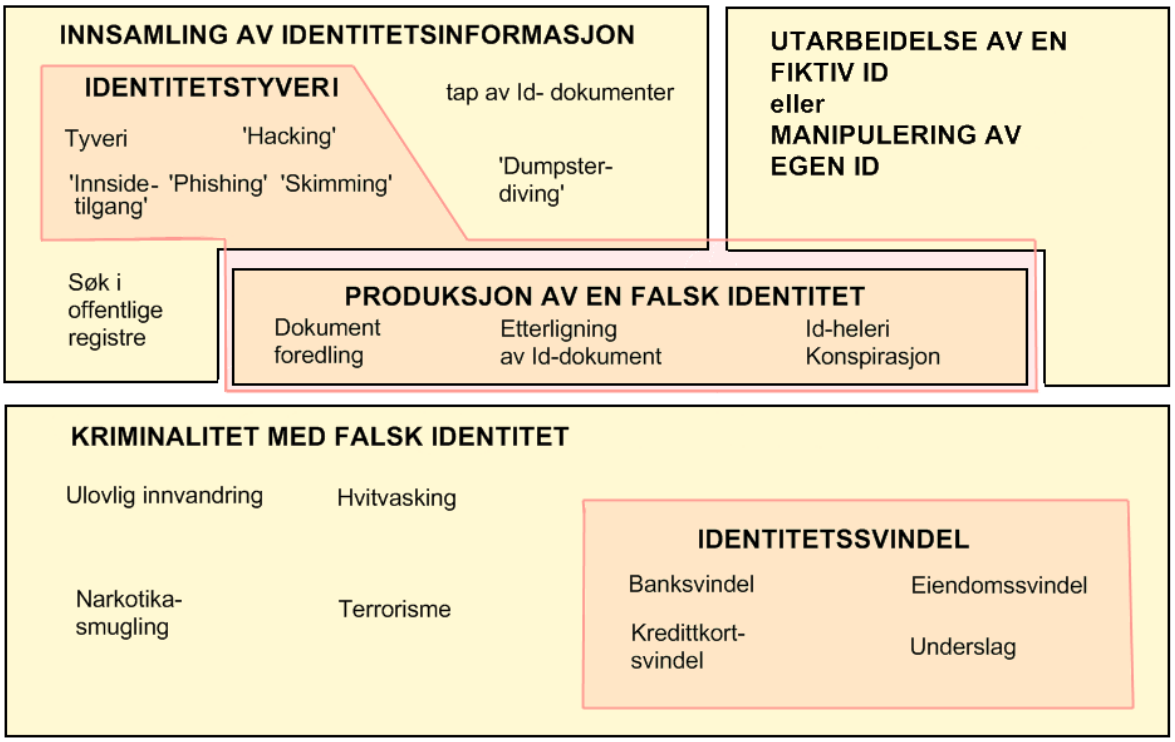
Det finnes mange metoder som var oppdaget per i dag som kriminelle miljøer bruker daglig til å skaffe personligopplysninger om folk. Terje Bjørlo som har over 20 år erfaring fra politi og som jobber i dag som etterforsker hos Lindorff Norge har sakt under ID Tyverikonferanse[7] 2010 at kriminelle miljøer som driver med ID svindel er veldig kreative for å begå svindelen. Han sier også at han vil gjerne ha disse menneskene i eget team for å kjempe mot kriminelle miljøer pga deres kreativitet til å finne ut nye metoder for ulovlig anskaffelse av identitetsinformasjon .

Uansett at det finnes forskjellige metoder for anskaffelse av personligopplysninger vi kan bruke skisse fra CIPPIC[8] som viser trinnene i en prosess ved samling av identitetsinformasjon i diagram 1.

---

7 Idtyverikonferansen Oslo 2010, i regi av NorSis og ID tyveri.info

[8] CIPIC – The Canadian Internet Policy and Public Interest Clinic, University of Ottawa, Faculty of Law



Figur 5-1 CIPPIC 2007

Her vi kan se at hele prosessen ved ulovlig anskaffelse av identitetsinformasjon kan sorteres i 3 hoved trinn.

Innsamling av identitetsinformasjon med metoder som kriminelle miljøer bruker daglig kan variere fra ganske enkelt (stjeling fra postkassa) til avanserte som skimming (kopiering av magnetstriper på kreditt og betalingskort).

5.1. Motivasjon

Kriminalitet med bruk av falske identiteter kan variere i stor skala. Motivasjon kan bli ulovlig innvandring eller narkotika smugler. I de fleste tilfelle motivasjon var økonomisk vinning.

I utgangspunkt bak de fleste saker som vi fant i vårt arbeid motiv bak ID tyveri og ID svindel var økonomisk vinning som motiv. Det er ikke alltid snakk om tyveri av andres identitet. Noen ganger opprettes egne falske identiteter for å utnytte systemene. NAV, Brønnøysundregistrene og Skatteetaten er bare en del av offentlig sektor som har utfordringer på dette område. Ved å benytte en falsk identitet kan en person skaffe forskjellige ytelser fra NAV.

21.02.2009 Oslo Tingrett i sak mot Tina Borg[9] har bestemt å straffe nevnte person i 120 dager i fengsel. Grunnlag er at I perioden 30.08.2001 til 30.04.2006 i Oslo, forledet hun NAV til å utbetale til sammen kr. 661.362,- ved å la sin søster Mikajela Nilsen presentere seg på sykehuset som Tina Borg, for derved å få folkeregistrert barna Romeo Borg og Julia Borg f. 25.10.2001. Hun fremsatte deretter krav om bidragsforskudd, overgangsstønad, barnetrygd, kontantstøtte og fødselsengangsstønad.
Handlingen medførte tap eller fare for tap for NAV med kr. 661.362,-

Ved DNA-test 29. mars 2006 møtte den "ekte" Tina Borg (tiltalte), og hun la da alle kort på bordet og forklarte at tvillingene Julia og Romeo ikke eksisterte. Har vi kan se at det er mulig å skaffe personnummer i Folkeregister uten at personene eksisterer

5.2. Innsamling av identitetsinformasjon

Når det gjelder metoder som brukes ved innsamling av identitetsinformasjon CIPPIC[15] har kategorisert disse metodene i tre grupper. Grupperinger er basert på hvilke metoder er brukt ved ulovlig anskaffelse av data.

Personalopplysningen kan skaffes:

- - Direkte fra offer,
- -Via teknologibasert metoder
- -Socialnetworking/manipulering.

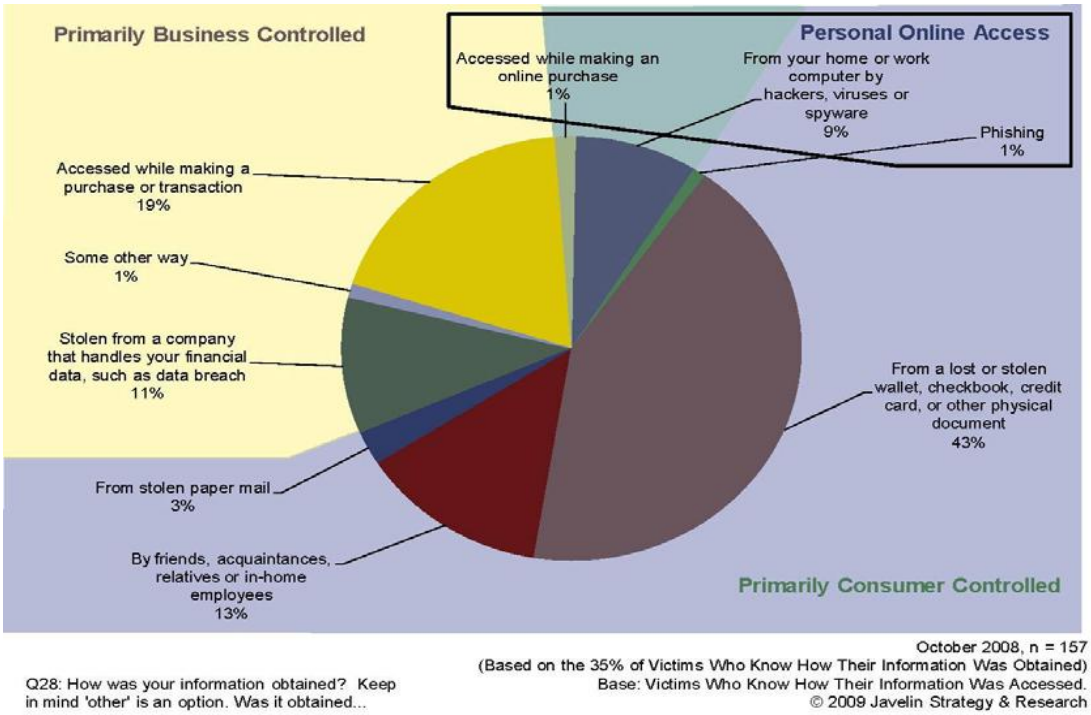
For å forstå forskjell mellom disse metodene vi skal nevne de mest brukte metoder innen var gruppe og vise eksempler slik at vi kan lettere forstå hva foregår bak svindelen.

5.2.1. Direkte fra offer

Denne metoden er den mest brukt metoden ifølge CIPPICsom vi ser i Figure 5-2. Den omfatter følgende:

Tyveri av lommebok, pass, mobiltelefoner, bærbar pc, post fra postkassa med dokumenter som inneholder personligopplysninger (selvangivelsen, skattekort, pass osv) skimming, interne misligheter, kjøp av stjålet informasjon osv.

[9] Oslo Tingrett sak nummer 08-124914MED-OTIR/3



Figur 5-2 CIPPIC 2010

5.2.2. Tyveri fra postkasser

I løpet av den siste tiden har tyveri av kort fra postkasser økt med over 30 % viser tall fra NorSiS[10].

"Vi ser en merkbar økning i ID-tyverier i alle slags former, men det som er skummelt og en gjenganger, er at alle ID-opplysninger er så lett tilgjengelige" sier administrerende direktør Knut Erik Clausen i Affinion International[11].

Hvor mange postkasser ligger rund omkring uten lås. Hvilken tiltak har vi på plass her i landet til å stoppe eller minimisere dette. Hvis vi ser på rutiner ved levering av pass finner vi en skrekk scenario. Ved bestilling av pass i Norge vet vi at vi må levere søknader og bli fotografert på politi stasjon ved personlig oppmøte. Det er ikke likt ved utlevering av pass til oss. Det blir tilsendt til oss via vanlig post å bli levert i vår

[10] NorSiS Norsk senter for informasjonssikring (NorSIS) er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge

[11] Affinion International ASA samarbeider med banker og kortutstedere og bare i Norden betjener selskapet rundt en million brukere

postkasse i konvolutt med størrelse av selve passet. Ved spørsmål om denne rutinen og hvorfor politi bruker ikke rekommandert post som krever personligoppmøte på postkontor slik at vi må legitimere oss før hentining av passet svaret ligger i merutgift på 72 millioner kroner[16]. I same artikkelen vi ser økning av pass som her forsvunnet i postgangen siden 2006. Tabell 5-1 viser trenden, vi ser at i 2010 det er stor økning av pass som her forsvunnet i forhold til 2009

Tabell 5-1 Tapt norsk pass

2006	2007	2008	2009	2010
211	272	253	325	537

Skjerpet ordning finnes nå hos flere banker ved sending av BankID[12] til kundene sine hvor bankene krever personal oppmøte på postkontoret ved gyldig identifikasjon som har hindret tap av bank ID i stor grad.

Det er ikke bare at brevene fra postkassa brukes til å stjele personlige opplysningene som kan misbrukes ved anskaffelse av falske identitetsdokumentasjonene. Vi ser også at postkassa tyveri brukes ved forfalskning av fakturer. I brev fra Forbrukerrådet til Finansnæringens fellesorganisasjon (FNO) står nylig at Bankklagenemnda behandlet en sak hvor en forbruker ble utsatt for svindel på en postsendt faktura (Uttalelse 2010-151)[17].

I korte trekk handler saken om at en forbruker som har mottat en faktura i posten fra en entreprenør. Fakturaen ble fisket ut av postkassen av en svindler som endret kontonummeret, og deretter la forfalsket faktura tilbake i postkassen. Forbruker har så betalt regningen over nettbanken til feil konto og vært i god tro på at oppgjøret gikk riktig for seg. Vi skal ikke gå videre i saken men med dette vil vi vise frem at svindelen som bruker denne metoden for anskaffelse av personligopplysninger kan begynne med enkelt fisking av postkassa.

[12] Bank ID er en personlig og enkel elektronisk legitimasjon for sikker identifisering og signering på nett.

5.2.3. Tyveri vi skimming

Ved direkte anskaffelse av personopplysninger vi må nevne en metode som er ganske kjent i Norge. Metoden heter ”Skimming” og er en fellesbetegnelse for ulovlig kopiering av magnetstriper på kreditt- og betalingskort. Personopplysninger kan kopieres fra magnetstripene ved hjelp av elektronisk utstyr. Vi må nevne at slikt utstyr er lovlig å importere til Norge.

Etter høyesterett fast i domi Agder lagmannsrett (Dato: 2010-12-20 Publisert: LA-2010-190988)[18]da to polakker var tiltalt og domfelt i tingsretten etter straffeløven straffeloven § 186 for oppbevaring av skimmingutstyr på Torp lufthavn. Påtalemyndigheten anket dommen til gunst for de siktede under henvisning til Høyesteretts dom 14. oktober 2010 i HR-2010-1745-A og nedla påstand om frifinnelse under henvisning til dommen i HR-2010-1824-A . Lagmannsretten frifant de siktede for kravet om straff etter straffeprosessloven § 322 første ledd nr. 3 med den begrunnelse at oppbevaring av skimmingutstyr ikke ble rammet av strl. § 186, slik bestemmelsen lød på gjerningstiden. Den gjeldende straffeloven har bare rammet personer som skaffer seg skimmingutstyr som er innkjøpt i Norge. De som har hatt med seg utstyr fra utlandet, har ifølge Høyesterett ikke gjort noe galt.

I pressemelding[19] sier juristminister Knut Storberget at Justisdepartementet ikke var klar over dette hullet i straffeloven, og at de derfor kaster seg rundt for å endre straffeloven § 186 til å omfatte import av denne typen utstyr. Han sier:

”Etter at dommen falt i Høyesterett har det vært svært viktig for meg å få tettet dette hullet i straffeloven raskest mulig. Utstyret har i dag kun et illegalt formål og det er derfor klart at all form for anskaffelse og besittelse av skimmingutstyr må kriminaliseres”

Det vises at det er veldig lettvint å skaffe slik utstyr på internett samtidig med veiledning for å bygge slik utstyr[20]. Pris for en vanlig magnetisk kortleser er ganske lavt og kan skaffes på nettbutikkene rund hele verden[21].

Med slik utstyr som kalles ”skimmers” eller ”wedges” vi skal beskrive prosessen ved ulovlig anskaffelse av data som vises i alle kort som har magnetstripe. Skimming oppstår som oftest i restauranter, hvor eieren mister kontakten med kortet hvis han må gi det til en servitør. Det tar omtrent to sekunder å skanne et kort gjennom en bærbar leser, og leseren registrerer all informasjon som finnes på kortet. Bærbar kortlesere er små nok til at noen lett kan skjule en i lommen, til og med i

hånden sin. I det siste opplever vi at skimmingutstyr blir mer kompleks og i dag kan installeres på minibanken, bensinstasjoner eller i butikker.

I Melding til Stortinget fra Den Kongelige Justis og Politidepartement (Meld.St.7 2010-2011) s.54 står

"Skimming regnes imidlertid ikke som identitetstyveri siden det er betalings formidlings data og ikke persondata gjerningspersonene er ute etter."

Vi kan se at uansett om påstand som står i meldingene, skimming kan brukes også for anskaffelse av data som kan senere misbrukes i en sak om identitetstyveri. I nevnte stortingsmelding står også anbefaling og forslag for endring av straffeloven § 186 og 190a (ny) om skimmingutstyr og ID – krenkelse.

Mens i Norge har vi ikke fortsatt lovverk som kan beskyte oss mot de som åpenbart vil bruke utstyr for skimming for å kopiere data fra folk, andre land kjempes mot skimming på en helt annet måte:

I EUROPOL REVIEW – general Report on Europlactivities[22] vises flere aksjoner over hele Europa for eksampel samarbeid mellom Østerrike, Bulgaria og Polen som resulterte pågripelse av flere personer som hadde fabrikk for produksjon av elektronisk skimming utstyr. s.39. I samme rapport vi kan se at operasjon "Fjord" mellom Payment Card Section, Garda Bureau of Fraud Investigation og IrishCustoms som resulterte pågripelse av en romansk person i Dublin som hadde skimming utstyr hos ham. I rapporten Europol estimerer at skaden ved bare skimming metoden i EU i 2009 er over 350 ,million euro

Identitetstyveri som kan forekomme ved bruk av skimming finnes i Norge. I det siste opplever vi at tyvene som bruker denne metoden bruker mer avansert teknologi ved installering av skimming utstyr på bankautomatene. Vi må passe på hvor vi plasserer fingrene når vi tar ut penger av bankautomater. For ved hjelp av avansert utstyr kan tastetrykk bli nøye overvåket. "Det er ikke lett å se denne", forteller politioverbetjent Janne Stømner ved Sentrum politistasjon.

"Når tyvene i tillegg har plassert en falsk kortleser som kopierer kortet ditt har tyvene alt de trenger for å misbruke kortet ditt", sier hun[23].

Vi ser at utfordringer egentlig ligger i lovverk. Fra dato når noe oppdaget at det finnes en svakhet i straffeloven det tar tid før endringer settes i verk. I mellomtiden utvikler kriminelle miljøer andre og mer avanserte metoder, og i tillegg ser de andre svakhetene som finnes i

dagens lovverk. Det er ikke bare politi som viser at skimming er til stedet i Norge. I siste rapport fra Finanstilsynet Risiko og sårbarhet analyse (ROS) for 2010[24] vises også statistikk fra flere finansinstitusjoner om tapt i kroner ved skimming og generelt tap med svindeltype betalingskort

Tabell 5-2 Svindeltype betalingskort (tapt i hele tusen kroner) (ROC Analyse 2010)

Misbruk av kortinformasjon, kort ikke til stede (internetthandel)	9401
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge 1.765	1765
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	31740
Kort tapt eller stjålet, misbrukt i Norge	14395
Kort tapt eller stjålet, misbrukt utenfor Norge 5.149	5149
Borte i posten 4.239	4239
TOTAL	66689

Det er ikke bare kredit og debit bankkort som skimmes. Alle kortene som har magnetiskstripe kan skimmes. I Norge finner vi en del høyskoler som fortsatt bruker kort med magnetiskstripe, for eksampel Høyskole i Gjøvik, fordelskort fra alle typer boligbyggelag, treningsstudio osv. Noen flyselskaper sender ut flybilletter med magnetstripe som kan skimmes.

5.2.4. Interne misligheter

Interne misligheter er også en metode som brukes til ulovlig henting av personopplysninger. I ROS analyse 2010[25] presenteres en definisjon på hva som er en utro tjener; ”En utro tjener er en medarbeider som misbruker sin tillit eller tilgang til systemer og informasjon. Motivet vil typisk være å utøve skade eller oppnå personlig gevinst.”

I rapporten “Trendrapport 2011 Kriminilitetsuvkilingen i Oslo” som ble publisert av Oslo politidistrikt, januar 2011[26] står også at innsider (utro tjener) som en av de største trusler mot Bank og finansnæring og mot offentlig sektor.

I rapport fra USA skrevet av Collins, JM og Hoffman, S.K[27] viser at nesten 70 % av personopplysninger som er stjålet fra forskjellige bedrifter kommer fra ansatte som jobber i disse firmaene. Disse menneskene har tilgang til personaldata på forskjellige nivåer. De kan få tilgang til dataene via bedriftsdatabaser som inneholder kundeopplysninger, via fakturaer eller via direkte kontakt med kunden. I Canada The Federal Privacy Commissionar gar opplyst om at det største problem når det gjelder identitetstyveri som gjøres via utro tjener er dårlig mangment og dårlig rutiner ved håndtering av forskjellige arkiver og datalagring prosedyrer[28]. Manglende risikovurdering og dårlig intern kontroll er også faktorer som øker risiko for tapping av personalopplysninger.

5.2.5. Kjøp av personligopplysninger

Kjøp av personopplysninger i form av bankkort er en av de metodene for å skaffe ulovlig personalopplysningen. I Press Release from U. S Department of Homeland Security[29] vi kan se at en aksjon mot en cardnetwok resulterte med pågripelse av 28 personer fra 8 forskjellige land. Personer involvert i on-line "carder networking" klarte å kjøpe og selge stjålet personopplysninger. Noen av de gruppene selger blanke kredittkort i tillegg med nødvendige algoritmene som brukes til å dekode informasjon som ligger på kortene.

I Operasjon FIREWALL klarte USA myndighetene å stoppe ulovlig kriminelle virksomhet som forsøkte å selge minst 1.7 millioner stjålet kredittkortnumre. Finansinstitusjon har estimert at faktisk tap knyttet til denne gruppa vær mer enn 4,300,000 dollars, men myndighetene beregnet at tap vil bli enda større hvis de ikke klarte å pågripe hele gruppa.

Symantec Global Internet Security ThreatReport[30] vi kan også se trenden når det gjelder pris som finnes på svart marked eller som Symantec definer som “under ground economy servers”. Disse serverne brukes av kriminelle miljøer for å selge stjålet informasjon, kredittkortnumre, personlige identifikasjonsnumre (PIN-koder) og e-postadresselister. Tabell 5-3 viser pris på forskjellige typer dokumenter som finnes hos kriminelle miljøer i verden.

Tabell 5-3 Pris på forskjellige typer dokumenter hos underground economy servers (Symantec Global Internet Security ThreatReport 2011)

Overall Rank 2009	2008	Iteam	Percentage 2009	2008	Range of Prices
1	1	Credit cardinformation	19%	32%	$0,85-$30
2	2	Bank Accountcredentials	19%	19%	$15-$850
3	3	Email accounts	7%	5%	$1-$20
4	4	Email adresses	7%	5%	$1,70/MB-$15/MB
5	9	Shell scripts	6%	3%	$2-$5
6	6	Full identities	5%	4%	$0,70-$20
7	13	Credit card dumps	5%	2%	$4-$150
8	7	Mailers	4%	3%	$4-$10
9	8	Cash-outservicies	4%	3%	$0-$600 plus50%-60%
10	12	Web site administration credentials	4%	3%	$2-$30

I rapporten står at trenden viser en nedgang men de påstår at dette blir et voksende problem. Grunnen til at de kommer med en slik påstand er at per i dag det finnes ganske tilgjengelig "crimewarekits" som er veldig enkelt å bruke og som ikke krever veldig mye kunnskap om teknologi som kriminelle grupper bruker. Da blir lettere for "vanlig" kriminelle å prøve med denne type kriminalitet.

5.2.6. Personalopplysning lekkasjer fra offentlig og privat sektor

Pga effektiviteten og med ønske og gi bedre service til sine innbyggere alle statlige og offentlige organer krever til papirløs samfunn. Det er bare over 880 forskjellige skjemaer som finnes på Altinn[13]. I

[13] Altinn er en nettportal og en teknisk plattform for å levere elektroniske skjemaer til det offentlige, men tilbyr også andre elektroniske tjenester, som meldinger fra det offentlige og innsynstjenester i offentlige registre.

Etatsbrosjyre[31] kan vi se tallene som viser at det er en stor økning av bruk av elektronisk skjema på Altinn med 23 millioner skjema som har passert Altinn siden 2004.

Vi ser at elektronisk dialog med innbyggere og med bedrifter viser kostnader gevinst og ikke minst effektiviteten med innrapportering til offentlig. På andre side elektronisk innrapportering og bruk av elektroniske veier kan koste enkelte ganske mye hvis rutinene og ikke minst implementering av disse rutinene er ikke på plass. Det finnes mange eksampler fra hele verden hvor befolkning har oppdaget at personopplysninger om de har slippet ut på internett ukontrollert.

Washigton Post har skrevet i en artikkel om publisering av stor mengde av personopplysninger på internett[32]. Her i Norge har vi også eksempler på hvor stor mengde av data var publisert hos flere norske redaksjoner, i Norge vært år sendes norske skattelister til flere norske redaksjoner som viser hvor mye enkelte av oss har tjent i siste år og hvor mye vi har betalt i skatt. I 2008 fikk redaksjonene litt mer data en vanlig. Med en feil i systemet på listene som inneholder opplysningene om hvor mye de enkelte hat tjent, kommet også personnummer til hver enkelt skattyter[33].

Det var stor diskusjon om dette burde være lovlig. I utgangspunktet har ligningsmyndighetene taushetsplikt om skattyterens forhold. Her i Norge finner vi enestående unntak og det er lovbestemt norske offentliggjøringen av skattelistene. I følge ligningsloven § 8-8 hvor det står:

"Skattelisten skal inneholde den enkelte skattyters navn, postnummer, poststed, fødselsår for personlig skattyter, organisasjonsnummer for upersonlig skattyter, den fastsatte nettoformue og nettoinntekt, skatter og avgifter. Skattelisten skal ikke inneholde opplysninger om personer med adresse som er sperret i henhold til bestemmelse gitt i eller i medhold av lov om folkeregistrering av 16. januar 1970 nr. 1, opplysninger om personer uten fast bopel og opplysninger om personer der opplysningene som inngår i skattelisten kan røpe et klientforhold.

Fullstendige skattelister kan utleveres i elektronisk form til pressen. Det kan kreves betaling ved utlevering av skattelister."

I siste setning ser vi at skattelistene kan utlevers i elektronisk form til pressen noe som medføre at listene er tilgjengelige hele året i nettavisene.

Enda verre er det at per i dag det er umulig å reservere seg mot å stå i skattelisten som skal offentliggjøres. Elektronisk samling av data er ganske enkelt nå. Skattelistene ble tilgjengelig på internett første gang i 2001.

I Stortingsbehandling i 2003-2004[34] ble masseutlevering opphørt og da alle opplysningene om gateadresse og fødselsdag var fjernet men i 2007 i Stortingsbehandling i 2006-2007[35]masseutlevering til pressen var gjeninnført. Loven var endret slik at tilgang til den elektroniske listen var kun tilgjengelig 3 uker på Skatteetatens nettsider akkurat som står i ligningsloven § 8-8. Det står ikke sær regler for pressen og derfor de listene i elektronisk form er alltid offentlig tilgjengelig. Det er flere som sier at dette kan misbrukes. Til og med det finnes i dag nettsiden "www.neitilskattelister.no" som viser bekymringer til dagens ordning som viser skattelistene på flere nettsider. Politi har ikke direkte bevis at offentliggjøring av skattelistene har direkte knytning mot kriminaliteten i stor utstrekning[36]men de sier:

"POD kan på grunnlag av de foreliggende opplysningene ikke se at det er grunnlag for å anta at informasjons innhenting fra skattelistene benyttes i stor utstrekning. Det er midlertidig grunn til å rette oppmerksomhet mot at vi har erfart noen få alvorlige enkelteksempler, og at informasjon fra skattelistene er ytterligere ett virkemiddel til bruk for innhenting av informasjon om aktuelle ofre for kriminalitet"

Politidirektoratet også påpeker i en pressmelding[37] at

"Gjennomgangen indikerer at det er sannsynlig at skattelistene anvendes for målretting av ulike former for kriminalitet som ran, trusler, tyverier og bedrageri"

Hvert år nordmann for tilsendt selvangivelsen fra skatteetaten. Det er en gullgruve for Id-tyver Datatilsynet i en pressmelding til TV2[38]. I samme pressemelding sier de at nesten 4 million nordmenn vil få tilsendt forhåndsutfylte selvangivelsene som er fulle av personopplysninger. Det bekymrer Datatilsynet:

"En av de viktigste ingrediensene i et id-tyveri er personopplysninger, så sånn sett er selvangivelsen et attraktivt dokument for id-tyver", sier direktør Bjørn Erik Thon i Datatilsynet

Siste lekkasje fra offentlig sektor ser vi i NRK sin artikkel om svakhet i NAV sitt system[39]. Det står at NAV sender over 2 million brev til sine brukere hver måned hvor de på forsiden av konvolutt står strekkode med personopplysninger om brukeren. Med ganske lett tilgjengelig

programvarene som kan lastes ned fra internett å installeres på mobil telefon klarte reporter fra NRK til å lese strekkode som står på fremsiden av konvolutten. Der står fødselsnummeret til personen i rekkefølge som er ganske enkelt til å lesse.

5.3. Teknologibasert Metoder

Teknologibaserte metoder bruker mer datasystemer for å svindle folk. Det finnes forskjellige metoder som svindlerne bruker. De mest kjent er: phishing, spionvare, viruser, forskjellige malware type som, backdoors, keyloggers, misbruk av informasjon som finnes i kastet datamaskiner osv. I følge rapporten fra Finanstilsynet "Risiko og sårbarhetsanalyse (ROS) 2010" finansbransjen rapporterer om økende trusselnivå innenfor internettkriminalitet. I en studie fra Hewlett Packard "Cyber Security Readiness"[40] vi kan lese at 56 % foretak i USA og 38 % av europeiske foretak mener at de har vært utsatt for et cyberangrep. Amerikanske og europeiske organisasjonene deler bekymring at et cyberangrep i vesentlig grad vil påvirke kritisk nasjonal infrastruktur i de nærmeste to årene. De fleste konkluderer også at cyberangrep er vanskelige å oppdage (88,5 %), ikke lar seg rette opp raskt (86,5%) og at det ikke eksisterer gode mottiltak mot slike (82,5 %). I dette kapitel vil skal beskrive litt nøyere phishing men de andre metodene vi skal bare nevne slik at leseren har forståelse at via disse metodene det er også mulig å miste verdifulle personaldata.

5.3.1. Phishing

"Phishing eller nettfiske er en betegnelse på digital snoking eller fisking etter sensitiv informasjon, som passord eller kredittkortnummer. Uttrykket kommer fra engelsk «fishing», der f-en er erstattet med «ph» (vanlig hackersjargong)"[14].

Vi kan også si at det er en blanding av to metoder: metoder som bruker teknologi og sosial networking eller manipulering. Svindel har med mål å presentere seg som en annen person, bedrift eller offentlig etat. Ved hjelp av slik metode kan man skrive inn personopplysninger som fødselsnummer, kontonummer, pin koder osv. De finnes forskjellige phishing varianter men en typisk phishing scenario er slik:

[14] http://no.wikipedia.org/wiki/Phishing

Svindleren sender e-post som ser legitimt ut. E-post inkluderer firma sitt logo, har informasjon som navn, adresse, telefonnummer til kundesenteret osv akkurat likt som virkelig bedrift. I selve e-posten de krever at kundene må verifisere opplysningene sine ved å svare på e-post eller å klikke på linken som skal vise web siden som ligner på virkelig bedrifts web siden hvor de kan "tryggere" skrive personalopplysningene.

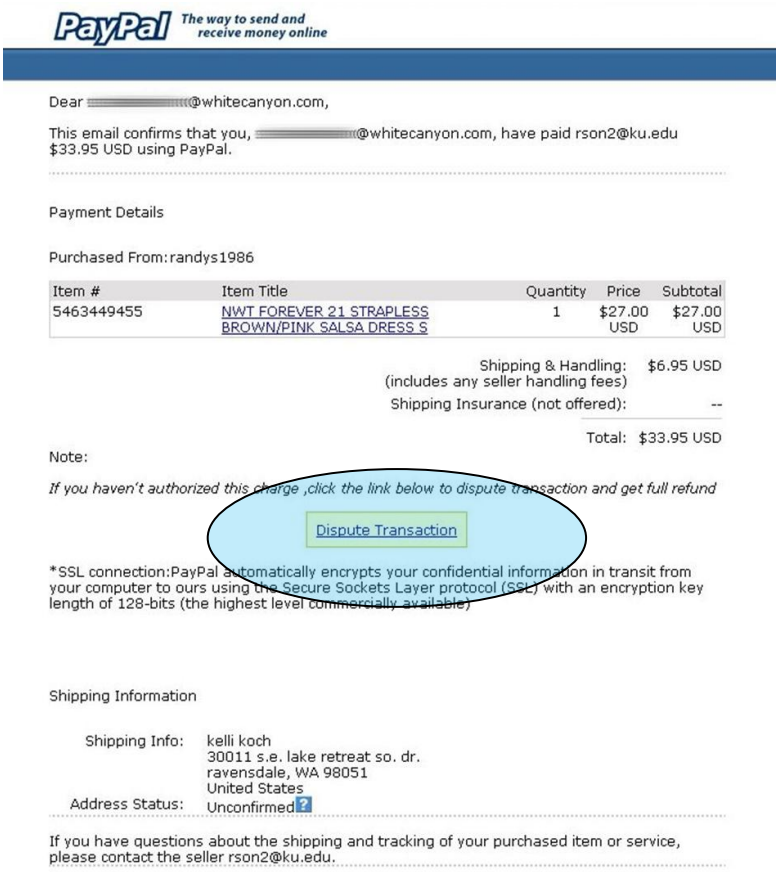
De fleste falske e-poster utgir seg som e-post fra nettbank eller en kjent betalings web servise, for eksempel PayPal. I eksempel som vi skal vise dere ser vi en falsk e-post som ligner på vanlig epost fra PayPal som viser konfirmasjon av en fullførte transaksjon. Selvfølgelig, selve transaksjon var falsk og offeret får mulighet til å klikke på linken som vil kansellere transaksjon og få pengene tilbake. Ved klikking på linken som står i e-posten risiko for å bli infisert med en ond kode øker kraftig. Selve falsk URL[15] var nesten perfekt:

Reel URL: https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Falsk URL: https://www.paypal.com.dllsll2.us/icmd=_login-submit.htm

For vanlig internett brukeren der er nesten umulig å se forskjell.

[15] Uniform Resource Locator- En URL-adresse er en unik adresse for en fil på Internett. Dette betyr at URL-adresser eksempelvis kan inneholde en ressurs, for eksempel en webside, et bilde eller en lydfil. Microsoft.com



PayPal The way to send and receive money online

Dear [redacted]@whitecanyon.com,

This email confirms that you, [redacted]@whitecanyon.com, have paid rson2@ku.edu $33.95 USD using PayPal.

Payment Details

Purchased From: randys1986

Item #	Item Title	Quantity	Price	Subtotal
5463449455	NWT FOREVER 21 STRAPLESS BROWN/PINK SALSA DRESS S	1	$27.00 USD	$27.00 USD

Shipping & Handling: (includes any seller handling fees) $6.95 USD
Shipping Insurance (not offered): --
Total: $33.95 USD

Note:

If you haven't authorized this charge ,click the link below to dispute transaction and get full refund

Dispute Transaction

*SSL connection:PayPal automatically encrypts your confidential information in transit from your computer to ours using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available)

Shipping Information

Shipping Info: kelli koch
30011 s.e. lake retreat so. dr.
ravensdale, WA 98051
United States
Address Status: Unconfirmed

If you have questions about the shipping and tracking of your purchased item or service, please contact the seller rson2@ku.edu.

Figur 5-3 Bilde og url adresser hentet ut fra PayPal web siden

Det samme opplevde DnB NOR i 2007 da mange kundene i DnB NOR fikk e-post som var godt utformet, med påstand at banken har problemer med en av sine databaser og trenger derfor at kundene oppdaterer kontoinformasjon. Heldigvis alle bankene i Norge har såkalt tofaktor[16] autorisering og skadene var ikke store.

Ved klikk på linken i e-post som svindleren har sendt til offeret kan oppleves en mer avansert form av phishing som kan gjøres at svindleren kan endre hostsfilen[17] på offeret sitt datamaskin. Hostsfilen blir ofte også forandret på av spionprogrammer, eller spyware.

[16] Autorisering hvor man har et brukernavn, et passord og i tillegg en nøkkel som genereres hver eneste gang man logger seg på nettbanken

[17] Hosts-filen er en datafil som brukes i et operativsystem for mapping vertsnavn til IP-adresser

Hostsfilen er en svakhet i dagens nettlesere og operativsystem, og som lett kan utnyttes av datakyndige kriminellere. Kriminelle miljøer kan gå inn på offer sitt datamaskin via nettet, koble seg inn i maskinens egen hostsfil, og overstyre IP-adresser. Nettleseren sjekker først med operativsystemet, som så spør Hostsfilen på datamaskinen, før den spør navnetjeneren ute på nettet. Det egentlig betyr at offer kan i god tro skrive inn www.nettbank.no i sin nettleser, men vil ikke komme til dette stede men til IP–adressen de datakriminelle vil som i utgangspunktet ligner som banken legitimt web siden. På denne måte kan de skaffe personalopplysninger om offeret og misbruke den videre.

Phishing-trenden i verden økte i siste halvpart av 2010, viser rapport "Global Phishing Survey 2H2010 [41]".Phishing-angrepene økte til 67 677 i løpet av siste halvdel av 2010, opp fra 48 244 i første halvår i fjor.

De påpeker at phishere også liker å fiske etter online legitimasjon av de som spiller online-spill, hovedsakelig World of Warcraft og Battle.net. De fleste legitimasjonene ble solgt på det svarte markedet.

Phishing-angrepets oppetid er avgjørende fordi jo lengre et phishing-angrep varer, jo større sannsynlighet er det for tap for offeret. Med offer menes privatpersoner, bedrifter eller offentlig institusjoner. Rapporten viser en gjennomsnittelig oppetid på 72 timer, noe som er "den lengste gjennomsnitt siden vi begynte våre målinger tre år siden," sier Rod Rasmussen, som er en del av teamet som har skrevet rapporten og som forklarer at de to første dagene av et phishing-angrep antas å være de mest lukrative for phisheren, så rask nedetid er avgjørende.

Det er ikke bare eposter som brukes for å svindle folk. Eksempler fra svindel ved bruk av sms er kjent her i Norge. Anne Dybo fra Økokrim opplyser[18] at det finnes et eksempel hvor en nordmann fikk en sms som var sendt fra et norsk telefonnummer med følgende tekst:

"Gratulerer! Mobilnummeret ditt har vunnet sum av £ 750.000 pounds i Nokia Mobile Promo 2010. E-post cole.nokia@ymail.com eller ring +447020486851"

Hvis offeret ringer dette telefonnumeret blir kontoen belastes med et stort beløp.

[18] Identitetstyveri konferanse (Oslo 2010)

5.3.2. Spionvare (spyware)

"Spionvare er programvare i form av ondsinnet kode (malware) som installeres (ofte skjult) på en datamaskin for å overvåke brukerens interaksjon med datamaskinen, uten at det foreligger informert samtykke til dette fra brukerens side"[19]. Disse programmer i utgangspunkt klarer å samle informasjon fra offeret sitt datamaskin om web sider som offeret bruker mest. Slik informasjon selges til reklamebyråer som bruker det til å sende uønsket reklamer til offeret. Andre typer av spionvarer brukes for innhenting av personlig informasjon som bruker for identitetstyveri eller svindel. Key loggers er en av dem. Med en slik spionvare som er ulovlig installert på offers sin datamaskin klarer svindlere å lagre og for tilsendt alt offeret gjør via tastatur. Trojansk hest er også en tipisk spionvare som er selvstartende program som kan slette innhold på offeret sitt datamaskin, de kan legge datamaskin til bot nettverk. I Risiko – og sårbarhetsanalyse 2010 de definerer et slikt nettverk som en type ondsinnet kode som gir angriperen mulighet til å ha kontroll over datamaskinen. De er som regel en del av et helt nettverk av infiserte maskiner, som er ofte skapt av infiserte maskinen fra hele verden. Kontrollsenteret i botnettet klarer å overvåke hele netverket online slik at de kan logger seg inn som kunden i nettbanken snart de for stjålet påloggingsdata.

5.4. Socialnetworking / manipulering

Sosial media Social networking presenterer egentlig en internettapplikasjon som gir brukeren mulighet til å kommunisere sammen via internett. For å delta i kommunikasjonen må brukeren logge seg inn på selve applikasjonen med personlige informasjonsprofiler. Selve profilen inneholder forskjellig informasjon som kan være tekst, bilde, lyd osv. Kommunisering i selve applikasjonen kan foregå via chat, e-post osv. De største og mest berømte applikasjonene er Facebook og My space [42] . I følge facebook.com[43] 2010 var 2010 et godt år for sosiale medier. Alle velkjente internett applikasjoner som driver med sosial networking viser vekst i antall brukere. Dette kan vi se i tabellen 5-4:

[19] http://no.wikipedia.org/wiki/Spionprogramvare

Tabell 5-4Antall registrert brukere (Facebook.com 2011)

	2010	2011
Twitter	75 millioner	175 millioner
Linkedin	50 millioner	100 millioner
Facebook	350 millioner	640 millioner

Med et så stort antall av brukere som deler informasjon via disse kanalene er det grunn til å anta at det skjer lekkasjer eller misbruk av informasjoner som publiseres på disse nettstedene. I 2008 i Storbritannia var det en rettsak: Matthew Firsht v Grant Raphael [44].

I 2008, Raphael kopierte materiale fra Facebook-siden til hans tidligere venn, Matthew Firsht, og opprettet en ny profil på Facebook med informasjon om Firsht. På denne klonede siden, oppførte Raphael Firsht sine seksuelle preferanser som "Looking for what I can get " og meldte seg på gruppen "Gay-jøder i London". Han skapte også en gruppe med navnet "Har Matthew Firsht løyet til deg?" angivelig for personer som Matthew Firsht skyldte penger til og løy om når han ville betale. Den klonede siden var på Facebook i 17 dager før Firsht ble oppmerksom på den. Han klarte med hjelp av Facebook-teamet å fjerne siden og måtte få søk ordre fra Domstolen som krever at Facebook må gi informasjon om e-postadressen til personen som har registret profilen og IP-adressene til datamaskinene som var i bruk i prosessen. Informasjonen pekte direkte til Raphael, som forvarte seg med en påstand om at noen andre kunne ha brukt hans bærbare PC i sin leilighet (flere ganger) og opprettet den falske profilen og gruppene. Dommeren fant forsvaret å være helt usannsynlig og tildelte Firsht 250 000 kr. i erstatning for ærekrenkelse og brudd på personvernet.

Det er ikke bare personopplysninger som kan misbrukes via nettsamfunnet. En artikkel i Aftenbladet[45]20 beskriver hvordan Israelske styrker måtte avlyse et planlagt angrep i Vestbredden fordi en israelsk soldat hadde opplyst detaljene om angrepet på facebook-profilen sin.

[20] Aftenposten

Slettmeg.no er et nettsted i regi av Datatilsynet som hjelper mennesker med å fjerne opplysningene sine fra internett. Slettmeg.no har i 2010 håndtert til sammen 3236 henvendelser via e-post, telefon, kontaktskjema og chat. Det er forskjellige årsaker til hvorfor folk vil slette opplysninger som finnes på internett, men vi har sjekket hvor mange henvendelser som gjelder identitetstyveri og sletting av falske identiteter som finnes i nettsamfunnet.

Slettmeg.no ser at det finnes 2 grupper henvendelser som har som mål å forfalske eller misbruke identiteter som opprettes på nettsamfunnet. Oppretting av falske profiler med opplysninger fra et annet menneske uten tillatelse og hacking av en annens persons profil.

Falske profiler står for 7 prosent av alle henvendelser.

Tabell 5-5 Oppreting av falske profiler fordelt på nettsider (Slettmeg.no 2011)

Facebook:	168	(72 %)
VG Nettby:	7	(3 %)
MSN:	5	(2 %)
Deiligst.no:	4	(1 %)
Penest.no:	3	(1 %)
Blogger.com	3	(1 %)
Myspace:	3	(1 %)
Blogg.no:	2	(1 %)
Hotmail:	2	(1 %)
Twitter:	2	(1 %)
Match.com:	2	(1 %)
LinkedIn:	2	(1 %)
Firstdate.com:	2	(1 %)
Windows Live Spaces:	2	(1 %)
Andre:	25	(12 %)
TOTAL:	232	

Når det gjelder hacking av profiler vi ser at hacking står for 5 prosent av alle henvendelser.

Tabell 5-6 Nettsteder som var involvert i hackede kontoer/profiler (Slettmeg.no 2011)

Facebook:	70	(44 %)
Hotmail:	64	(40 %)
Gmail:	6	(4 %)
MSN:	4	(3 %)
Yahoo:	3	(2 %)
VG Nettby:	3	(2 %)
Windows Live:	3	(2 %)
Blogger.com:	1	(1 %)
Zinga Poker (FB applikasjon)	1	(1 %)
Blogg.no:	1	(1 %)
Formspring.me	1	(1 %)
Uspesifiserte sider:	2	(1 %)

6. **Hvor lett er å miste identitet**

Andre forskningsspørsmål som vi skal prøve å forklare er hvor effektive metodene som svindlerne ofte bruker for å skaffe personopplysninger fra offeret er.

Før eksistensen av kredittkort og internett, begrenset identitetstyverier seg til tyveri av kasserte dokumenter i håp om å finne et dokument som inneholder identitetsopplysninger.

Nå til dags med daglig bruk av Internett og økt bruk av web-basert handling via nettbank, har identitetstyveriene tatt en annen retning.

Det ser ut til at det var vanskeligere å begå identitetstyveri tidligere. Før internett måtte tyven aktivt forfølge offeret for å finne en måte å stjele dennes identitet, og da måtte de direkte lyve for flere personer for å få noen form for gevinst. Vi kan si at identitetstyveri ikke ble utført så ofte på grunn av fraværet av datamaskiner. I de siste 20 år har vi opplevd en økt av bruk av datamaskiner over hele verden. Resultatet av dette er at mer og mer informasjon blir lagret digitalt, og flere og flere transaksjoner kan utføres helt uten menneskelig kontakt. En identitetstyv trenger ikke lenger nødvendigvis å snakke med en person for å begå forbrytelsen, tyven kan nå gjøre det ved å stjele personalia fra nettet. De trenger ikke å kjenne til offeret personlig for å utnytte denne identiteten. Det eneste de trenger å vite står i et stjålet bankkort eller i en annet dokument som inneholder personopplysninger. Med slik informasjon kan de bestille forskjellige falske dokumenter på nettet. Disse kan misbrukes senere. Vi skal prøve å beskrive hvor enkelt det er å bestille disse falske dokumentene fra internett i et case scenario.

I en undersøkelse [46]fra TNS Gallup på vegne av bestilling fra NorSiS prøvde de å sjekke hvor høy prosent av befolkning som er blitt utsatt for identitetstyveri de siste to årene. Intervjuene har blitt gjennomført via TNS-Gallups Catiavdeling via telefonintervju. Spørsmålene har blitt stilt til et representativt utvalg på 2000 respondenter. Definisjonen som ble brukt er denne undersøkelsen var:

"Identitetskrenkelse er uberettiget bruk av både stjålet og fiktiv identitet, med forsett om å oppnå en økonomisk vinning for seg

eller andre, eller å påføre tap eller ulempe for andre. Har du I LØPET AV DE SISTE 2 ÅRENE blitt utsatt for at noen andre harbrukt din identitet til å begå slike straffbare handlinger?"

Andelsom svarte JA på dette spørsmålet var 3,1 %. SSB[21] 22 i deres befolkningsstatistikk per 01.01.201023 viser at i Norge bor det nesten 4.9 millioner mennesker hvorav 3,9 million er eldre en 16 år. Hvis vi bruker tall fra et representativt utvalg kan vi anslå at 124 000 nordmenn har vært utsatt for identitetstyveri i løpet av de siste to årene. Dette er et antall personer som tilsvarer innbyggertallet i hele Stavanger by.

For å illustrere hvor lettvint det er å miste identitetsopplysninger kan vi se på tallene fra en identitetstyveriutstiling i regi av NorSIS.

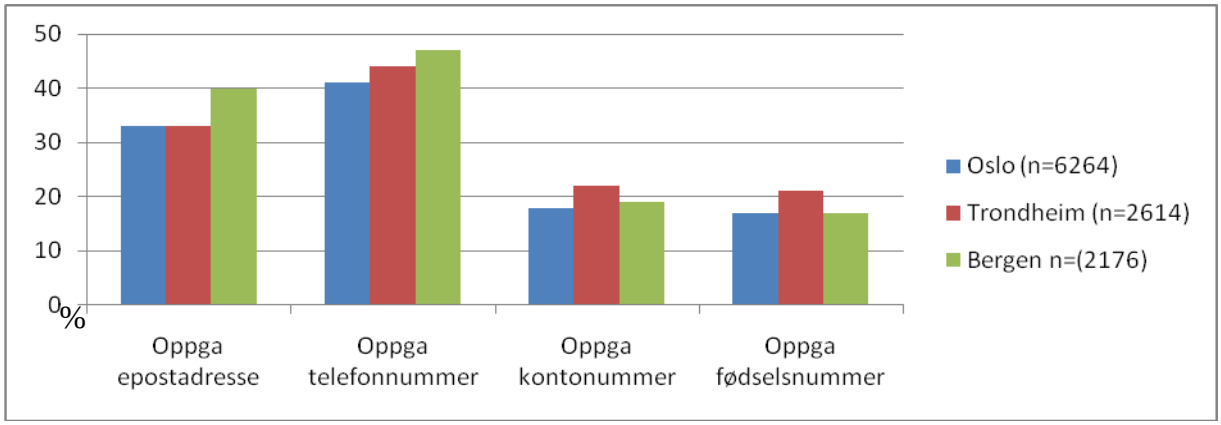
Sammen med Norsk Teknisk Museum installerte NorSIS en skjerm med teksten "Vinn en Ipod". Alle de som viste interesse for å vinne en iPod måtte besvare noen enkle spørsmål. Etter å ha besvart disse spørsmålene fikk de tilbud om å få vite om de hadde vunnet iPod'en. Det eneste de måtte gjøre på slutten var å oppgi noen personopplysninger. Informasjonen de skulle registrere var e-postadresse, telefonnummer, kontonummer og fødselsnummer. Etter at de hadde fylt inn personopplysningene kommer beskjeden: "Du har blitt lurt! Dette var ikke en konkurranse, men en test på hvor langt du er villig til å gå for å kunne vinne en iPod. Alle personopplysningene du har fylt inn kan misbrukes av Id-tyver."

Til slutt fikk de vite hvor mange andre som har latt seg lure og at de kanskje burde være mer forsiktige med hvor de oppgir sine personopplysninger i fremtiden.

[21] – Statistisk Sentralbyrå

[22]SSB – Statistisk Sentralbyrå

[23]http://www.ssb.no/folkemengde/tab-2010-03-11-01.html



Figur 6-1 Antall personer som har oppgitt person informasjon (NORSIS 2010)

Ved kombinering og misbruk av flere typer av data som e-post, telefonnummer, kontonummer eller fødselsnummer kan tyven finne en lettere vei til å utnytte noen.

Dataene viser at det folk lettere gir fra seg opplysninger om e-post og telefonnummer enn kontonummer og fødselsnummer.

Dette forteller oss at de attributtene som er lett å endre, som e-post (alle kan åpne e-post konto når som helst) telefonnummer (som er veldig lett å endre), gir et falskt inntrykk av at denne informasjonen er ikke så viktig og at ingen trenger å stjele denne typen informasjon. Når det gjelder fødselsnummer viser tallmaterialet at folk er mer forsiktig å dele denne type av informasjon. Det betyr at folk anser dette attributtet som personlig. Dette gjelder også kontonummer fordi kontonummer er en direkte link til pengene våre.

De aller fleste av respondentene trodde ikke på viktigheten av å beskytte sitt telefonnummer. De glemmer at det er veldig enkelt å sjekke på nett gjennom ulike web sider som gulesider.no eller 1881.no, og så på opplysningene om telefonummerseieren, adresse og i de fleste tilfeller et bilde av huset hvor eieren bor og eventuelt bilde av postkasse hvor eieren mottar post. Hvis man går videre, via skattelister som er distribuert via forskjellige nettsider, kan tyven se personens inntekt og dermed klassifisere og gjøre valg av ofre. Via Brreg.no tyven kan sjekke om telefoneier har et foretak registrert i Norge osv. Bare et telefonnummer kan bli potensielt farlig parameter som tyven kan bruke mens de driver med identitetstyveri.

Hva skjer hvis noe misbruker vår identitet? I første omgang vi kan konkludere med at det koster penger, tid og ikke minst går ut over

helsen når vi opplever at noe har brukt vår identitet uten at vi vet om det.

For å vise hvor ubehagelig det er når vi oppdager at vi har vært ofre for identitetstyveri kan vi se på et eksempel hvor en av våre medborgere hadde blitt utsatt for identitetstyveri. Notatet som vi skal vise her er hentet fra NORSIS. Av hensyn til personvernet skal vi ikke oppgi det rette navnet til person og hans bosted.

Ola Normann ble utsatt for at noen misbrukte hans identitet, og det er ikke noe han tenker tilbake på med lystige tanker. Det hele startet tidlig i 2002. Personen som gjorde det hele var ikke spesielt datakyndig. Ola følte seg som en idiot, og det hele ble ikke bedre når politimannen som tok i mot anmeldelsen ikke helt trodde dette var mulig. Hans argument var "Det er ikke mulig å få tak i en annen persons fødselsnummer". Ergo, det var offeret selv som var den mistenkte i starten. Svindleren klarte å lure til seg nesten 150 000 kroner i diverse lån i offerets navn, samt mobiltelefon og abonnement hos Telenor, og et hi-fi anlegg fra Thorn med mer. Han prøvde også å omadressere posten til en postboksadresse i Sarpsborg. Ola bodde i Oslo på den tiden. Omadresseringen fikk han avverget siden Posten var så snille og sendte ut et bekreftelsesbrev hvor det sto: "Takk for at du benytter deg av Postens tjenester", og da med en bekreftelse på til og fra dato. Litt seinere viste det seg at svindleren hadde gjort dette fordi han hadde bestilt gebyrfritt Visa kort som skulle sendes i posten.

Men hvordan fikk svindleren tak i Olas personopplysninger?

Han hadde fått tak i opplysninger fra noen separasjonspapirer i forbindelse med et samlivsbrudd og han var heller ikke spesielt begavet i databruk. Men han klarte det; og man kan jo stille seg spørsmålet om hvordan han kunne få til noe slikt? I følge Ronny handlet det i stor grad om dårlig håndverk og sviktende sikkerhetsprosedyrer i alle de sakene hvor hans identitet var innblandet. Det er overraskende hvor slurvete folk er med slike ting. Det var tydeligvis ingen som gjennomførte kontroll av de opplysningene vedkommende hadde oppgitt i lånesøknader, informasjon som dessuten var feil. Uttak av mobiltelefon og nummer var gjort uten at han hadde framvist identifikasjonspapirer. Det som virkelig er slitsomt i slike saker er når kredittsjekkbrevene strømmer på og man hele tiden må følge opp.

Angsten handler om de tingene du ikke vet om du i det hele tatt vil oppdage. Angsten er også et resultat av redselen for ikke å bli trodd.

For Ola ble dette en lang kamp mot låneinstitusjoner og politi, og en angst som stadig ble større når han skulle sjekke postkassa. Nå var ikke Olas identitet den eneste som vedkommende svindler misbrukte. Han ble til slutt tatt, og fikk faktisk en dom på 18 måneder. Men betyr det at han ikke lenger har tilgang til ofrenes personopplysninger?

Det er nå gått syv år siden denne saken, men den dag i dag føler Ola fysisk ubehag ved å oppdage konvolutter med ukjent avsender i sin egen postkasse.

Det skal ikke mye til for å miste identitet eller en deler av den, men det tar veldig mye tid til å reparere skadene. I enkelte tilfeller vi kan konkludere at dersom vi en gang mister identiteten kan vi aldri bli hundre prosent sikre på at det ikke vil skje igjen.

7. **Identitet i Norge**

Førerkort, pass, bankkort, det er de vanligste identifikasjonsbevis som vi bruker her i Norge. I alle de bevisene står en unik identifikator som viser hvem vi er. Det er personnummer med 11 siffer og bilde av oss. En annet unik identifikator som viser også hvem vi er organisasjonsnummer. Det viser ikke hvem vi er personlig men viser hvilken bedrift vi sier at vi representerer. Samtidig ved å presentere organisasjonsnummer vi presenter også en rekke informasjon om bedrift. Navn av daglig leder eller eieren, adresse hvor virksomhet befinner seg, hvilken næring de driver med osv. Alt i alt disse informasjonene er også potensiell led ved skaffelse av data som kan misbrukes av kriminelle miljø.

7.1. Fødselsnummer

I forskriften FOR 2007-11-09 nr 1268: Forskrift om folkeregistrering, finnes reglene hva må registreres ved oppretting av fødselsnummer. I paragraf 2-2 vi kan se de tekniske spesifikasjonene ved opprettelse fødselsnummer samtidig hvem og i hvilke tilfelle fødselsnummer kan endres.

Fødselsnummeret skal ha elleve siffer. De seks første siffer består av vedkommendes fødselsdato i rekkefølge to siffer for dag, to for måned, to for år. De fem siste siffer, personnummeret, består av tre individsiffer og to kontrollsiffer.

Kvinner skal ha like tall og menn ulike tall som siste individsiffer.

Fødselsnummeret tildeles i Det sentrale folkeregister og administreres av Skattedirektoratet.

Fødselsnummeret kan endres når fødselsdato eller kjønnsstatus endres.

Fødselsnummeret kan også endres når Politidirektoratet med hjemmel i politiloven § 14b har gitt tillatelse til bruk av fingerte personopplysninger. Skattedirektoratet fastsetter i instruks nærmere regler for utfylling og gjennomføring av denne bestemmelse.

I paragraf § 2-3. står om fastsettelse av fødselsdato:

"For personer som fødes i Norge fastsettes fødselsdatoen på grunnlag av fødselsmeldingen, jf. § 3-1 nr. 1.

For personer som innvandrer og som tidligere har vært registrert som bosatt i Norge, fastsettes fødselsdatoen på grunnlag av det som allerede er registrert i Det sentrale folkeregister.

For personer som innvandrer og som tidligere ikke har vært registrert som bosatt i Norge, fastsettes fødselsdatoen på grunnlag av vedkommendes pass eller tilsvarende legitimasjonsdokument når det gjelder de som ikke trenger oppholdstillatelse.

For de som trenger oppholdstillatelse, fastsettes fødselsdatoen på grunnlag av det som er registrert i utlendingsmyndighetens register (DUF) eller i vedtak fra utlendingsmyndigheten, med mindre denne myndighet har satt fødselsdag og måned til 1. januar. I slike tilfeller skal fødselsdag og måned settes til den registreringsdag og måned innvandringen har fått i Det sentrale folkeregister.

For de tilfeller der fødselsdatoen som er registrert i DUF eller i vedtak fra utlendingsmyndigheten fremstår som fingert, er basert på egenerklæring eller dokumentasjon med liten bevisverdi, kan fødselsdag og måned settes til den registreringsdag og måned innvandringen har fått i Det sentrale folkeregister.

Det samme gjelder der antall tilgjengelige personnumre for den aktuelle fødselsdato er svært lavt.

I paragrafen 2-3 vi kan se rutinene ved fastsettelse av fødselsdato varierer og har kan vi konkludere at det kan ses som første trinn ved mulig identitetsforfalsking.

Som vi ser her, fødselsnummer kan fås eller ved født i Norge eller hvis person har oppholdstillatelse. Hvis vi snakker om nyfødt barn prosessen for å nå norsk personnummer er slik:

Sykehuset sender en melding til folkeregisteret ved fødsel med beskjed at dere har fått barn. Folkeregisteret,som er en del av Skateetaten, må gjør en kontroll for å sjekke at barn kan ha norsk fødselsnummer kontrollerer om barnet kan ha norsk fødselsnummer. Hvis svar er positivt sendes melding til mor om tidelt fødselsnummer sammen med skjema hvor foreldrene må oppgi hvilket navn barn skal ha. Foreldrene har plikt til å svare med navn innen 6 måneder og sende skjemaet til folkeregisteret. Etter navn er registrert, sendes ut fødselsattest.

Fødselsattesten viser at navnet er godkjent og skal tas med ved eventuelt dåp[47].

I rapport "Personal Information leakge: A study of Online Systems in Norway"[48] fra Universitet i Bergen Andr´e N. Klingsheim and Kjell J. Hol vises hvordan bygges fødselsnummer som er identifikator i Norge. Mange web portaler i Norge bruker fødselsnummer som brukernavn ved påloging i interne systemer. Eksample er studentweb i norske høyskoler. Rapporten viser utfordringer i denne rutinen. Andr´e N. Klingsheim and Kjell J. Hol viser at systemer som krever svak autentikasjon kan lede til ID tyveri.

7.2. D-nummer

D-nummer er en midlertidig identifikasjon – som brukes isteden for fødselsnummer - for personer som oppholder seg i Norge på midlertidig basis. D-nummer blir typisk tildelt asylsøkere og gjestearbeidere. D-nummeret har også elleve siffer som fødselsnummer.I § 2-5. I forskriftenFOR 2007-11-09 nr 1268: Forskrift om folkeregistrering står:

"D-nummeret skal ha elleve siffer. De seks første siffer består av vedkommendes fødselsdato i rekkefølge to siffer for dag der første er tillagt fire, to for måned, to for år. De fem siste siffer, personnummeret, består av tre individsiffer og to kontrollsiffer.

Som individsiffer for personer født:

a) før 1. januar 2000 brukes serien 000-499,

b) etter 1. januar 2000 brukes serien 500-999.

Kvinner skal ha like tall og menn ulike tall som siste individsiffer.

D-nummeret kan bare endres når fødselsdato eller kjønnsstatus endres.

D-nummeret tildeles i Det sentrale folkeregister og administreres av Skattedirektoratet. Nærmere bestemmelser om tildelingsmyndighet gis av Skattedirektoratet".

7.3. Organisasjonsnummer

En av identitetsindikator i Norge er organisasjonsnummer. Organisasjonsnummer identifiserer en bedrift eller organisasjon som etablerer virksomhet i Norge. Alle som blir registrert i Norge under Enhetsregisteret og Foretaksregisteret får automatisk identifikator som

er består av 9 siffer. Dette 9 siffer identifikator kalles organisasjonsnummer.

Organisasjonsnummer identifiserer juridiske personer som har ansvar for bedriften. Disse personene er som daglig leder, styringsmedlem, regnskapsfører osv. Alle disse personene har tildelt enkelte roller i Brønnøysund registeret som gir dem fullmakt til å rapporetre til offentlig etater forskjelige dokumenter på veien av bedrift og ofte disse dokumentene inneholder personligopplysninger, skattekort er bare en av de.

Kriminelle miljøer kan misbruke denne identifikatoren for å ta kontakt med kundene. Kundene i god tro kan svare på henvendelser som kommer ikke fra bedrift som bruker ulovlig data fra en annen bedrift. De kan sende forfalske fakturer, kan kreve opplysninger om bankonto osv.

Ikke minst med et organisasjonsnummer som er opprettet ved forflask D nummer kan kriminelle miljøer bruke bedrift til å utnytte forskjellige ytelser fra NAV. Mer detaljene om dette vi skal skrive i kapittel 11.

7.4. Hvem kan tildele og rekvirere identifikatorene i Norge

I forrige kapitel vi har ser at identifikatorer i Norge at nøkkel som svindler og kriminelle miljøer vil gjerne ha. Disse opplysningene er første trinn til å gjennomfore svindel. Istedenfor at svindler må stjele personalopplysninger fra en person de kan også utnytte rutinene for å skaffe en reel identitet i Norge. Med en slik identitet kan de utnytte offentlig etater med for eksampler dagpenger eller sykepenger fra NAV eller at de kan opprette bedrift i Norge som skal brukes for å gjennomfore svindel i Norge.

Derfor er det viktig for å se hvem i Norge har lovbestemt rett til å rekvirerer D nummer og hvilken rutiner finnes hos rekvirenter ved rekvirering de to identifikatorer i Norge.

I forskriftenFOR 2007-11-09 nr 1268: Forskrift om folkeregistrering § 2-6 sier følgende om hvem som kan tildele D nummer:

"D-nummer tildeles fysisk person som ikke fyller vilkåret for å få tildelt fødselsnummer, og som er:

a) skatte- eller avgiftspliktig til Norge, herunder til Svalbard, jf. Svalbardskatteloven § 2-1 og § 2-2,

b) i forretningsforhold med norsk bank eller annen institusjon som er underlagt reglene i lov 10. juni 1988 nr. 40 om finansieringsvirksomhet og finansinstitusjoner (finansieringsvirksomhetsloven),

c) registreringspliktig i Foretaksregisteret, Løsøreregisteret eller Konkursregisteret,

d) rolleinnehaver i juridiske enheter, jf. Enhetsregisterloven § 5 annet ledd bokstav f og § 6 første ledd bokstav a-e og h, eller har tilsvarende rolle i utenlandsk deltakerlignet selskap (DLS) eller i selskap som nevnt i skatteloven § 2-4 eller som utfører rapporteringsoppgaver på vegne av slike rolleinnehavere,

e) kontohaver i Verdipapirsentralen,

f) eier av fast eiendom som omfattes av Matrikkellova,

g) omfattet av ordning som forvaltes av Arbeids- og velferdsetaten eller Helseøkonomiforvaltningen, eller som har rettighet utledet fra slik person,

h) bosatt på Svalbard, jf. forskrift om register over befolkningen på Svalbard § 2,

i) under autorisering av Statens autorisasjonskontor for helsepersonell (SAFH).

Endret ved forskrifter 28 aug 2009 nr. 1122 (i kraft 1 okt 2009), 27 okt 2009 nr. 1315".

I forskriftenFOR 2007-11-09 nr 1268: Forskrift om folkeregistrering § 2-7 sier følgende om hvem kan rekvirere D nummer:

"D-nummer rekvireres fra tildelingsmyndigheten av den registreringsenhet som har behov for D-nummer for å registrere personer som er nevnt i § 2-6.

Dersom ikke annet er bestemt, skal rekvisisjon skje på særskilt blankett, fastsatt av Skattedirektoratet. Vedlagt rekvisisjonen må følge bekreftet kopi av legitimasjonsdokument. Legitimasjonen skal være utstyrt med fotografi av personen og inneholde opplysning om:

- *a) fullt navn,*
- *b) fødselsdato,*
- *c) kjønn og*
- *d) statsborgerskap.*

I tillegg skal det gis opplysning om adresse i hjemlandet og om oppholds-/kontaktadresse i Norge. Dersom rekvirenten mener det er nødvendig, skal det også gis opplysning om sivilstand.

Det eller de legitimasjonsdokumenter som fremlegges, skal være utstedt av offentlig myndighet eller av et annet organ hvis kontrollrutiner for dokumentutstedelser er betryggende og det er allment akseptert at dokumentet for øvrig har et tilfredsstillende sikkerhetsnivå.

Kravet til innsendt kopi av legitimasjonsdokument gjelder imidlertid ikke når arbeids- eller oppdragsgiver overfor det skattekontor som Skattedirektoratet bestemmer, har bekreftet at en persons identitet er riktig oppgitt. Kravet til innsending gjelder heller ikke for personer som kommer inn under § 2-6 bokstav g) når Arbeids- og velferdsetaten eller Helseøkonomiforvaltningen bekrefter på rekvisisjonen at legitimasjonsdokument som nevnt i foregående ledd ikke er tilgjengelig for personen. Når rekvisisjonen gjelder asylsøker, skal likevel bekreftet kopi av registreringsbevis for asylsøkere (asylsøkerbevis) vedlegges.

Skattedirektoratet kan i særlige tilfelle dispensere fra kravet til legitimering og fra kravet til innsending av legitimasjon. Skattedirektoratet kan også i forbindelse med etablering av prøveordninger for utenlandske arbeidssøkende gi andre regler om rekvirering mv. og tildeling av D-nummer."

I paragrafen ovenfor ser vi at kravet til innsending av kopi av legitimasjonsdokumentene gjelder ikke hvis arbeids-eller oppdragsgiver har bekreftet at en personsidentitet er riktig oppgitt. Her vi kan umiddelbart se utfordring i rutinene slik de er i dag. Vi må undersøke at de som har lov til å rekvirere D nummer har personell som er utdannet og har nødvendig kunnskap og systemverktøy for å avdekke eventuale falske dokumentene.

Det er flere offentlig etater samtidig noen private selskaper som er godkjent rekvirent av D nummer. De som er ikke godkjent rekvirent er:

Privatpersoner, utdanningsinstitusjoner, arbeidsgivere, organisasjoner etc. De må henvende seg til en godkjent rekvirent ut fra hvilket behov de har.

De som er godkjent rekvirent av D-nummer i Norge er:

- Skattekontoretor,
- Sentralskattekontoret for utlandssaker når utenlandsk arbeidstaker arbeider i Norge for utenlandsk firma
- NAV for EØS arbeidssøkere og mottakere av trygdeytelser.
- Banker, finansinstitusjoner og forsikringsselskaper for forretningsforhold med norsk bank eller annen finansinstitusjon
- Verdipapirsentralen vedrørende verdipapirer
- Brønnøysundregistrene for registrering i foretaksregisteret, enhetsregisteret eller løsøreregisteret

Som vi kan se det er flere aktorer i Norge som har myndighet til å rekvirere D nummer. Når det gjelder organisasjonsnummer det er Brønnøysund register som er eneste aktør for å rekvirere organisasjonsnummer i Norge. Ved å sjekke hvordan rutinene er implementert hos forskjellige rekvirenter vi kan se potensielle svakhetene som svindlere kan utnytte.

8. **Rutiner for rekvirering av D-nummer**

I kapittel 8.4 vi har beskrevet hvem som kan rekvirere D-nummer i Norge. Her skal vi beskrive rutinene som finnes hos rekvirentene når det gjelder rekvirering av D-nummer. En del av opplysningene om rekvirering finnes på rekvirentenes nettsider og noen detaljer fikk vi da vi gjorde intervjuer med de. Før vi begynner å vise frem rutiner ved rekvirering av D-nummer hos forskjellige rekvirenter, kan vi se på antallet tildelte D-nummer i Norge som viser nesten 500 000.

Tabell 8-1 Rekvirering D nummer fordelt på rekvirenter, (Skatteetaten 2011)

Navn	2005	2006	2007	2008	2009	2010
Skatt øst	9 193	12 344	18 122	20 630	16 095	14464
Skatt sør	4 497	5 971	7 855	8 202	6 837	6118
Skatt vest	3 522	5 137	7 057	9 704	7 636	6090
Skatt Midt-Norge	2 501	3 566	3 982	4 314	3 777	3483
Skatt nord	1 667	2 029	2 750	3 149	3 296	3478
Fylkesskattekontor	11	49	81	2		0
Skattefogden		2				1
Sysselmannen på Svalbard	1					0
Svalbard Skattekontor	124	113	174	184	184	163
Rikstrygdeverket, registerseks	1	1				1
Pensjonstrygden for sjømenn	31	22	38	17	63	34
Folketrygdkontoret for utenlandssaker	2 546	310	3	4	2	2
Statens pensjonskasse	2		4	57	25	2
Skattedirektoratet		2				0
Sentralskattekontoret for utenlandssaker	16 401	29 400	32 275	27 432	14 946	11685
NORAD	1	1				0
Utlendingsdirektoratet			2	2		0
Maritimt Aa-register	4 990	5 930	7 254	6 018	5 003	1337
Utenriksdepartementet	2			2		0
Arbeidsdirektoratet	1 722	2 147	1 687	410	365	41
Banker, finansinstitusjoner	6 103	8 272	7 817	8 162	7 317	6008
Brønnøysundregistrene	2 837	3 332	3 776	3 682	3 458	3562
Trygdekontor-NAV	4 667	10 004	15 968	21 664	17 569	14826
Verdipapirsentralen	1					0
Diverse	62	58	6		9	2
Helseøkonomiforvaltingen					7 834	7412
Totall	60 882	88 690	108 851	113 635	94 416	78709

8.1. NAV

Nav er en av rekvirentene og de utfører cirka 30 000 – 40 000 rekvireringer årlig. Grunnen at NAV rekvirerer D-nummer ligger i Forskrift om folkeregistrering. Det følger av forskriftens § 2-6 bokstav g at D-nummer kan tildeles til personer som er omfattet av ordning som forvaltes av Arbeids- og velferdsetaten, eller som har rettighet avledet fra en slik person.

Barn og/eller ektefeller til en person som omfattes av NAVs ordning går under denne bestemmelsen. Det samme gjelder for personer som skal registreres i NAVs Arbeidsgiver- og arbeidstakerregister, NAVs arbeidssøkerregister, herunder arbeidssøkere fra EØS-land, før de måtte komme i arbeid (og blir skattepliktige).

I følge NAV det er den registreringsenhet som har behov for D-nummeret som skal rekvirere D-nummer til personer som er nevnt i forskriftens § 2-6.

Vi ser at NAV er pålagt med forskriften til å rekvirere D-nummer til de personene som ikke fyller vilkåret for å få tildelt fødselsnummer, men som har krav på forskjellige ytelser fra NAV, for eksempel dag penger eller sykepenger. For at en person kan motta ytelser fra NAV må de være registrert i folkeregisteret.

Rutinene ved rekvirering av D nummer er slik:

- NAV bruker en blankett ved rekvirering av D nummer. Blanketten er revidert i henhold til forskriften og inneholder felter for alle opplysninger som personregisteret krever for tildeling av D nummer.
- I tillegg til blanketten som må fylles ut på NAV Lokal kontor må vedkommende vedlegge en del dokumentasjon. Dokumentasjonen som må vedlegges er kopi av gyldig pass eller nasjonalt ID kort. Minimumskravet til det som må vises frem er et dokument som har følgende:
- bilde
- personens fulle navn,
- fødselsdato,
- kjønn
- statsborgerskap

Det finnes unntak for nordiske borgere som kan fremvise gyldig førerkort og gyldig personbevis/ personutskrift/ utdrag fra befolkningsdatasystemet/ attestasjon fra folkeregisteret i hjemlandet som skal være signert og stemplet.

- Kravet til innsending gjelder ikke for personer som kommer inn under forskriften § 2-6 bokstav g når Arbeids- og velferdsetaten bekrefter på rekvisisjonen at legitimasjonsdokumentet som nevnt i første avsnitt ikke er tilgjengelig for personen. Det kan for eksempel dreie seg om bipersoner som oppholder seg i land hvor det ikke er enkelt å få legitimasjonsdokumenter som tilfredstiler de nevnte kravene. Men det kan også gjelde personer som oppholder seg her i landet, men som ikke har rett til fødselsnummer fordi sakene deres ikke er ferdigbehandlet av utlendings- og innvandringsmyndighetene. Slike personer vil som oftest ikke ha dokumenter som tilfredsstiller kravene til legitimasjonsdokument.

- Når rekvisisjonen gjelder asylsøker, skal likevel bekreftet kopi av registreringsbevis for asylsøkere (asylsøkerbevis) vedlegges.
- Kopien skal være bekreftet rett kopi.
- I tillegg er det krav om adresse i hjemlandet og om oppholds-/kontaktadresse i Norge.

Det finnes et misbrukspotensial for denne blanketten. Det er derfor NAV har valg å ha rutinen som sier at selve blanketten ikke må tas ut av NAV-kontoret.

Fullstendig utfylt skjema med vedlagt bekreftet kopi av legitimasjonen sendes til Personregisteret. Arbeidssøkere hos NAV som ikke har D-nummer eller norsk personnummer, vil i hovedsak være arbeidssøkere på EØS-vilkår. Arbeidssøkende EØS-borgere har oppholdsrett i Norge i inntil seks måneder, og har rett til å registrere seg som arbeidssøkere hos NAV. Disse er "omfattet av ordning som forvaltes av Arbeids- og velferdsetaten", slik at D-nummer kan innhentes etter forskrift om folkeregistrering § 2-6 bokstav g. Det samme gjelder for asylsøkere som har fått midlertidig arbeidstillatelse.

8.2. Skatteetaten

Skatteetaten er en norsk statlig etat med ansvar for folkeregistrering og fastsettelse og innkreving av skatt, arveavgift og merverdiavgift og er underlagt Finansdepartementet[24]. Personregisteret er en del av

[24] www.skateetaten.no

Skatteetaten som har formelt ansvar for å generere fødselsnummer og D-nummer i Norge. I tillegg til at Skatteetaten har ansvar for tildeling av fødselsnummer og D-nummer kan de også selv rekvirere begge typer identifikasjonsnummrene. Skattekontoret kan rekvirere Personnummer og D-nummer vedrørende skatte- og avgiftsplikt mens Sentralskattekontoret for utlandssaker (SFU) rekvirerer personnummer og D-nummer når utenlandsk arbeidstaker arbeider i Norge for utenlandsk firma.

Rekvirering av D-nummer hos Skatteetaten ble endret i 2011. I en pressmelding fra Skatteetaten [49]står at pga det faktum at falske identiteter har blitt et økende problem i Norge, innfører Skatteetaten nye rutiner for søknad om skattekort eller om søknad om rekvirering av D-nummer. Når det gjelder skattekort var det tidligere slik at alle personer med D-nummer i Norge fikk tilsendt skattekortene per post, men fra 2011 krever Skatteetaten personlig oppmøte for identitets- og legitimasjonskontroll.

I samme pressemelding sier skattedirektør Svein Kristiansen at de håper at dette vil føre til færre falske identiteter basert på D-nummer og at de vil få bedre oversikt over personer med D-nummer.

"Grundigere identitetskontroll mener vi er et helt nødvendig tiltak for å møte dagens trusselbilde. Vi følger utviklingen på dette området og vil sette i verk andre tiltak dersom det er nødvendig" sier skattedirektør Svein Kristensen.

Når det gjelder rutinene ved rekvirering av D-nummer er de det samme som vi fant hos andre rekvirenter. Den som skal ha D-nummer må selv møte opp på skattekontoret med gyldig legitimasjon. Minimumskrav til dokumentasjon er:

- navn
- fødselsdato,
- kjønn
- statsborgerskap
- bilde

Kopi av gyldig pass eller nasjonalt id-kort skal vedlegges. Alle kopier må være bekreftet rett kopi av norsk offentlig myndighet. I begrepet offentlig myndighet definerer skatteetaen: skattekontor, politi, NAV, Brønnøysundregistrene, tingsretten, autorisert regnskapsfører, advokat, autorisert eller statsautorisert revisor, norsk utenriksstasjon, notarius publicus eller annen offentlig myndighet og i tillegg aksepterer

skatteetaten dokumenter som har bekreftet rett kopi av norske banker og forsikringsselskaper.

Ved personaloppmøte hos en av skattekontorene i hele landet må de også fylle ut skjema RF-1209 (Skattekort for utenlandske borgere) som sendes til Personregisteret i Skatt Nord Hammerfest.

Utenlandske arbeidstakere som skal jobbe hos utenlandsk arbeidsgiver, må søke Sentralskattekontoret for Utenlandsaker (SFU) om D-nummer og skattekort.

8.3. Bankene

I "Nasjonalt ID-kort"[50] rapport fra Justis- og Politidepartementet kan vi se at i henhold til oppgave fra Norges Bank er det per 2005 utstedt nesten 5 million kort med bankaksept-funksjon. I rapporten står også at det antas at slike bankkort er det meste utbredte ID-kort i Norge. Bankkort utstedes til brukeren primært for å dokumentere kundeforhold og for identifisering i banken. Disse kortene utstedes i stor grad med bilde og personinformasjon som inneholder fødselsnummer eller D nummer.

Fra 01.03.2007 begynte banknæringen med en regel som krever fremlagt pass ved utstedelse av bankkort som inneholder visuel personinformasjon (bilde). For personer som verken har personnummer eller D-nummer har banknæringen et minstekrav til dokumentasjon i forbindelse med oppretting av kontonummer, noe som umiddelbart starter rekvisisjon av D-nummer.

Minstekravene er fastsatt av myndighetene i hvitvaskingsloven med tilhørende forskrifter[51]hvor det stilles absolutte krav til identitetskontroll:

Ved etablering av kundeforhold skal rapporteringspliktige kreve gyldig legitimasjon av kunden. Kundeforhold anses i følge forskriften etablert når kunden kan bruke den rapporteringspliktiges tjenester.[52]

Identitetskontroll skjer alltid ved kundens personaloppmøte men det finnes untakk når dette ikke er praktisk gjennomførbart. Personer som ikke har fødselsnummer eller D-nummer må fremvise legitimasjon som inneholder:

- Fult navn
- fødselsdato
- Fødested
- kjønn

- statsborgerskap
- fast adresse

Alle bankene bruker en blankett med rekvirering av D-nummer som sendes til Personregisteret. Sparebank1 viser informasjon om hvordan D-nummer kan rekvireres og viser link til Skatteetatens side hvor de kan finne og laste ned selve blanketten. Informasjonssjef i DnB NOR Aud Helen Rasmussen vil ikke avsløre hvilken rutine de har ved rekvirering av D-nummer. Hun sier at de skal rekvirere minst mulig antall av D-nummer og hun mener at det er ikke bankenes hovedoppgave å rekvirere D nummer. Hun også sier at jeg bør ta kontakt med FNO som de har rapporteringsansvar til.

8.4. Brønnøysund register

Brønnøysundregistrene er en forvaltningsenhet med ansvar for en rekke nasjonale kontroll- og registreringsordninger for næringslivet. Alle personene som vil etablere bedrift i Norge må søke hos Brønnøysundregistrene. Dette innebærer at de melder til Brønnøysundregistrene hvem som skal være daglig leder, innehaver, forretningsfører eller en annen kontakperson i denne bedriften. Med daglig leder/forretningsfører mener Brønnøysundregistrene personer som har ansvar for administrativ ledelsen av bedrift og som har myndighet til å representere bedriften utad.

Brønnøysundregistrene kan rekvirere D-nummer fra Det sentrale folkeregisteret. Dette fremgår av forskrift om folkeregistrering § 2-7 jf. § 2-6. Vilkåret for at Brønnøysundregistrene skal rekvirere D-nummer er at en utenlandsk person uten norsk fødselsnummer trenger D-nummer i forbindelse med registrering i Brønnøysundregistrene.

Alle disse personene må ha et norsk fødselsnummer eller D-nummer og derfor har Brønnøysundregistrene mulighet og plikt til å rekvirere D-nummer. I veiledning for Samordnet registermelding [53]som er en veiledning for alle som skal registrere bedrift i Norge står følgende om tildeling av D nummer:

”D-nummer er et eget nummer som identifiserer utenlandske personer uten norsk fødselsnummer. D-nummer tildeles av Sentralkontoret for folkeregistrering, og skal brukes i alle sammenhenger der det er behov for en slik identifisering overfor norske myndigheter. For at Brønnøysundregistrene skal kunne bestille D-nummer, må du legge ved en bekreftet kopi av gyldig legitimasjonsdokument med:

- bilde
- personens fulle navn,
- fødselsdato,
- kjønn
- statsborgerskap

For eksempel pass. Kopien skal enten være bekreftet av nordisk politimyndighet, norsk offentlig myndighet, norsk advokat, utenlandsk enhet med notalrialkompetanse, norsk autorisert regnskapsfører, norsk statsautorisert eller registrert revisor. I tillegg må kopien være stemplet av den enheten som bekrefter dokumentet. Vi anbefaler at blanketten «Anmodning om tildeling av D-nummer» benyttes. Du får blanketten ved å kontakte Brønnøysundregistrene, eller ved å laste den ned fra:

http://www.brreg.no/blanketter/ d-nummer_last_ned.html. ”

Når det gjelder signatur som er en fullmakt til å opptre og underskrive på bedrifts vegne i forretningsforhold må det oppgis navn, adresse og fødselsnummer eller D-nummer til de som er tildelt signatur.

Videre sender Brønnøysundregistrene blanketten til Skatt nord – Hammerfest, Personregisteret som tildeler D-nummer til vedkommende.

9. **Metode**

Hver gang vi prøver å finne svar til et spørsmål eller prøver å finne ut hvorfor et ukjent fenomen skjer, er det viktigste vi må gjøre på forhand er å definere problemstilling og undersøke fenomenet slik at andre som skal bidra til å finne svar har et klart bilde av fenomenet. Derfor er riktig valg av metoden for å gjøre en undersøkelse veldig viktig.

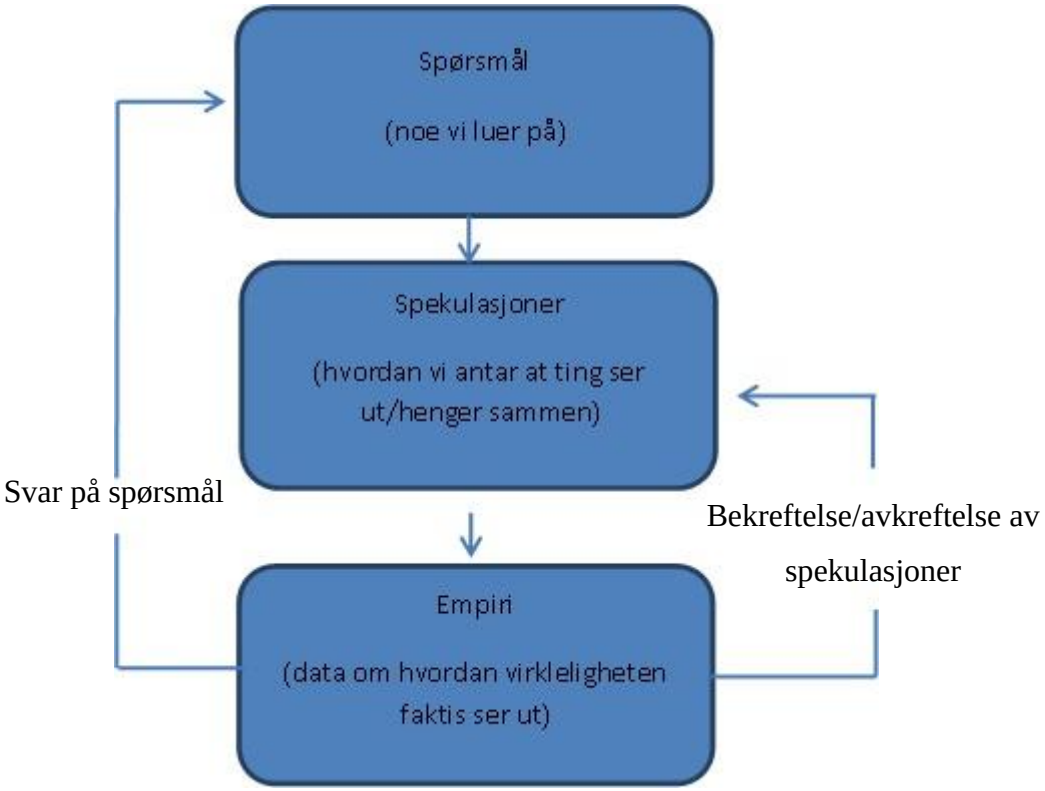
Vanligvis de som undersøker problemstilling har allerede spekulasjoner om selve problemet og har sine meninger om hvorfor dette skjer. Dette er vanlig situasjon hvor spørsmål og spekulasjoner finner plass. Vi vet ikke med 100 % riktig svar for problemet, men har spekulasjoner om dette.

I vår oppgaven vi påstår at identitetstyveri og identitetsvindel er et voksende problem i verden. Videre spør vi oss, finnes slik tendens her i Norge også. Uansett at det finnes ikke eksakt tall om problemet i Norge (vert fall ikke statistisk) vi kan påstå på grunn av eksempler som vi fant at slik tendens kan forventes i Norge. Vi mener også at rutiner som finnes i forskjellige etater ved rekvirering av forskjelige idintifikatore i Norge (fødselsnummer, D-nummer og organisasjonsnummer) kan gi svindleren mulighet for å opprette en falsk eller fiktiv identitet og at med en slik identitet misbruke offentlig etater som NAV eller Brønnøysund registrene.

Her ser vi at spørsmål og spekulasjon er på stedet. For å sjekke hvordan forholdene faktisk er, trenger vi en praktisk undersøkelsen som skal beskrive virkelighet. En slik undersøkelsen kan gi oss svar på spørsmålet eller gir oss tilbakemelding at vår spekulasjon er riktig, delvis riktig eller feil. Slik praktisk undersøkelsen kaller som Jacobsen (2005) empirisk undersøkelsen.

I empirisk undersøkelsen sjekker vi at våre spekulasjoner og våre spørsmål har fast grunn eller at det er bare finnes i vår fantasi. Det kan gi oss grunn at vi fortsetter med forskning eller at vi må endre måtte vi tenker på problemet.

Alle undersøkelsene går gjennom følgende faser:



Figur 9-1 Faser i undersøkelsen (Jacobsen 2005)

9.1.Gjennomføring av undersøkelser

Jf. Jacobsen (2005) består en undersøkelsesprosess av 8 faser:

Fase 1: utvikling av problemstilling

Fase 2: valg av undersøkelsesdesign

Fase 3: Valg av metode, kvalitativt eller kvantitativt

Fase 4: Hvordan samle inn data

Fase 5: Hvordan velge ut enheter

Fase 6: Hvordan analysere data

Fase 7: Hvor gode er de konklusjonene vi har trukket

Fase 8: Tolkning av resultater

Alle disse fasene er gjennomgått i forbindelse med gjennomføring av denne oppgaven. I det videre i dette kapittelet vil jeg gjennomgå noe

teori rundt valg av undersøkelsesdesign, valg av metode og hvordan samle inn data.

9.2. Undersøkelsesdesign

Det finnes mange måter å designe undersøkelsen. En måte å gjøre dette er å bruke to dimensjoner som Jacobesn (2005) gjør for å systematisere dette materialet. De to dimensjonene er om studien går;

I bredden (ekstensiv) eller dybden (intensiv)

Og om studien er beskrivende eller forklarende

9.2.1. Ekstensiv design

Med ekstensiv design som går i bredden mener vi at vi må undersøke mange enheter. Dette betyr at vi prøver å finne ut en forklaring for fenomenet eller å beskrive hyppigheten av fenomen. Vi har allerede fant ut at omfanget av identitetstyveri i Norge per i dag er ganske ukjent. Det finnes ikke statistikk som viser omfang eller hyppighet av svindelen som er gjort med bruk av falske eller fiktive data. Enkelte etater kommer med noen tall men gyldig statistikk finnes ikke per i dag. Enkelte tall som viser identitetstyveri kan øke mulighet for å generalisere funnene som er kjent problem med denne type design .Eksempel på generalisering er påstand at 124 000 nordmenn har vært utsatt for identitetstyveri i siste to årpga av en representativt tall fra undesøkelsen som har vi nevnt i kapitel 6.

9.2.2. Intensive design

Intensive design eller design som går i dybden prøver å finne ut så mange detaljer som mulig med hensikt til å beskrive fenomen på best mulig måtte. Selve identitetstyveri fenomen er ganske kjent i verden og i Norge men påstand atrekvirering av personnummer eller D nummermed dagens rutinene hos forskjellige rekvirenter kan inneholde høyrisiko, trenger ikke å vare helhetlig forståelig for alle. Derfor vil vi undersøke hvordan rekvirenter opplever fenomenet som er en av parameterne ved intensive design og prøve å kartlegge hvordan kobling mellom rekvirering og mulig svindel kan oppstå.

Pga spesielt problemstilling med identitetstyveri, antall rekvirenter, og at i Norgealle rekvirenter er kjent med utfordring ved identitetstyveri det er naturlig å velge undersøkelsendesign som går i dybden. Vi kan selvfølgelig bruke ekstensive design for å undersøke hvordan de rutinen ved rekvirering av personnummer eller D nummer er følget opp hos alle

saksbehandlere hos hver enkelt rekvirent (bare i NAV jobber 16 000 mennesker). Det er relativt åpenbart at en slik undersøkelsesdesign vil være ressurskrevende, både i utforming og i analysearbeidet. Hensikt med oppgaven var ikke å sjekke kvalitet av rutinene hos rekvirenter men å finne ut helheltig forståelse av høy risiko som finnes med dagens rutiner ved rekvirering.

Den andre dimensjonen av en undersøkelsesdesign er om undersøkelsen skal gi en beskrivelse eller en forklaring.

9.2.3. Beskrivende design

En undersøkelse som har en beskrivende (deskriptiv) design vil forsøke å beskrive en situasjon, en oppfatning, meninger, resultat osv. For å gjennomføre en undersøkelse med deskriptivt design kan vi kort se på 5 ulike studier:

- Tverrsnittstudie: Beskriver virkeligheten kun på ett tidspunkt. Eksempel: hva synes du om dagens rekvirering av D nummer.
- Tidsseriestudier: Her vil vi forsøke å beskrive en utvikling over tid. Altså at vi sammenligner resultater fra to eller flere undersøkelser for å si noe om utviklingen. I tidsseriestudier er ikke nødvendigvis utvalget i undersøkelsene de samme personene, men de er hentet fra samme populasjon.
- Kohortsstudier: Her undersøkes utvikling over tid, men her må utvalget være det samme. Endringene over tid vil bare framkomme på gruppenivå.
- Panelstudier: Også her er utvalget det samme over tid, men her vil en samle inn data slik at en kan se på utvikling over tid på individnivå.
- Retrospektiv tverrsnittstudie: på en måtte det er likt som tverrsnittstudie men deltakerne i undersøkelsen må svare på hvordan situasjonen var tilbake i tid.

9.2.4. Forklarende design

Forklarende design innebar at et fenomen kunne frambringes med sikkerhet ved at et eller noen forhold ble manipulert (Jacobsen,2005) og må tilfredsstille tre forhold:

- Det må være samvariasjon mellom det vi antar er årsaken, og det vi antar er virkningen

- Årsak må komme før virkning i tid, og det må være tidsmessig nærhet mellom årsak og virkning
- Kontroll for alle andre relevante forhold

Hvis vi se vår oppgaven som har påstand at svakhet ved rekvirering av D nummer kan ledde til identitetstyveri, vi kan sjekke at de tre forholdene er på stedet:

Sammenheng mellom årsak og virkning:

Hvis det er sammenheng vet at svindleren kan rekvirere D nummer via rekvirenter med en falsk pass og skaffe gyldig ID fra Norge og kan utnytte ytelser fra NAV, vil dette kravet være tilfredsstilt.

Årsak før virkning:

Hvis vi viser at antall pass som er forsvunnet i postgangen er mindre etter eventuelt nye rutine som krever personligoppmøte på postkontor med gyldig ID, vil dette kravet være tilfredsstilt.

Kontroll for andre relevante forhold:

I utgangspunkt er det umulig til å sjekke alle relevante forhold som kan oppstå i en situasjon. Det er vanskelig å ha en full oversikt over alle slike forhold. Kan vi være 100 % sikkert hele tiden at vi har nok kunnskap for åavdeke falske pass eller andre falske ID dokumentene. Dette kravet kan tilfredsstilles med å eliminere andre mulige forklaringsmetoder som if. Jacobsen, 2005 kaller vi eksperimentelle design.

Mens forklarende design innebar at et fenomen kunne frambringes med sikkerhet ved at et eller noen forhold ble manipulert, deskriptivt design går på å beskrive problemstilling i en situasjon på et gitt tidspunkt, eller se på utviklingen i et utvalg over tid. Samtidig deskriptive design prover å beskrive utviklingen i en spesiell gruppe over tid eller utviklingen hos enkeltpersoner over tid.

Vi ser at statistikk over identitetstyveri i Norge finnes ikke. Identitetstyveri kan oppdages ganske senere og noen ganger offentlig etater finner oppdagelse av identitetsyveri etter mange år. Alle disse faktorene viser fre at det bli vanskelig å velge denne design i full skala.

Vi kan oppsummere gjennomgangen ovenfor med at valg av undesøkelse design er i tett sammenheng med problemstilling. De ofte er det beste å kombinere ulike design. Ved kombinasjon kan vi ført

oppleve at ulike designene utfylle hverandre og kan gi oss bedre forståelse av fenomenet.

9.3. Valg av metod

I forhold til valg av metode i utgangspunkt må vi vurdere valg av to type undersøkelsen, kvalitativ eller kvantitativ. Forklaringen på forskjellen mellom kvalitatvie og kvantitative data kan jf. Dey (1993) skrives på følgende måte: "Mens kvantitative data operere med tall og størrelser, opererer kvalitative data med meninger. Meninger er formidlet i hovedsak via språk og handlinger".

Tall kan naturligvis også formidle meninger, men når vi snakker om identitetstyveri og hvordan mennesker opplever det det er lettere å beskrive dette gjennom språk en tall.

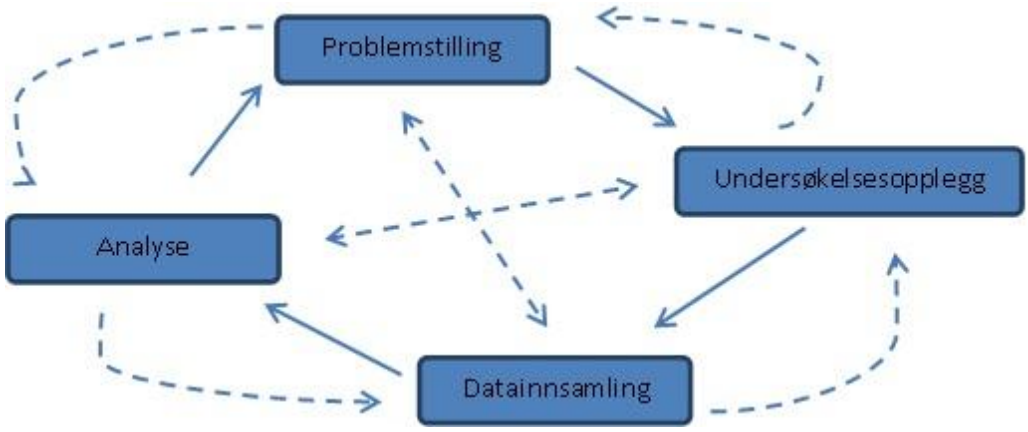
Valg av kvalitativ eller kvantitativ metode trenger ikke å være to motsetninger. De kan selvfølgelig kombineres. Figur under illustrerer dette. Begge alternativer har sine gode sider og svakheter som vi har nevnt tidligere. Med kombinasjon av kvalitativ og kvantitativ undersøkelsen kan vi begrense ulempene som finnes ved enten å velge en ren kvalitativ eller ren kvantitativ metode.

Figur 9-2 Blaning av metoder (Jacobsen 2005)

9.3.1. Kvalitativ metode

Fordelene med en ren kvalitativ metode er at vi kan gå dyp i problemstillingen. Det finnes ikke begrensing hvor detaljert vi vil gå i undersøkelsen. Vi kan skaffe fram nyansene og via slik undersøkelsen vi kan få tilbakemeldinger som kan bidra at undersøker endre mening om problemstilling, lærer mer om fenomenet og kan i utgangspunkt endre den opprinnelige problemstillingen. Det kan også defineres at kvalitativ

undersøkelse prosessen kan sees som en interaktiv prosess (Jacobesen, 2005). Figur 10-3 illustrerer dette.



Figur 9-3 Interaktiv prosess (Jacobsen 2005)

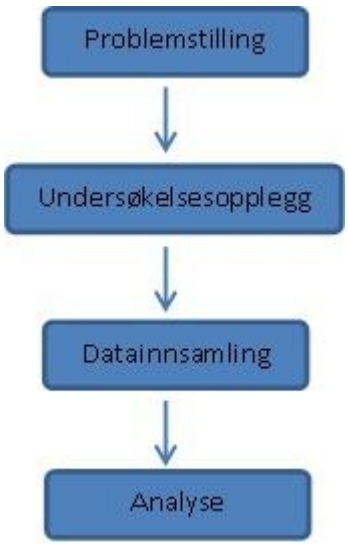
Svakhet med denne metoden er at den er ressurskrevende. Generaliseringsproblem gjennom usikkerheten til om svarene fra deltakerne er representative for andre enn dem selv er en kjent svakhet med denne metoden. Selve tolkning av resultatene kan bli komplekse siden de er så detaljert. Et annet problem med kvalitativ metode er det som Jacobsen (2005) kaller undersøkelseseffekten, men som i andre sammenhenger ofte omtales som Hawthorn-effekten[25].Det betyr at når vi gjør intervjuer det kan hende subjekt som er på intervju endre atferd av den grunn. Det er også spørsmål hvordan deltakerne i undersøkelsene vil eller kan svare sant på spørsmål i en intervjusituasjon. Dette vil naturligvis avhenge av spørsmålenes karakter og hvem som intervjuer deltakeren. If. Jacobsen (2005) vi kan velge kvalitativ tilnærming når vi er interessert i tema som trenger nærmere avklaring i hva som ligger i et begrep eller fenomen og har som regel hensikt til å få fram hvordan mennesker fortolker og forstår situasjon eller problemstilling.

9.3.2. Kvantitative metoden

Kvantitative metoden er effektivitet. Det er enkelt å lage og sende spørsmålene via dagens teknologi. Bruk av datamaskin, sms, papir

25 På 1920- og 1930-tallet ble det gjennomført en del produksjonsstudier ved Hawthorn-fabrikken i USA som viste at undersøkelsene i seg selv økte produksjonen.

utgaver som sendes på post til stor uvalgt av undersøkelser er vanlig kanalfor gjennomføring kvantitativ undersøkelsen. Kostnader ved kvantitative undersøkelsen er mindre enn gjennomføring av kvalitative undersøkelsen og dette kan gi oss mulighet til å velge mange respondenter som kan gi oss et representativ utvalgt. Eksempel på dette opplever vi ved kontakt med bankene i Norge. Hvis vi ringer bankene og spør om for eksempel bilforsikring, vi får også epost med undersøkelsen hvor de vil gjerne ha tilbakemelding fra kundene om hvordan de opplevde samtalen med kundeservice. Undersøkelsen via spørreskjema gir oss mulighet til å begrense varighet av undersøkelsen ved definering når undersøkelsen skal starte og når det skal sluttes.If. Jacobsen (2005) vi kan se den kvantitative undersøkelse prosessen som en sekvensiell prosess. Figur 3.4 under illustrerer dette



Figur 9-4Sekvensiell prosess (Jacobsen 2005)

Stor fordel med denne type undersøkelsen er lettere og ikke minst lettere analysearbeidet etter datainnsamling.Det er mye letere å systematisere data og å strukturere informasjon enn fra en kvalitativ undersøkelse. Med kvantitative undersøkelse vi kan unngå problem med nærhet til deltakerne somfinnes i kvalitative undersøkelse. "Nærhet" til undersøkeren kan være så tett at den kan gi uønskede effekt ved at vi mister evnen til kritisk refleksjon. Med kvantitative undersøkelse vi kan lettere holde en kritisk "avstand".

Ulempen med denne metoden er at den kan fort bli for overfladisk og enkel. Spørsmålsstillingene må være konkrete, og det krevet at vi må

passe hvordan vi definerer spørsmålene. Det er også risiko at vi stiller ikke de riktige spørsmålene som kan føre til misforståelse og til feil svar. Metoden gir liten eller ingen mulighet til å korrigere spørsmålene underveis. En kvalitativ metode vil med større sannsynlighet kunne avdekke dette problemet

Vi kan oppsummere gjennomgangen ovenfor med at kvalitativ metode ofte passer best i de tilfeller hvor vi ikke har en klar problemstilling og vi vet lite om det tema som skal undersøkes, mens kvantitativ metode ofte passer best hvor vi har god kjennskap til tema som skal undersøkes.

9.4. Innsamling av kvalitative data

Ved å undersøke hvordan forskjellige rekvirenter rekvirerer D nummer og med tanken å undersøke hvordan de opplever identitetsyveri problemstilling det er naturlig å velge kvalitativ tilnærming og derfor det er viktig å velge hvordan vi skal samle kvalitative data.If. Jacobsen, 2005 det finnes 4 forskjellige metoder for kvalitativ datasamling:

- Det individuelle, åpne intervjuer
- Gruppeintervjuet
- Observasjon
- Dokumentundersøkelse

Metoden som jeg har valgt i oppgaven var det åpne individuelle intervjuet. Denne datainnsamlingsmetoden if, Jacobsen (2005) er den vanligste innenfor kvalitativ metoden. Det kan defineres som en vanlig dialog mellom undersøker og undersøkt. På grunn av at i Norge finnes ganske få rekvirenter av D nummer det egner seg til denne metoden for datainnsamling. Jeg hadde plan til å intervjuere hoved aktorer ved rekvirering av D Nummer, Skatteetaten, NAV, Brønnøysund register og FNO som representerer bankene i Norge. For oppgaven er det ganske viktig å vite hva det enkelte rekvirenter sier om problemstilling med D nummer rekvirering og identitetstyveri og hvordan de fortolker ansvar ved rekvirering. Pga avstand til representanter fra NAV, Skatteetaten og FNO valgt jeg å foreta intervjuet ansikt til- ansikt men med Brønnøysund register pga stor avstand og kostnader valgt jeg intervju via telefon uansett at noen undersøkelse viser også at det kan være lettere for intervjuobjekt å lyve eller "slå en plate" i intervjueren ved telefonintervju (Frey & Oshi, 1995) I tillegg hadde jeg en del korespondering via internett.

Intervjuene hadde en varighet mellom en og to timer. Og fant stedet hos undersøkte.

I tillegg til innsamling av primærdata i form av ord, setninger, fortellinger og uttalelser brukte jeg også en form av innsamling av kvalitative data som kalles dokumentundersøkelsen (Jacobsen, 2005). Pga manglende statistikk når det gjelder omfang av identitetsyveri og manglende statistikk fra rekvirenter det var vanskelig å samle inn informasjon direkte fra kilde. Da måte jeg benytte offentlig dokumenter, søknadsskjemaer, årsrapporter, artikler fra forskjellige publikasjoner og fra web sider. Naturlig ved bruk av denne metoden måtte jeg gjør en valg hvilke dokumenter jeg velger ut og hvor stor troverdighet de dokumentene har. Vi gravde ganske dyp for å få meste av dokumenter som jeg har brukt i oppgaven men oppsummering er slik at rutinene som for eksempel banke ved rekvirering av D nummer og ved identitetskontroll er ikke tilgjengelig og de vil ikke uttaler seg om dette. Ved innsamling av primærdata jeg hadde en viss grad kontroll over forholdene som kan påvirke påliteligheten til datane. Jeg hadde søknadsskjema ved rekvirering av D nummer, hadde årsrapport som viser tapt av kroner hos bankene ved skimming osv. Ved bruk av sekundærdata jeg hadde ikke denne kontrollen men måtte valgte artiklene og årsrapportene i god tro at de er troverdig pga manglene mulighet til å sjekke dette videre.

9.5. Valg av enheter som skal intervjueres

Det er flere offentlig etater samtidig noen private selskaper som er godkjent rekvirent av D nummer

De som er godkjent rekvirent av D-nummer i Norge er:

- Skattekontoretor,
- Sentralskattekontoret for utlandssaker når utenlandsk arbeidstaker arbeider i Norge for utenlandsk firma
- NAV for EØS arbeidssøkere og mottakere av trygdeytelser.
- Brønnøysundregistrene for registrering i foretaksregisteret, enhetsregisteret eller løsøreregisteret.
- Banker, finansinstitusjoner og forsikringsselskaper for forretningsforhold med norsk bank eller annen finansinstitusjon.
- Verdipapirsentralen vedrørende verdipapirer

Jeg har valgt å intervjuere de meste representative rekvirenter:

Skatteetaten som presenter første to på lista, NAV, Brønnøysund register og FNO som presenterer siste to. I utvalg av personer til åpne

intervjuer jeg har søkt på personer som har direkte kjennskap til identitetsyveri problemstilling og med kjennskap til rekvirering av D nummer.

10. Case

Innen kvalitativ tilnærming finnes det flere datainnsamlingsmetoder som vi allerede har nevnt i kapitel 5. På grunn av manglende statistikk over identitetstyveri i Norge var det nødvendig å beskrive problemstillinger og potensielle konsekvenser som rekvirenter kan bli utsatt for. Siden denne oppgaven tar for seg at det er mulig å skaffe gyldig identifikator i Norge via rekvirenter slik at den kan misbrukes i offentlig sektor, faller det naturlig å presentere noen caser som omhandler hvordan dette kan gjøres. Dette vil bli gjennomgått i forhold til den konkrete situasjonen som vi skal presentere hvor vi håper å bekrefte eller avkrefte at vår påstand er riktig.

Via forskjellige caser prøvde jeg å skaffe en reell situasjon som kan oppstå hos rekvirenter. Det blir da lettere å forstå situasjonen og det kan være en god start for et intervju.

Vår case starter med det faktum at det har vært lekkasjer i Norge både fra private selskaper og fra offentlig etater[54]. Disse lekkasjene, sammen med andre metoder for ulovlig anskaffelse av personopplysninger i norge, var dokumentert og beskrever i kapitel 5.

10.1. Case 1

La si i vår teori at person Sven Svensson vil prøve å utnytte en offentlig etat, i vår case Arbeids- og velfredsetaten. NAV er en statlig etat under Arbeidsdepartementet og har ansvar for gjennomføring av arbeids- og velfredspolitikk. Det er også NAV sitt samfunnsoppdrag å levere tjenester til både enkeltmennesker og fellesskapet. Etaten har utbetalt 376 milliarder kroner i 2010 [55]. Av utbetalt beløp er 125,7 milliarder kroner utbetalinger av pensjoner og 55,4 milliarder kroner for uførepensjon.

Av det utbetalte beløpet er 125,7 milliarder kroner utbetalinger av pensjoner og 55,4 milliarder kroner for uførepensjon.

Her ser vi at en stor etat med mange milliarder kroner som utbetales til private personer kan bli et mål for kriminelle miljøer. Vi har allerede

beskrevet at det finnes statistikktall fra NAV som viser vår påstand om at det var flere forsøk på å utnytte andres personopplysninger for å skaffe ulovlige ytelser fra NAV.

I vår teori går vi videre med påstanden om at Sven klarte å skaffe Ola Nordmanns personnummer. Vi ser at før et konkret offer velges ut gjør de kriminelle en seleksjon. Offentligjøring av skattelistene er et sted som kan brukes til å finne de meste "attraktive" ofrene. Et godt eksempel på hvordan de velger et offer er den kriminelle gruppa som var bak det som er kjent som Plastic Fantastic-saken [56] .

I kapitel 5 har vi skrevet om forskjellige metoder ved innsamling av identitetsinformasjon.

Neste steg er å skaffe falske dokumentene som skal brukes senere. I verden finnes det mange steder som produserer falske dokumenter. Det er ikke nødvendig å kjenne noen kriminelle som kan skaffe slike dokumenter. På weben finnes det mange nettsider som selger slike tjenester. Prisklasse for forskjellige dokumenter finner vi i en rapport fra Symantec (tabell 4).

Når Sven har navnet og personnummeret til Ola Nordmann er første steg som gjelder innsamling av identitetsinformasjon ferdig. Via www.gulesider.no eller www.1881.no eller andre steder som viser adresse er det ganske lett å finne ut hvor Ola bor. Via kriminelle miljøer eller på nettet bestiller Sven to typer forfalskede dokumenter. Ved "bestilling" sender Sven opplysningene om Ola, bilde av seg selv og bilde av et vanlig bankkort. Dokumentet som Sven har bestilt er et pass med opplysningene om Ola. Passet inneholder Olas navn, personnummer og i tillegg navn på stedet hvor passet er utstedet (stedet hvor Ola bor) med bilde av Sven, det andre er et bankkort som er helt likt et vanlig bankkort som vi har sett i forskjellige banker i Norge.

Kvaliteten på de falske dokumentene som finnes i Norge er så god at det er vanskelig å se forskjell uten en nøye ekspertise som må gjøres, sier Terje Bjørlo[26] som har over 20 års erfaring fra politi og som i dag jobber som etterforsker hos Lindorff Norge.

Med to de to forfalskede dokumentene kan Sven begynne kriminaliteten med falsk identitet.

[26] Idtyverikonferansen Oslo 2010

Bestiling av varer som krever personligoppmøte på postkontoret med ID-dokument var en av de tilltakene som flere selskaper har utarbeidet i siste årene. Hvis du bestiller mobiltelefon fra netcom må du viser frem id-dokument ved henting av varer. I tillegg krever netcom en betaling på 91 kroner på posten når du henter varen. Men så lenge du gjør dette kontant er det ikke noe problem å hente varer som tyven har bestilt.

"Under 100 kroner for en flunkende ny iPhone må anses som god busineiss for svindlerne"

skrives i en artikkel som ble publisert i DinSide [57].Med de forfalskede dokumentene som Sven har er det ikke vanskelig å gjennomføre svindelen.

Det finnes flere typer av kriminalitet som foregår ved bruk av slike ID-bevis. Kjøp av alkohol av mindreårige er også en sak hvor vi ser dette problemet.

10.2. Case 2

John Smith er ikke fra Norge. Han har en kriminell fortid i hjemmelandet og har planer å fortsette dette i Norge. Han har venner fra Norge som vet hvordan systemet fungerer i Norge og som forklarer ham hva han må gjøre for å komme til Norge, hvor han kan prøve å svindle den Norske staten for å få en annen identitet, slik at han kan renvaske sin identitet.

Sven må først og fremst skaffe en falsk identitet.

Norge er en drømmeland for mange mennesker, sier Samfunnsøkonom Greg. J som hadde en workshop ved Universtitet i Stavanger [58]hvor han presenterte forskning som bidrar til å løfte fattige ut av fattigdom i USA. Men det er ikke bare fattige som har lyst til å komme i Norge. Mange kriminelle har også tanker om å operere i Norge. Bare i 2009 registrerte Norge over 65000 innvandringer [59], viser tall fra SSB samtidig viser samme kilde at det er 11400 nye norske statsborgere [60] i Norge. Samtidig var det over 17 000 asylsøkere som har kommet i 2009 i Norge [61]. Grunnen til at vi nevner disse tallene er det faktum at en del kriminelle miljøer misbruker norsk asylpolitikk slik at disse opplysningene ved velging av falske pass er ganske viktig. Ett eksempel er en albansk mann som fikk oppholdstillatelse i Norge ved hjelp av et falskt pass og falsk identitet [62].Denne personen hadde flere falske identitetsdokumenter, i dette tilfellet pass fra forskjellige land som han brukte ved søking av oppholdstillatelse i Norge. Vi kan anta at John kan gjøre akkurat det samme. Han bestiller en falsk pass med bilde av ham,

men med oppsyningene om en annen person som han bruker som identitetsbevis.

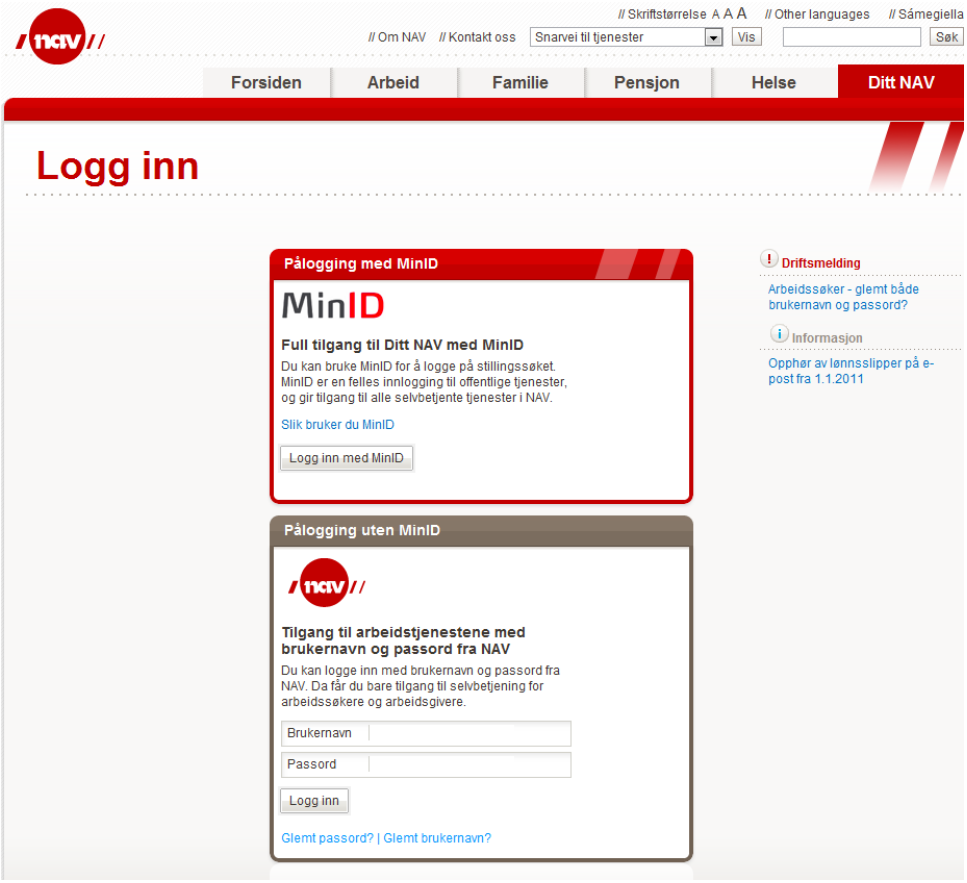
John vil jobbe i Norge og derfor trenger han et D-nummer som kan skaffes via rekvirenter. En mulighet er å gå via arbeidsgiver. John klarer å finne jobb i en bransje som mangler arbeidstakere. Et godt eksempel er bygge- og anleggsbransjen i Norge som har et stort antall arbeidstakere fra utlandet. Vi antar at arbeidsgiveren har behov for flere folk som kan jobbe hos ham pga et stort byggeprosjekt. John vet om det og melder seg på oppdraget. Arbeidsgiveren sender melding til NAV med opplsyning om at John vil starte jobb hos han. Pga manglende opplysninger om John krever NAV kopi av pass ved rekvirering av D-nummer. Arbeidsgiver ber John å ta kopi av passet sitt. NAV mottar kopi av pass og sender rekvisisjon til Personregisteret. Personregisteret rekvirerer D-nummer og sender tilbake melding om dette til NAV som også sender informasjon om dette til arbeidsgiver. Arbeidsgiver gir beskjed til John at han har gyldig D nummer i Norge. Dette brevet tar John med seg til banken og oppretter kontonummer og i tillegg kan han søke om norsk førekort som kan brukes som identifikasjon i Norge.

John jobber hos arbeidsgiveren en måned og begynner å klage på at han har vondt i ryggen. Med denne type belastningsjobb som finnes i bygge bransjen kan John etter 4 uker kreve sykepenger. Kravet om minst 4 uker arbeid er bestemt i Folketrygdloven § 8-2 hvor det står:

”For å få rett til sykepenger må medlemmet ha vært i arbeid i minst fire uker umiddelbart før han eller hun ble arbeidsufør (opptjeningstid). Fravær i et arbeidsforhold uten gyldig grunn regnes ikke med i opptjeningstiden.”

Dette gjelder ikke bare fast ansatte men også ekstrahjelper og andre deltidsansatte. Med sykepenger i lomma kan John kan tilbake til hjemmelandet og få sykepenger fra Norge. Muligheten for at han må komme på møte hos NAV er en pris som de fleste tyvene vil akseptere.

Det er ikke bare sykepenger som kan misbrukes. Rett til dagpenger har også mulighet for å misbrukes. John har jobbet er stund og slutter etter par måneder. Han har fortsatt gyldig D-nummer og melder seg arbeidsledig hos NAV. Han vet at han må sende meldekort via nav.no for å bekrefte at han ikke står i jobb. Han gjør dette hver måned på NAV.no:



Figur 10-1 Innloging bilde på www.nav.no

Ordningen med sending av meldekort via internett er også diskutabel. John kan sitte i et annet land å få tilsendt ytelser fra NAV uten at Nav vet om dette. Hvis NAV ikke sjekker IP-adressene som er brukt ved innsendning av meldekort kan ikke Nav kontrollere at John ikke befinner seg i Norge, og han kan fortsette å misbruke NAV sitt system.

10.3. Case 3

John har D-nummer og vil opprette sin egen bedrift og svindle NAV via denne. Først må han registrere bedriften. På www.brreg.no finnes alle opplysningene som kreves ved oppretting av bedrift.

Det koster nesten ingenting å opprette et enkeltmannsforetak i Norge. Ved registrering av foretak kreves D-nummer. Hvis John har allerede et D-nummer kan han da bruke Altinn.no for å sende samordnet registermelding for oppretting av bedrift eller han kan sende papirskjemaet. Hvis han ikke har et D-nummer må han sende søknad til

Brønnøysundregistrene med kopi av falskt pass. Han bruker blanketten "Anmodning om tildeling av D-nummer som kan lastes ned fra Brønnøysund nettside [63].

Brønnøysundregistrene sender så skjemaet til Personregisteret som tildeler D-nummer til John. Med D-nummer John kan registrere en bedrift og ansette flere fiktive personer. Han sender melding til NAV om at han vil ansatte flere arbeidstakere og sender falske kopier av pass for alle. NAV risikerer dermed å rekvirere D-nummer til fiktive personer som kan utnytte NAV sitt system som beskrevet i case 1.

11. Resultater

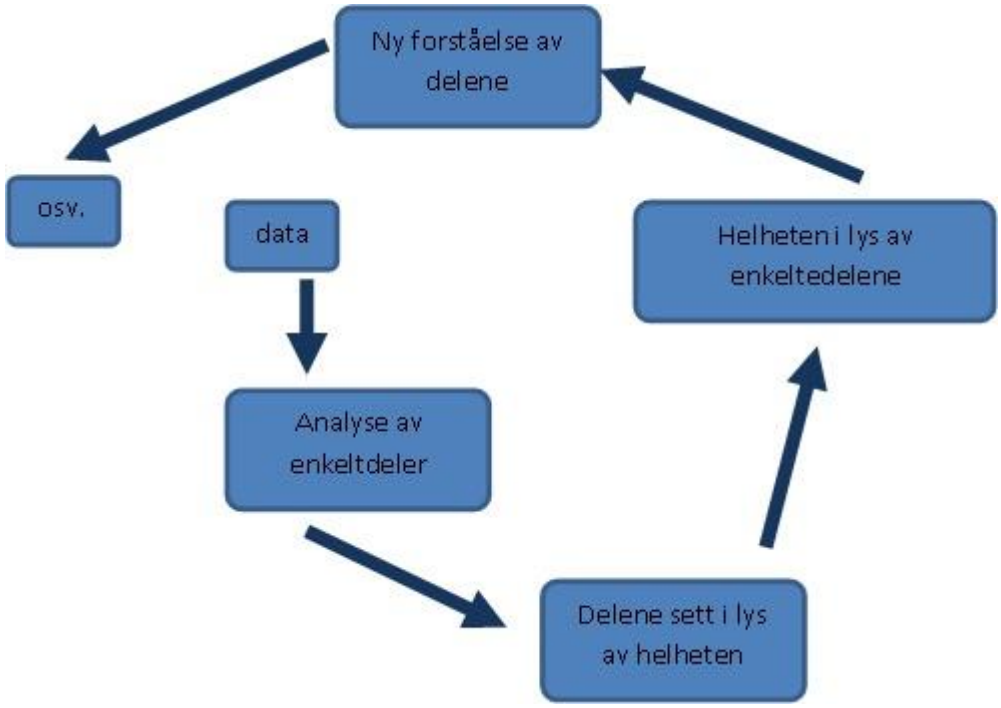
Før intervjuene trodde jeg at det skulle bli vanskelig å intervjue personer som kunne oppfatte det slik at jeg lette etter svakheter i deres system ved rekvirering av D nummer. Jeg prøvde å starte samtalen uten noen form av begrensninger eller føringer. Jeg presenterte problemstillingen på generelt grunnlag og forklarte mitt formål med oppgaven. Samtidig via casene som var beskrevet i kapitel 10 prøvde jeg å visualisere problemstiling.

Hos alle de jeg intervjuet fant jeg en felles forståelse rundt problemet og alle mente at dette er et viktig tema og en utfordring som de er godt kjent med.

Ved valg av spørsmål jeg har fokusert på å undersøke relevante fakta og å avklare mine observasjoner når det gjelder hvordan rekvirenter rekvirer D-nummer. Jeg har tenkt gjennom spørsmålene for å avklare rutiner og utfordringer som har jeg observert, samtidig som jeg prøvde å finne ut hvorvidt det finnes en felles forståelse av problemet.

11.1. Analyse av data

Etter intervjuene har jeg samlet all informasjon og startet med analysen, som hadde en kvalitativ tilnærming. Med dette mener jeg at jeg sammenstilte forskjellige intervjuer og prøvde å finne mønstre i svarene fra rekvirentene. Jeg konsentrerte meg om de sentrale detaljene som jeg måtte trekke fram. For å finne en kobling mellom detaljene og helheten brukte jeg metoden som Jacobsen 2005 beskriver som hermeneutisk metode. Hermeneutisk metode har en spiralform som kan illustreres:



Figur 11-1 . Hermeneutisk metode (Jacobsen 2005)

Jacobsen 2005 sier også at analyse av kvalitative data kan deles i 3 steg:

- Beskrive
- Systematisere og kategorisere
- Sammenbinde

Gjennom spørsmålene som intervjuobjektene fikk av meg og deres i utgangspunktet klare svar klarte jeg å redusere uoversiktlig informasjon. Ved å kategoriserer spørsmålene i forskjeliger temaer prøvde jeg å danne kategorier som jeg hadde tenkt å bruke for å sammenligne dataene fra alle intervjuene, i forsøk å finne mønstre i svarene.

Disse kategorier med følgende sporsmål er:

Rekvirering av D-nummer rutiner:

- Hvordan oppfatter dere utfordringene omkring D-nummer?

- Hvilke rutiner har dere ved rekvirering av D nummer?

- Hvordan sikrer dere rutinene ved rekvirering av D nummer?

Identitetskontroll ved rekvirering av D-nummer:

- Klarer dere å gjennomføre god identitetskontroll ved rekvirering av D-nummer?

- Har dere tilstrekkelig kompetanse for å foreta identitetskontroll ved rekvirering av D-nummer?

Informasjonsutveksling mellom etater

- Følger dere de endringene som Skatteetaten implementerte ifbm med nye rutiner for å hindre ID-tyveri og ID-svindel (Skatteetaten har ikke fått dette spørsmålet)

- Hvordan samarbeider dere med andre offentlig etater for å hindre ID-tyveri?

- Hvordan opplever dere kommunikasjonen mellom etater ifbm med D-nummerutfordringen?

Jeg fikk intervjue representanter fra NAV, Brønnøysundregistrene, Sentralskattekontoret for utlandssaker (SFU) ,Folkeregisteret og FNO (Finansnæringens hovedorganisasjon). Resultatene nedenfor beskriver svarene fra de forksjelige rekvirentene og viser deres oppfatning av problemet.

11.2. Resultater fra NAV

NAV har rekvirert over 150 000 D-nummer i løpet av de siste 5 årene. Det er en av de etatene som rekvirerer flest D-nummer i Norge. For NAV er det nødvendig å rekvirere D-nummer slik at de kan registrere personer som har krav på ytelser. Hele datasystemet i NAV er bygget opp slik at de knytter saker mot personnummer eller D-nummer.

NAV sier at de er klar over utfordringen ved D-nummerrekvirering. De sier at de vet om eksistensen av risiko i dagens ordning som kan resultere med generering av falske identiteter. NAV opplyser at de har liten erfaring med misbrukssaker knyttet til falske D-nummer men at de har eksempler der personer er dømt for trygdemissbruk som er knyttet til oppretting av fiktive identiteter. Alle disse sakene gjelder imidlertid misbruk av personnumer og ikke D-nummer. Men selv om de ikke har opplevd misbruk av D-nummer i stor grad, ser de en del utfordringer

når det gjelder ajourhold av opplysninger om D-nummerpersoner i DSF etter at D-nummeret er tildelt.

Når det gjelder beskrivelse av NAVs rutiner ved D-nummerrekvirering ser vi at det er ganske tydelig at de følger kravene for tildeling av D–nummer nøye. Disse kravene er bestemt i forskrift av 9. november 2007 nr. 1268 om folkeregistrering § 2-5 til 2-7. De har etablert rutiner for rekvirering i henhold til folkeregisterforskriften.

NAV prøver å hindre manipulering av blanketten for rekvirering av D-nummer slik at den ikke er tilgjengelig på internett og at den bare finnes på NAV sitt intranett. Selv om NAV prøver å beskytte seg mot eventuell misbruk av blanketten er det rimelig grunn til å tro, at med 18 000 ansatte i NAV, er det ganske stor risiko for at selve blanketten kan lastes ned fra intranett og kan bli tilgjengelig utenfor NAV sine lokaler.

Rutinene for rekvirering av D-nummer vurderes og oppdateres ved endring av forskriftene. I praksis implementeres rutinene slik at saksbehandler i utgangspunkt sjekker at brukeren har alle dokumentene på plass og at kopier er stemplet med rett kopi.

Når det gjelder identitetskontroll av dokumentene som er nødvendig ved rekvirering av D-nummer ser NAV at det er en vanskelig oppgave. Det krever resurser og nødvendig opplæring som de har ikke per i dag. Å avdekke falske identifikasjonsdokumenter er nesten umulig. Det er ganske begrenset i hvilken grad identitetskontroll utføres. NAVs saksbehandlere sjekker gyldighet av pass og at bilde i passet stemmer med personen som krever D-nummer.

Å avsløre falske identitetspapirer er vanskelig uten spesialkompetanse. Dette bekreftes av at politiet uttaler at det også er krevende for drevne etterforskere å avdekke falske dokumenter. Det er derfor en viss risiko for at NAV ikke oppdager falske identitetspapirer med dagens ordning.

At det ikke er noe krav om personlig oppmøte for at de skal tildele D-nummer, medfører at det ikke er mulig å foreta noen kontroll av selve legitimasjonsdokumentet. Videre innebærer det at det ikke foretas noen kontroll av at innehaver av legitimasjonsdokumentet er den samme person som på legitimasjonsdokumentet og dette øker risikoen for feil rekvirering av D-nummer.

Ved spørsmål om de endringene som Skatteetaten implementerte ifbm med nye rutiner for å hindre ID tyveri og ID svindel svarer NAV at de jobber med å forbedre interne rutiner knyttet til rekvirering av d-nummer. Det er ikke besluttet hvordan NAV skal forholde seg til de nye

rutinene i Skatteetaten. Skatteetaten uttaler selv at andre etater ikke må legge deres identitetskontroll til grunn, men gjennomføre egen kontroll. Selv om de ikke har besluttet hvordan de skal forholde seg til endringene, har de et godt samarbeid med Skatteetaten både på direktoratsnivå og på operativt nivå ved NAV Kontroll.

NAV opplever at det er økende oppmerksomhet rundt D-nummerordningen både i forvaltningen og i politisk ledelse og det er en positiv trend framover som skal hindre ID tyveri i stor grad.

Selv om NAV prøver å hindre identitetstyveri ved å etablere rutiner som følger lovverket viser de at manglende ressurser og kompetanse kan medføre at identitetstyveri ikke er synlig hos dem. Vi kan si at NAV følger lovverk ifbm med rekvirering av D–nummer, men med dagens identitetskontroll har de begrenset mulighet for å hindre identitetstyveri

11.3. Resultater fra Brønnøysund register

Brønnøysundregistrene kan rekvirere D-nummer fra Det sentrale folkeregisteret. Dette fremgår av forskrift om folkeregistrering § 2-7 jf. § 2-6.

Vilkåret for at Brønnøysundregistrene skal rekvirere D-nummer er dersom en utenlandsk person uten norsk fødselsnummer trenger D-nummer i forbindelse med registrering i Brønnøysundregistrene.

Som rekvirent er Brønnøysundregistrene sin rolle kun å avdekke et behov for D-nummer i forbindelse med registrering. Rekvisisjon av D-nummer i Enhetsregisteret og Foretaksregisteret skjer kun i forbindelse med registrering, det vil si enten ved at søknaden kommer samtidig med at de mottar en melding om registrering i Enhets- og/eller Foretaksregisteret, eller at det klart kommer frem i søknaden at det gjelder personer som har eller skal registres med rolle i Enhets-/Foretaksregisteret.

Rekvisisjon av D-nummer i Løsøreregisteret eller Ektepaktregisteret skjer kun når søknad om D-nummer kommer sammen med dokumentet som skal tinglyses i Løsøreregisteret eller i Ektepaktregisteret.

Hvis behovet for D-nummer er oppfylt krever Brønnøysundregistrene utfylt skjema ”Anmodning om tildeling av D-nummer med nødvendige kopier av legitimasjonsdokument. Normalt vil det være pass og nasjonalt ID-kort som inneholder de nødvendig opplysninger nevnt ovenfor. Etter hovedreglen skal dokumentet være utstedt av offentlig myndighet men de vurderer dette kun på et formelt grunnlag, det vil si

ved å forholde seg til innholdet i de dokumentene som de mottar og legger til grunn at innholdet stemmer med de faktiske forholdene.

Brønnøysundregistrene er kun rekvirent av D-nummer. De sier veldig klart at deres rolle er å påse at den dokumentasjon som kreves etter forskrift om folkeregistrering § 2-7 er vedlagt. Brønnøysundregistrene sender nødvendig dokumentasjon til Personregisteret i Hammerfest for tildeling av D-nummer. I følge Brønnøysundregistrene er det Personregisteret som har formalkontrollen og som godkjenner eller avviser tildeling av D-nummer jf forskrift om folkeregistrering § 2-8.

Det føres en begrenset kontroll da Brønnøysundregistrene kun er rekvirent av D-nummer. Brønnøysundregistrene har anledning til å rekvirere D-nummer uten at den som skal tildeles nummeret møter fram personlig. Brønnøysundregistrene har derfor ikke en mulighet til å foreta en reell legitimasjonskontroll ved rekvireringen all den tid personlig oppmøte ikke er påkrevd. Med en slik begrenset kontroll, er risikoen for at de rekvirerer D-nummer på grunnlag av falske legitimasjonsdokumenter derfor til stede. De kjenner ikke til at vi har rekvirert D-nummer på bakgrunn av falske legitimasjonsdokumenter, men kan heller ikke utelukke det.

Tidligere har det vært liten kommunikasjon mellom etater angående D-nummerordningen. Da det nå har vist seg at stadig flere ønsker å komme seg inn i det norske systemet ved bruk av falsk identitet, har også Brønnøysundregistrene merket en økt interesse og behov for kommunikasjon etatene imellom. De har inntrykk av at det er satt fokus på å stramme inn ordningen for rekvisisjon og tildeling av D-nummer.

Pr i dag er det kun de som skal ha D-nummer og skattekort som må møte opp på skattekontoret og vise frem gyldig legitimasjon. Økt oppmøteplikt og sikkerhetstiltak hos noen rekvirenter kan medføre at misbrukstilfellene vil øke hos Brønnøysundregistrene og andre rekvirenter for de med falsk legitimasjon.

Brønnøysundregistrene sier at det kan være et behov for at rekvirentene får et reelt ansvar for identitetskontroll. Men dette innebærer at rekvirentene må ha en bredere formell og reell kompetanse, og tilgang til relevant informasjon for å kunne vurdere fremlagt dokumentasjon. En slik oppgave bør derfor profesjonaliseres hos en, eller et fåtalls instanser.

11.4. Resultater fra FNO

Bankene utsteder i utgangspunktet bankkort for å identifisere sine egne kunder. For å opprette konto i banken må personen ha fødsels- og personnummer eller D nummer. Personer som ikke har en av de to identifikatorer må de henvise til Skateetaten eller bankene selv må sende rekvisisjon til Personregisteret. Bankene har lagt vekt på opplæring av ansatte for å sjekke pass og andre legitimasjonsdokumenter som de krever før de sender rekvisisjon videre. De har implementert dataverktøy for sjekking av utenlandske reisedokumenter, de har installert UV – lys ved kopimaskin og i kasse på nesten alle lokalkontorer.

"Vi observerer personens reaksjonsmønster når vedkommende blir kontrollert og ved tvil ber vi om å få beholde passet en dag for ytterligere kontroll. Men vi har begrenset mulighet til å verifisere et dokument og en identitet, dette gjelder spesielt mot utenlandske statsborgere"

sier Einar Jørgenrud [27] som jobber i sikkerhetsavdelingen i Sparebank 1 gruppen, med særskilt fokus på hvitvasking, ID-tyveri og fysisk sikkerhet.

Her vi ser at banknæring har investert mer i tekniske utstyr en de fleste offentlige etater for å sjekke identitetsdokumentene før de sender rekvisisjon for D nummer videre. Grunnen er den nye hvitvaskingsloven som trådte i kraft i 2009. Formålet med hvitvaskingsloven er å bekjempe hvitvasking[28] av utbytte fra straffbare handlinger. Selve loven medfører en rekke forpliktelser som bankene er pålagt å etterleve. De sentrale plikter i henhold til loven er:

- - Identitetskontroll
- - Registrering og oppbevaring av opplysninger
- - Undersøkelses- og rapporteringsplikt
- - Interne kontroll- og kommunikasjonsrutiner

Bankene følger direktivene som gjelder identitetskontroll svært nøye. Ved etablering av kundeforhold krever bankene gyldig legitimasjon av

[27] Idtyverikonferansen Oslo 2010

28 Hvitvasking er å sikre utbytte fra straffbar handling. (www.hvitvasking.no)

kunden og i fleste tilfellene personlig oppmøte. Som gyldig legitimasjon regnes alltid fysisk legitimasjon.

Bankene, slik som offentlig etater, krever at legitimasjonsdokumentene fremlegges i original eller unntaksvis bekreftet kopi.

For juridiske personer (bedrifter som skal opprette bankkonto) fastsetter forskriften følgende krav til legitimasjonsdokumenter:

- For juridisk person registrert i Foretaksregisteret skal det fremlegges firmaattest som ikke er eldre enn 3 måneder
- For juridisk person registrert i Enhetsregisteret men ikke skal Foretaksregisteret det fremlegges utskrift fra Enhetsregisteret som ikke er eldre enn 3 måneder
- Juridisk person som ikke er registrert i Enhetsregistert men som er registrert i annet offentlig register, skal dokumentere lignende, entydig identifiserende kjennetegn, opplysninger om navn (firma), forretningsadresse eller hovedkontor og eventuelt utenlandsk organisasjonsnummer, og opplyse om hvilket offentlig register som kan verifisere opplysningene
- Dersom juridisk person ikke er registrert i et offentlig register, skal det kreves legitimasjon for en fysisk person på vegne av juridisk person i henhold til lovens § 5 og § 6
- Legitimasjon fremlegges av den eller de som har disposisjonsrett over konto eller depot, eller som har rett til å gjennomføre transaksjoner

Her ser vi at bankene følger forskriften og krever flere offentlig dokumenter før de endelig godtar persons eller bedrifts identitet.

Ved spørsmål om ansvar ved tildeling av D-nummer eller utsettelse av andre dokumenter som kan bevise identitet er FNO veldig klar at det er offentlige myndigheter som har ansvar for dette. Når bankene krever D-nummer ved oppretting av bankkonto for privatpersoner mener de at personregisteret har ansvaret for identitetskontrollen og ikke bankene. Aud Helen Rasmussen som jobber i DnB NOR som informasjonssjef og hu sier under intervjuet at de rekvirer veldig få D-nummer. Årsaken er at de har ikke mulighet til å sjekke kundens identitet. De har dårlig erfaring med en albansk liga som klarte å lure DnB NOR med falske pass fra Belgia, Italia og Bulgaria. I 2010 anmelde de 95 saker til politi og i 2009 rundt 80 tilfeller. Derfor har de valgt å nekte å godta pass fra disse landene for å skaffe D-nummer. Hun er veldig klar over problemet og sier at det er oppgave for politi og ikke for bankene til å sjekke disse dokumentene.

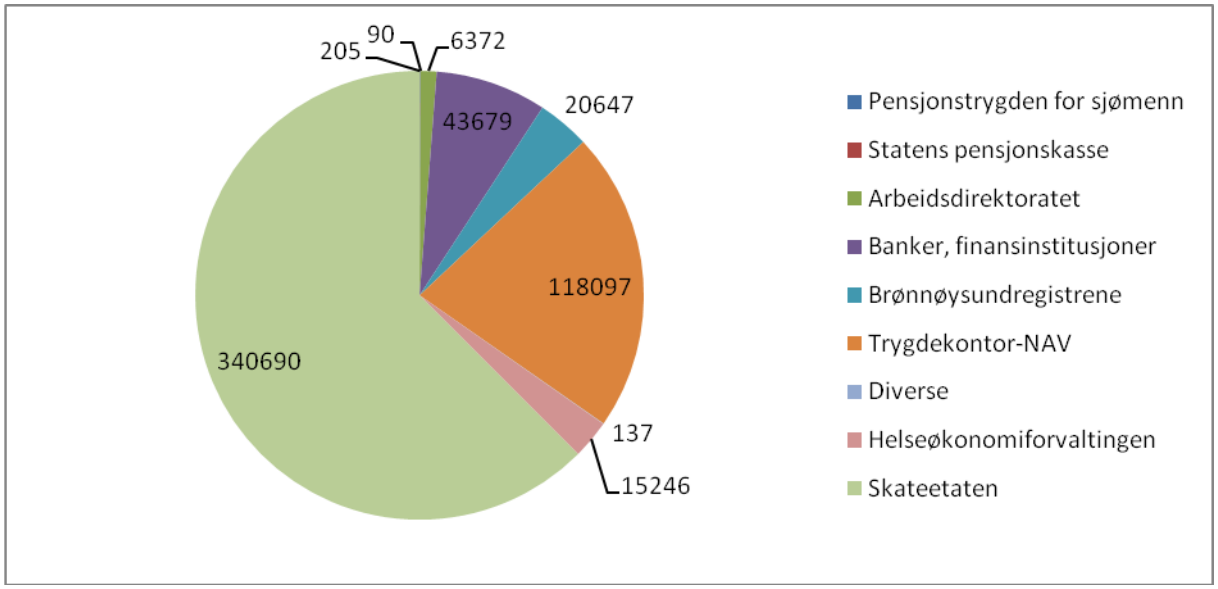
FNO har ikke myndighet til å si hva bankene bør gjøre men de sender råd, tips og anbefalinger til bankene. De påpeker også at ved oppretting av bankkonto må alle komme med pass og at bankene ikke aksepterer bankkort som identifikasjonsbevis og stiller spørsmål hvorfor offentlig etater gjør dette. Ved å ikke rekvirere D-nummer til personene som bankene ikke klarer å gjøre en god identitetssjekk på, mener FNO at bankene viser samfunnsansvar.

Jeg prøvde å få litt mer statistikk fra FNO når det gjelder D-nummer rekvirering og ID-tyveri saker. Grunnen til at jeg har lett etter disse tallene fra FNO er fordi alle bankene som jeg hadde kontakt med nektet å gi meg eksakte tall. De har sagt at de har meldt alle saker og tall til FNO som de har rapporteringsansvar. Svaret fra FNO er at vi ikke kan stole på tallene fordi det finnes egentlig en veldig forskjellig forståelse omkring hva egentlig ID-tyveri hos bankene er. I tillegg til at det ikke i noe lovverk finnes en definisjon på hva identifikasjonskontroll er kompliserer saken ved rapportering.

Bankene samarbeider med andre banker via FNO og klarer å følge retningslinjene ved oppdagelse av ID-tyveri. Alle sakene anmeldes til politiet. De viser store interesse å få tilgang til databaser som kan hjelpe de i saker hvor de klarer ikke å gjøre en identitetssjekk. Tilgang til databaser som viser stjålne pass er ett av ønskene som FNO mener kan hjelpe bankene mot ID-tyveri.

11.5. Resultater fra Skateetaten

Skatteetaten er en norsk statlig etat med ansvar for folkeregistrering. Personregisteret er en del av Skatteetaten som har formelt ansvar for å generere fødselsnummer og D-nummer i Norge. I begynnelsen av intervjuet kom de med statistikk vedrørende D-nummer rekvirering.



Figur 11-2 Rekvirering av D nummer i perioden 2005-2010, Skatteetaten

Figure 16 viser totalt antall tildelte D-nummer på bakgrunn av rekvisisjon fra alle rekvirenter i perioden 2005 til og med 2010. Her ser vi at det er skatteetaten som rekvirer flest D-nummer i Norge. Vi ser også at en av de største rekvirentene er NAV og finansinstitusjonene.

Det er også et viktig tall som Personregisteret har kommet fram til og det er det faktum at siden de fikk ansvaret for tildeling av D-nummer har de tildelt totalt 1 454 212 D-nummer. Alle de D-numrene står per dags dato aktive i Det Sentrale Folkeregister.

Personregister kommer ganske åpent med påstand om at det finnes store svakheter ved dagens rutiner ved rekvirering av D-nummer hos alle rekvirenter. De sier at det finnes eksempler hvor rekvirenter sender rekvisisjon på enkelte personer som egentlig ikke trenger D-nummer. De påpeker også under intervjuet at det er rekvirentene som har ansvar for rekvirering og identitetskontroll og ikke Personregisteret. Selve rutinene ved rekvirering av D-nummer hos Skatteetaten er under revisjon og per i dag det finnes en felles gruppe som under Finansdepartementet vil vurdere rutiner ved rekvirering av D-nummer og bruk av fødsels og personnummer. Ved mottak av rekvisisjon fra rekvirent har ikke Personregisteret myndighet til å stoppe prossessen. De reagerer bare hvis de oppdager manglende dokumentasjon eller ved oppdagelse av dubletter (hvor rekvirent sender rekvisisjon for person som allerede har en D-nummer), men selve identitetskontrollen og

dokumentasjonssjekken må skje hos rekvirentene og ikke hos Personregisteret. De sier også at det ikke finnes en veldig definert rolleavklaring mellom rekvirent og Personregisteret som har ansvar for selve generering og tildeling av D-nummer. Personregister påpeker at rekvirenter har behandlingsansvar ved rekvirering av D-nummer.

Store tall viser at D-nummer registeret er et statisk register. Dette betyr at det ikke finnes oppdateringsrutiner når et D-nummer er generert. Ved endring av adresse, navn osv hos personer som har fødsels- og personnummer er de pålagt med forskrift om folkeregistrering at endringene må meldes til Personregisteret. Det gjelder ikke for personer med D-nummer. Dette betyr at hvis for eksempel en person med D-nummer dør blir ikke dette registrert i Det Sentrale Folkeregisteret. Politiet sender melding til Personregisteret ved utreise eller bortvisning for personer som har fødsels- og personnummer men ikke for personer med D-nummer. Derfor har vi i Norge nesten 1,5 millioner aktive D-nummer. Hvor mange av de D-nummer som er reelt aktive kan ikke Personregisteret svare på.

Ved spørsmål om hvorfor Personregisteret ikke krever bilde av personer som skal få D-nummer slik at identitetskontrollen kan bli bedre for andre private og offentlig etater som bruker folkeregister data, svarte de at det må gjøres store lovendringer som kan godkjenne en slik rutine.

Personregisteret mener at det er behov for en stor revisjon av rutiner ved D-nummerrekvirering og at dette er en felles utfordring for hele norske samfunnet og at med mandatet fra Finansdepartementet de og andre aktører i gruppa skal forsøke å finne en bedre løsning ved rekvirering av D nummer.

12. Konklusjon

Identitetstyveri er en form av kriminalitet som er etablert i verden og Norge er ikke noe unntak. I Norge opplever vi at kriminelle miljøer som har som formål å bruke forskjellige metoder for ulovlig anskaffelse av personopplysninger er etablert. Som i resten av verden, Norge har de samme utfordringene for å hindre denne type kriminelle handlinger.

Konsekvenser i offentlig etater er ikke synlig i same grad som i andre land. Grunnen er at det ikke finnes en statistikk som kan vise frem dette problemet. Det er et stort behov for norsk statistikk, da ID-tyveri hittil ikke har vært definert som kriminelt og ingen har tatt initiativ til å etablere statistikk på dette tidligere.

Med denne oppgaven prøvde jeg å vise frem metoder som svindlerne bruker til å utnytte offentlige etater. Oppgaven hadde også som formål å undersøke hvordan rekvirering av D-nummer skjer i Norge via forskjellige rekvirenter. Antagelsen var at rekvirering av D-nummer på grunn av dårlig identitetssjekk kan være en inngangsdør for kriminelle som kan ha en stor konsekvens for hele det norske samfunnet. Nesten alle rekvirenter fremhever at denne risikoen finnes hos dem. Svake rutiner og ikke minst en udefinert rolle som rekvirenter har per i dag i lovverket kan ha konsekvenser i framtiden. Vi opplever at offentlige etater og andre rekvirenter på egen hånd forsøker å minimisere risiko men at de ikke klarer det i vesentlig grad på grunn av forskjellige roller som de har i samfunnet og forskjellige meninger om hva som menes med identitetskontroll ved D-nummerrekvirering.

Vi også opplever at offentlig etater i Norge ser identitetskontrollen som en ”tilleggsoppgave” og at de fleste ikke klarer å skille mellom fremvisning og kontrollering av identitetsdokumenter. Nesten alle rekvirenter, spesielt offentlige etater har fokus på fremvisning i større grad enn kontroll. Grunnen er at det mangler reell kompetanse og tilgangene til relevant informasjon for å kunne vurdere fremlagt dokumentasjon.

Gjennom oppgaven ser vi at spørsmålet om hvem som har ansvaret for å kontrollere en identitet før rekvirering av D-nummer fortsatt er uklart. Det er åpenbart at en definert identitetskontroll krever høyt kvalifisert personell med god kunnskap til fenomenet dokumentforfalsking. Per i dag er det slik at alle rekvirenter mener at kunnskapen om dette

fenomenet er veldig lav hos saksbehandlere i forskjellige etater og private aktører som kan rekvirere D-nummer. Det kreves at saksbehandlere og andre aktører som kan rekvirere D-nummer har nødvendig kunnskap, verktøy og klare rutinebeskrivelser for å gjennomføre en identitetskontroll og en dokumentasjonskontroll.

Mellom etater og andre aktører som kan rekvirere D-nummer må det etableres en full forståelse om konsekvensene ved rekvirering av D-nummer med dagens rutiner. Gjennom casene prøvde vi å vise frem konsekvensene. En rekvirent kan rekvirere D-nummer i henhold til sitt formål uten å vite at de kan lett misbrukes hos andre etater. Derfor må en økt forståelse og et tettere samarbeid mellom rekvirenter etableres på et høyere nivå. Dette er ikke en enkel oppgave fordi det kreves resurser og tid, men er nødvendig for å hindre en av de viktigste første steg mot et ID-tyveri. Med en gang et D-nummer er etablert hos en svindler har det åpnet seg en mulighet for misbruk.

Det er klart at det er viktig å endre lovverket slik at det bli enklere å definere roller og plikter ved rekvirering av D-nummer. Klare definisjoner og rutiner kan pålegge rekvirenter å gjennomføre identitetskontroll og dokumentasjonskontroll fra en felles standard som må etableres hos alle rekvirenter. Ikke bare vil loven da gjøre det lettere å veilede rekvirenter til hva de må gjøre, men det vil også gi oss en mer entydig definisjon av identitetstyveri.

Vi konkluderer tilslutt med at det er behov for mer statistikk når det gjelder ID-tyveri i Norge, det er behov for ytterligere sikring og tiltak mot identitetstyveri i Norge som kan komme via D-nummer tildeling. En felles plattform ved etablering av rutiner ved rekvirering av D-nummer hos alle rekvirenter vil øke tilliten mellom offentlig etater og vil tette hullene i systemet som svindleren kan finne per i dag.

Ikke minst må dialog mellom rekvirenter, og da spesielt mellom offentlig og privat sektor, finne sted. Utveksling av erfaringer og oppdatering av rutiner er viktige oppgaver som rekvirentene står fremfor.

Det er ingen enkel oppgave, men vi mener at dette er første trinn i riktig retning for å minimalisere mulighetene for misbruk av offentlige etater i Norge.

Referanser:

[1] FTC (Federal Trade Commision) http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (sist lest 07.05.2011)

[2] http://www.datatilsynet.no/templates/article____1891.aspx (siste besøkt 07.5.2011)

[3]http://www.nav.no/Om+NAV/Tall+og+analyse/Annen+statistikk/Misbruksstatistikk/Misbruksstatistikk/975+personer+anmeldt+for+trygdebedrageri.265689.cms (siste besøkt 07.5.2011)

[4] http://www.dn.no/forsiden/politikkSamfunn/article1825228.ece (siste besøkt 25.04.2011)

[5] http://www.nettavisen.no/okonomi/article2727087.ece (siste besøkt 13.05.2011)

[6] (Flerkulturell forståelse, Thomas Hylland Eriksen (red.)TANO Aschehoug 1997)

[7] Peter Steiner has been reproduced cartoon on page 61 of July 5, 1993 issue of The New Yorker

[8] Oklahoma University Police Department. "Identity Theft – Part 1 – Introduction to Identity Theft – The Police Notebook" 18 October 2004.URL: http://www.ou.edu/oupd/idtheft.htm (siste besøkt 07.5.2011)

[9] Organisasjonen for økonomisk samarbeid og utvikling 2009:16

[10] Identitetstyveri- Peter Kruize2009 , Københavns Universitet Det Juridiske Fakultet

[11] SIFO Oppdragsrapport 2-2010, Lisbet Berg og Ragnhild Brusdal

[12] http://www.oa.no/nyheter/article3793715.ece (siste besøkt 17.04.2011)

[13] http://www.dn.no/forsiden/politikkSamfunn/article1825228.ece (siste besøkt 25.04.2011)

[14]http://www.nav.no/Om+NAV/Tall+og+analyse/Annen+statistikk/Misbruksstatistikk/Misbruksstatistikk/975+personer+anmeldt+for+trygdebedrageri.265689.cms (siste besøkt 25.04.2011)

[15] http://www.cippic.ca/documents/bulletins/Techniques.pdf (siste besøkt 07.5.2011)

[16] http://www.vg.no/nyheter/innenriks/artikkel.php?artid=10014266 (siste besøkt 07.5.2011)

[17] http://www.fno.no/no/Hoved/Aktuelt/Aktuelle-FNO-brev/Aktuelle-FNO-brev-2011/Problemer-knyttet-til-forfalskning-av-faktura-og-forslag-til-tiltak/ (siste besøkt 14.01.2011)

[18] http://www.lovdata.no/cgi-wift/wiftldles?doc=/app/gratis/www/docroot/lr/lra/la-2010-190988.html&emne=skimming*&& (siste besøkt 05.04.2011)

[19] http://www.politikkavisen.no/arbeiderpartiet__Dno/_Regjeringen-foreslr-kriminalisere-enhver-anskaffel.php (siste besøkt 11.06.2011)

[20] http://www.camelspit.org/handyswipe/ (siste besøkt 05.04.2011)

[21] http://www.tyner.com/magnetic/compare.htm (05.04.2011)

http://www.incodenet.com/magnetic/miniport-comparison.htm

http://www.hackershomepage.com/

http://bcdata.com/portablemsr.html

http://www.mag-stripe.com/portable.htm

[22]http://www.europol.europa.eu/publications/Annual_Reports/Europol_Review_2009.pdf (siste besøkt 08.04.2011)

[23] http://www.tv2nyhetene.no/innenriks/krim/advarer-mot-nye-skimmingbander-3218481.html (siste besøkt 08.04.2011)

[24]http://www.finanstilsynet.no/no/Artikkelarkiv/Pressemeldinger/2011/1_kvartal/Ny-risiko--og-sarbarhetsanalyse-om-finansforetakenes-bruk-av-informasjons--og-kommunikasjonsteknologi-IKT-lagt-fram/(siste besøkt 13.04.2011)

[25]http://www.finanstilsynet.no/Global/Venstremeny/Rapport/2011/ROS_analyse_2010.pdf (siste besøkt 13.04.2011)

[26] https://www.politi.no/vedlegg/lokale_vedlegg/oslo/Vedlegg_1080.pdf (siste besøkt 13.04.2011)

[27] Collins, J.M. and Hoffman, S.K.,"Identity Theft: Predator Profiles", submitted to Security Journal (2004). Manuscript available from JudithCollins - judithc@msu.edu.

[28] Neil Sutton, "Canadian financial institutions among global leaders in security", http://www.itbusiness.ca/it/client/en/home/News.asp?id=39775&cid=7 (siste besøkt 13.4.2011)

[29] http://www.secretservice.gov/press/pub2304.pdf (siste besøkt 13.04.2011)

[30] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf (siste besøkt 17.04.2011)

[31] https://www.altinn.no/upload/Altinn_Etatsbrosjyre_web.pdf (siste besøkt 17.04.2011)

[32] http://www.washingtonpost.com/wp-dyn/content/article/2005/05/24/AR2005052401347_pf.html (siste besøkt 17.04.2011=

[33] http://www.skatt.no/skatt/nyheter_arkiv/sendte_ut_/?utskrift=1 (siste besøkt 17.04.2011)

[34] http://www.stortinget.no/no/Saker-og-publikasjoner/Saker/Sak/?p=28724 (siste besøkt 22.03.2011)

[35] http://www.stortinget.no/no/Saker-og-publikasjoner/Saker/Sak/?p=36474 (siste besøkt 22.03.2011)

[36] http://www.regjeringen.no/pages/13353964/politiet_2010.pdf (siste besøkt 22.03.2011)

[37] http://e24.no/lov-og-rett/politidirektoratet-mener-skattelister-utpeker-ransofre/3439768 (siste besøkt 22.03.2011)

[38] http://www.tv2nyhetene.no/innenriks/forbruker/posten-frykter-tyveri-av-selvangivelsen-3448828.html(siste besøkt 22.03.2011)

[39] http://www.nrk.no/nyheter/norge/1.7644021(siste besøkt 22.03.2011)

[40]http://h40059.www4.hp.com/cybereurope/Kit4and5PonemonExecSummary.pdf (siste besøkt 18.05.2011)

[41]http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf (siste besøkt 19.05.2011)

[42] Kaplan, A. M. & Haenlein, M. (2009) Users of the world, unite! The challenges and opportunities of Social Media. Kelley School of Business, Indiana University. Science direct.

[43] http://www.facebook.com/note.php?note_id=10150140568281509 (siste besøkt 23.05.11)

[44] http://www.p4.no/story.aspx?id=280344 (siste besøkt 23.05.11)

[45] http://www.aftenbladet.no/utenriks/Avlyste-angrep-etter-Facebook-lekkasje-1904636.html (siste besøkt 24.05.2011)

[46] http://www.norsis.no/nyheter/2010-11-25-124000-ID-tyveri-ofre.html (siste besøkt 24.05.2011)

[47] http://www.skatteetaten.no/no/Alt-om/Folkeregistrering/Fodsel/ (siste besøkt 25.04.2011)

[48] http://www.ii.uib.no/publikasjoner/texrap/pdf/2008-370.pdf (siste besøkt 25.04.2011)

[49]http://www.skatteetaten.no/no/Bibliotek/Publikasjoner/Pressemeldinger/2011/Nye-rutiner-for-skattekort-til-personer-med-D-nummer/ (siste besøkt 25.04.2011)

[50] http://www.regjeringen.no/upload/JD/Vedlegg/ID-kort-Sluttrapport.pdf (siste besøkt 25.04.2011)

[51]http://www.lovdata.no/cgi-wift/wiftldles?doc=/app/gratis/www/docroot/all/nl-20090306-011.html&emne=hvitvaskingslov*&& (siste besøkt 25.04.2011)

[52] http://www.hvitvasking.no/Lov-og-forskrift/Hvitvaskingsloven/Identitetskontroll/ (siste besøkt 25.04.2011)

[53] www.brreg.no/blanketter/veiledning/pdf/veil_samord.pdf (siste besøkt 25.04.2011)

[54] Skateetaen skandale, http://www.dinside.no/787026/anmelder-skattedirektoratet)(siste besøkt 22.04.2011)

[55] Årsmelding for regnskapet 2010 www.nav.no/Om+Nav

[56] http://www.dn.no/forsiden/utenriks/article2103632.ece (siste besøkt 26.04.2011)

[57] http://www.dinside.no/826669/forbloffende-lett-aa-bli-lurt (siste besøkt 22.04.2011)

[58]http://www.politikkavisen.no/www_uis_no/0102_11748_12310464_45_39_77_523_1040_792_EUTF8.html (siste besøkt 22.04.2011)

[59] http://www.ssb.no/aarbok/tab/tab-089.html (siste besøkt 22.04.2011)

[60] http://www.ssb.no/statsborger/tab-2010-05-27-01.html (siste besøkt 22.04.2011)

[61]http://www.udi.no/Oversiktsider/Statistikk-og-analyse/Statistikk-/Asyl/Asylsoknader-fordelt-pa-statsborgerskap/Asylsoknader-fordelt-pa-statsborgerskap-2000-2009/ (siste besøkt 22.04.2011)

[62] Id Tyverikonferansen 2010, Daniel Jan Jusowitsky og http://www.tv2nyhetene.no/innenriks/simone-parisi-jobbet-ni-aar-under-falskt-navn-3181402.html (siste besøkt 22.04.2011)

[63] http://www.brreg.no/blanketter/d-nummer_last_ned.html (siste besøkt 22.04.2011)