Københavns Universitet
Det Juridiske Fakultet

Identitetstyveri

Peter Kruize
Oktober 2009

Indholdsfortegnelse

Forord

Forhåndenværende rapport om identitetstyveri har været en udfordring på mange måder. Ikke kun for politifolk og anklagere er det svært at omstille sig til kriminalitet i den virtuelle verden, men det samme gælder for kriminologer. Det har været en interessant rejse gennem informations-teknologiske begreber og konstruktioner.

Som ikke-jurist har det også været en udfordring at få nogenlunde styre på de juridiske aspekter i forbindelse med identitetstyveri. I denne forbindelse vil jeg gerne takke Vagn Greve og Mads Bryde Andersen for deres hjælp. Ansvar for teksten ligger selvfølgelig hos mig.

Udviklinger relateret til identitetstyveri går hurtigt. Jeg har forsøgt at være up to date, men jeg vil ikke udelukke at jeg har mistet initiativer på denne front.

Projektet er økonomisk støttet af Justitsministeriets Forskningspulje.

Peter Kruize,
Jægerspris, 16. oktober 2009.

KAPITEL 1

Indledning

Bedrageri i millionklassen
Det er en 24-årig mand fra Randers, der nu er anklaget for op mod 250 tilfælde af databedrageri for over en million kroner begået fra september til december sidste år. Den 24-årige var i den periode postbud i Vorup, en forstad til Randers, og via sit arbejde tilegnede han sig identifikationspapirer, som han brugte til at flytte otte personers folkeregisteradresse til et sommerhusområde på Norddjursland. Han købte postkasser som han opstillede ved otte tomme sommerhuse - og derefter bestilte han diverse betalingskort som han så brugte. Derudover har han åbnet disse personers breve med dankort og tilegnet sig de oplysninger, der gjorde det muligt at købe varer ved brug af kortene. Det gik dog ikke i længden; folk fattede mistanke og henvendte sig til politiet, som ved hjælp af et samarbejde med Post Danmark afslørede den 24-årige i fredags, da han stod og tømte en af sine falske postkasser. Manden er også sigtet for den 29. februar at have stjålet fire postsække fra et depot i Vorup ved brug af en nøgle han havde fra sin tid som postbud. Han skulle angiveligt bruge brevene til at skaffe sig flere ID-papirer til oprettelse af flere falske folkeregisteradresser. Den 24-årige erkendte samtlige forhold og blev i lørdags varetægtsfængslet i fire uger.
Kilde: Thomas Bansø, TV2 Østjylland, 10. marts 2008

1.1 Begrebet identitetstyveri

Begrebet 'identitetstyveri' er godt i gang med at finde fast fodfæste i det danske sprog. En søgning på Google giver 31.000 hits på dette begreb. I langt de fleste tilfælde bliver identitetstyveri brugt i forbindelse med internet(handel). Internettet er uden tvivl en vigtig katalysator, hvad angår misbrug af en anden persons identitetsoplysninger, men at sløre sin egen identitet har altid været en del af den kriminelle verden. I denne forbindelse bliver der talt om online og offline identitetstyveri. Ifølge en amerikansk offerundersøgelse fandt kun 10 procent af det samlede antal identitetstyverier i 2006 sted online, mens 90 procent fandt sted ved konventionelle metoder, det vil sige offline (OECD, 2009, s.39-40). Tal fra det samme forskningsinstitut viser imidlertid at online identitetstyveri er voksende for i 2008 ligger andelen allerede på godt 20 procent (JSR, 2009).

Identitetstyveri er et ofte anvendt begreb, men der er ikke en almen accepteret definition af begrebet. Juristerne Tranberg & Langsted bruger begrebet identitetstyveri som synonym for

phishing i deres bidrag til bogen 'Internetretten'. Phishing beskrives snævert i deres fremlægning: "Kort beskrevet går det ud på, at svindlere forsøger at franarre brugere af internettet deres kreditkort- eller bank-oplysninger." (Tranberg & Langsted, 2008, s. 537). Der findes imidlertid ikke en juridisk definition af identitetstyveri. Juridisk set er identitetstyveri et misvisende begreb. Ordet tyveri lægger op til, at en person ejer sin identitet som man ejer en materiel ting (Prins & Van der Meulen, 2006). Rigsadvokaten tilkendegiver på spørgsmål fra retsudvalget, at "en falsk profil på internettet, hvor man udgiver sig for at være en anden eksisterende person, som udgangspunkt ikke i sig selv kan anses for strafbar." (JM, 2009, s. 1-2).

Rådet for IT-sikkerhed definerer identitetstyveri som følgende:

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

Ifølge denne definition er der to led i forbindelse med identitetstyveri: (1) at tilegne sig en andens personoplysninger og (2) at udgive sig at være denne person. Rådet for IT-sikkerhed tilslutter sig dermed, ved denne definition, måden hvorpå identitetstyveri ofte defineres internationalt. McNally & Newman (2008) påpeger, at der ikke er konsensus om definitionen af identitetstyveri, men at begrebet generelt refererer til en situation, hvor en person anvender en andens personlige oplysninger til at begå svig eller misbrug. Også OECD kommer frem til den konklusion, at der ikke findes en internationalt accepteret definition, og kommer selv frem til følgende beskrivelse (OECD, 2009, s. 16):

> 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.

Ifølge McNally & Newman bliver identitetstyveri (identity theft) og identitetssvig (identity fraud) ofte brugt som synonymer. Binder & Gill (2005) definerer identitetstyveri (identity theft) som det at overtage og misbruge en anden persons identitet, mens de definerer identitetssvig (identity fraud) som det at antage en fiktiv identitet. Binder & Gill påpeger, at "unfortunately, when you review the legislation, many times the term identity theft appears to be used interchangeably with the term identify fraud." (Binder & Gill, 2005, p. 8). I Europols Organised Crime Threat Assessment (OCTA) bliver identitetssvig både betragtet som misbrug af rigtige personoplysninger og misbrug ved hjælp af fiktive oplysninger, mens identitetstyveri retter sig kun til misbrug af rigtige personoplysninger.[1]

[1] "Identity fraud is defined as the use of false identifiers, fraudulent documents, or a stolen identity in the commission of a crime. Identity fraud is broader than identity theft in that identity fraud refers to the fraudulent use of any identity, real or fictitious, while identity theft is limited to the theft of a real person's identity."(Europol, 2006, p. 18).

Det diskuteres også, hvorvidt kortsvindel hører under begrebet identitetstyveri. Særligt repræsentanter fra finansverdenen mener, at det ikke burde være sådan (se fx Cheney, 2005, p. 2). Denne diskussion er specielt aktuelt i USA, og The Federal Identity Theft and Assumption Deterrence Act fra 1998 inkluderer kortsvindel i begrebet identitetstyveri.[2]

Frygt for identitetstyveri er overdrevet

I USA er frygten for identitetstyveri blevet så stor, at problemet nu er genstand for en hel industri, som tilbyder beskyttelse. Men tallene for, hvor mange der rent faktisk bliver udsat for identitetstyveri fortæller ikke hele historien. Når undersøgelserne viser, at 20 procent af befolkningen har været udsat for identitetstyveri, så skyldes det hovedsageligt, at tilfælde hvor et kreditkort er blevet tabt eller stjålet og siden misbrugt også tæller med. Virkeligheden ligner langt fra de scenarier, skræmmebillederne tegner, med spion-programmer på hjemmepc'en eller forbrydere, der gennemroder skraldespanden for at finde personoplysninger. Samtidig bliver størstedelen af pengene ved identitetskriminalitet stjålet ved hjælp af opdigtede identiteter og anslås at udgøre op mod tre fjerdedele af de penge, der bliver stjålet gennem identitetskriminalitet.

Kilde: Jesper Stein Sandal, Computerworld, 16. november 2005.

I denne rapport anvendes Rådet for IT-sikkerheds definition af identitetstyveri. Det betyder, at brugen af en *fiktiv* identitet ikke regnes under begrebet identitetstyveri. Anvendelse af en anden persons identitet begrænses ikke til den digitale, virtuelle verden; også misbrug i den reelle verden regnes under begrebet identitetstyveri.

1.2 Projektets formål og problemstillinger

Formålet med projektet er, at skabe overblik over fænomenet identitetstyveri. Det gælder begrebet i sig selv, men også omfang, udvikling, forebyggelse og bekæmpelse af identitetstyveri. Mere specifikt ses der nærmere på følgende problemstillinger:

- Hvordan foregår identitetstyveri og hvilke varianter findes der i praksis?
- I hvilket omfang er danskere udsat for former af identitetstyveri, og hvordan forholder Danmark sig internationalt?
- Hvilke forebyggende tiltag er indført i Danmark eller forventes indført på kort sigt?
- Hvad er forventningerne for de kommende år?

1.3 Undersøgelsesmetoder

Ved hjælp af litteraturstudier og internetsøgning er et overblik dannet over aktørerne og offentliggjorte oplysninger om former for identitetstyveri i Danmark. Oprindeligt var planen at holde

[2] Ifølge denne lov er der tale om identitetstyveri, når en person "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to id or abet, any unlawful activity that constitutes a violation of Federal Law."

interviews efterfølgende med repræsentanter for private og offentlige aktører, som har en central viden om (en form for) identitetstyveri. Gennemgang af tidsskrift- og avisartikler har imidlertid givet et godt indblik i potentielle interviewkandidaters syn på udviklingen. Derfor er der ikke holdt interviewsamtaler, men relevante aktører er blevet spurgt om supplerende oplysninger.[3] Der er søgt kontakt med:

- Københavns politi
- Rigspoliti (NITEC)
- Finansrådet
- DK•CERT

Derudover er der indhentet informationer direkte fra borgere (ofre). Justitsministeriet har tilbudt at tage spørgsmål omkring identitetstyveri med i deres løbende offerundersøgelse. Disse spørgsmål (se bilag 1) er stillet til 1.007 respondenter i marts 2009 og 846 respondenter i juni 2009 - i alt 1.853 respondenter.

Offerundersøgelsen er gennemført som et led i Danmarks Statistiks omnibusundersøgelser. Omnibusundersøgelsens deltagere udvælges tilfældigt via Danmarks Statistiks CPR-register, således at de udgør et repræsentativt udsnit af befolkningen afgrænset til personer mellem 16 og 74 år. Danmarks Statistik søger herefter efter personernes telefonnumre. Alle månedlige bruttostikprøver er på 1.700 personer. Heraf ekskluderes de, der viser sig at være emigrerede eller døde, samt de, der har meddelt Danmarks Statistik, at de ikke ønsker at blive ringet op med henblik på at deltage i undersøgelser, jf. herom senere. Den resterende del udgør nettostikprøven. Denne tæller omkring 1.500 personer hver måned. Det betyder, at nettostikprøven omfatter ca. 3.000 personer. Med 1.853 deltagere ligger svarprocenten på ca. 62 procent.[4]

Rapportens struktur

Rapporten er delt op i tre kapitler omhandlende forskningsresultater (2-4) og et afsluttende kapitel. I kapitel 2 ses der nærmere på de forskellige faser i processen ved identitetstyveri: tilegnelse af oplysninger, misbrug af oplysninger og følgerne af misbrug. Kapitel 3 har fokus på omfang, art og udvikling af identitetstyveri. Hertil benyttes adskillige kilder. Kapitel 4 giver overblik over myndighedens og private aktørers anstrengelser til at forebygge og bekæmpe identitetstyveri. I det afsluttende kapitel opsummeres resultaterne, drages konklusionerne og lægges op til diskussion.

[3] Desuden er der søgt kontakt til prof. Vagn Greve (strafferet) og prof. Mads Bryde Andersen (IT-ret) for at afklare enkelte basale juridiske spørgsmål.

[4] For mere detaljeret information vedr. stikprøven henvises til Balvig & Kyvsgaard (2009) Udsathed for vold og andre former for kriminalitet, s. 9-11.

KAPITEL 2

Identitetstyveri dissekeret

De forskellige varianter af identitetstyveri har det tilfælles, at specifikke identitetsoplysninger tilegnes af gernings-personen og at disse oplysninger bliver misbrugt på et senere tidspunkt. Det betyder, at der er en tidsforskel mellem tilegnelse og misbrug. Det tager også tid før forurettede finder ud af, at hans identitetsoplysninger er blevet misbrugt. I nedenstående skema ser tidsperspektivet ud som følgende:

(T1)	(T2)	(T3)
Tilegnelse af identitetsoplysninger	Misbrug af identitetsoplysninger	Følger af misbrug
----------O----------		----------O---------->
	begyndelse af viktimisering	opdagelse af viktimisering

Efter: McNally (2008, Figure 1, p. 35)

2.1 Tilegnelse af identitetsoplysninger

Der er mange måder, hvorpå gerningspersonen kan tilegne sig en andens identitetsoplysninger. Offentligt tilgængelige registre, som telefon og navneregister, indeholder oplysninger som navn, adresse og telefonnummer. Ved hjælp af for eksempel hjemmesiden www.krak.dk kan denne slags personoplysninger erhverves. Også stadigt flere borgere lægger frivilligt personoplysninger ud på egne websider eller på sociale netværksider som Facebook eller My Space.

Ved identitetsoplysninger tænkes automatisk på oplysninger tilhørende individuelle personer, men der findes også eksempler at virksomheder bliver udsat for identitetstyveri. I juni 2009 har den norske justitsminister Knut Storberget lanceret en internetside i forbindelse med et nationalt projekt til at bekæmpe identitetstyveri (www.idtyveri.info). På denne side bliver blandt andet virksomheder gjort opmærksom på risikoen af identitetstyveri: "Norske virksomheter handler hvert år for store summer og innkjøpsansvarlige har fullmakter til slik handel. Det handles på nettet, hos leverandører og i butikker. En fellesnevner for de fleste kjøpene er at man har fullmakt til å gjøre en slik handel. Det er eksempler på at en uvedkommende kartlegger hvem som har disse fullmaktene og forfalsker virksomhetens papirer for å svindle virksomheten. Ved

eksempelvis å forfalske en firmaattest kan en svindler klare å tilegne seg kreditt eller andre fordeler på vegne av virksomheten."

I nogle publikationer (fx OECD, 2009) skelnes der mellem online og offline identitetstyveri. Online identitetstyveri henviser til internettet eller en mobiltelefon. Computeren er tilsluttet internet, og dermed er det muligt at trænge ind i computeren og/eller kommunikerer med brugeren. Offline identitetstyveri indebærer, at der er tale om en handling i den fysiske verden. Dette kan godt være en teknisk handling, fx skimming.

2.1.1 Online tilegnelse af personoplysninger

Den mest omtalte metode til at tilegne sig identitetsoplysninger er phishing: at fiske efter personoplysninger i den digitale verden. Phishing kan ske på forskellige måder, og hver gang en ny metode opdages, bliver et nyt navn opfundet. I det hollandske 'Nationale Trusselbillede' (Nationale Dreigingsbeeld, NDB 2008, s. 204-206) beskrives følgende metoder:

- Phishing: en e-mail med et link til falsk webside hvor personlige oplysninger indtastes.
- Spear-phishing: mere personlig tilrettet e-mails med samme formål som phishing.
- Pharming: brugere som kontakter en institution eller virksomhed online bliver hemmeligt omdirigeret til en falsk webside. Denne omdirigering sker ved hjælp af malware (malicious software) som computeren er smittet med. Installation af malware sker ofte gennem e-mails, websider, at downloade software eller gennem søgemaskiner.
- Spy-phishing: malware lurer indtastninger på tastatur af.
- Vishing (phishing via VoIP – Voice-over-IP-systemer): i stedet for en falsk webside bliver telefonen brugt til at franarre oplysninger.
- SmiShing (phishing via sms): en sms med besked at sende oplysninger ind, eller en link til en falsk webside.

Ved phishing med henblik på identitetstyveri er formålet for det meste at få fat i kortoplysninger eller adgangskoder til en netbank. Gerningspersonen kan også tilegne sig kortoplysninger indirekte, det vil sige ved at købe oplysningerne. Der findes internetsider, hvor man for få penge kan købe kortoplysninger fra et land efter eget valg. I en DR-udsendelse, 'Testen – det usikre internet', (6. maj 2009) vises blandt andet, at det er muligt at købe kreditkortoplysninger på nettet. Ifølge Symantecs er det især østeuropæiske og russiske bander, der står bag hemmelige internetsider, hvor der handles med stjålne, personlige oplysninger (Ertmann, 2008). Også i chatrooms på internettet kan man lægge hånd på kredit-kortoplysninger som følgende eksempel illustrerer:

I efteråret 2003 i den lille østjyske by Hammel, tilhørende Silkeborg politikreds, deltog to-tre drenge på 14-15 år i edb-undervisningen på Søndervangskolen. Den ene af drengene, Lasse, er særdeles velbevandret i brugen af computere og internetmediet, og trods sin lave alder har han sit eget IT-supportfirma. Mens de deltog i undervisningen, surfede Lasse på internettet og søgte blandt andet på bogstaverne CCW, der i computerkredse er et kendt søgeord for at få adgang til forskellige chatrooms og servere. Samtidig downloadede han et hjælpeprogram betegnet MIRC, hvorefter han kunne logge sig på et bestemt chatroom. Det chatroom, Lasse besøgte, var et af de chatrooms, hvor 'hackere' lægger mange 'stjålne oplysninger' ud til gavn for andre med kriminelle hensigter. Efter at Lasse havde fundet frem til nogle af disse oplysninger, printede han dem ud. Det var kreditkort-oplysninger bestående af blandt andet kortnumre og udløbsdatoer, hvilket benyttes ved bestilling af varer på internettet, som Lasse havde sikret sig."
Kilde: Korsgaard, 2005, s. 9.

Denne historie finder sted i 2003 og det er et spørgsmål, om den slags informationer stadigt gratis bliver delt i chatrooms i anno 2009. Adskillige kilder peger på, at 'hacking for fame' et uddøende fænomen og på at 'hacking for fortune' er den dominante doktrin (se fx NDB 2008, s. 207). Mikko Hyppönen, research-chef for IT-sikkerhedsfirmaet F-secure, deler hackere op i to generationer. De fleste hacker-angreb i perioden 1986-2003 kom fra USA, Vesteuropa og Japan. Destruktiv virus blev spredt; hackere tjente ingen penge på dem, men gjorde det for sjov. Efter 2003 kommer angrebene primært fra Brasilien, Rusland og Kina, og der er millioner at tjene for hackere. "Vi kæmper ikke længere mod amatører, men organiserede professionelle. Mange samarbejder via nettet uden at kende hinanden. De har forskellige fagområder; nogle udvikler virussen, mens andre fx står for pengeoverførslerne." (Koszyczarek, 2009a)

Kreditkort- eller andre slags oplysninger kan også bliver stjålet fra en database eller et register. I givent fald bryder hackere ind i et computersystem, hvor disse data er gemt. Det kan fx være en webbutiks kundekartotek. På denne vis lykkedes det hackere i slutningen af 2008 at stjæle 95 million kreditkortinformationer fra Heartland (den amerikanske pendant af PBS). Ifølge F-secure lykkes det hackerne at komme ind ved hjælpe af et inficeret PDF-dokument. I maj 2009 oplyser F-secure, at hackere i høj grad er skiftet over til at anvende PDF-filer. I 2008 kom 29 procent af angrebene via en PDF-fil, mens andelen er steget til 49 procent i de første måneder af 2009. (Koszyczarek, 2009b)

2.1.2 Offline tilegnelse af personoplysninger

Kortoplysninger kan også komme gerningspersonen til kendskab ved 'fysisk' tyveri (taske- eller pungtyveri, indbrud) eller ved skimming. Ved skimming bliver enten den magnetiske strip på betalingskortet kopieret eller kortoplysningerne (kortnummer, udløbsdato og csc-nummer[5]) kopieres ved nedskrivning. Det sidste kan typisk ske i en restaurant eller i en butik.

[5] CSC-nummer står for Card Security Code

En anden kilde til tilegnelse af personoplysninger er affaldsposen. På engelsk tales om 'dumpster diving'. Ikke kun borgere, men også (offentlige) virksomheder smider ofte papirer i skraldespanden som indeholder svigfølsomme[6] og svigfarlige[7] oplysninger. Ifølge en undersøgelse, hvor affald fra 500 husstande er gennemsøgt, smider 71 procent af husholdninger i Holland svigfølsomme oplysninger i skraldespanden. En ud af ni husholdninger smider svigfarlige oplysninger væk (Fellowes Benelux, s. 4).

Endelig er postvæsenet en ofte nævnt metode i tilegnelsesprocessen af personoplysninger. Det kan være ved at stjæle post (lige som episoden med postbuddet, beskrevet i kapitel 1) eller ved at flytte en persons adresse og således modtage en andens post. Pr. 1. oktober 2009 indfører Post Danmark, at man skal legitimere sig ved flytning af adressen. Henrik Larsen fra Post Danmark siger til Lokal-Avisen: "Ved at bede kunder, der flytter til ny adresse, om at vise legitimation, hindrer vi misbrug af andres identitet, hvilket er hele formålet med de nye ordninger" (8. september 2009, s. 11).

2.2 Misbrug af identitetsoplysninger

Identitetsoplysninger kan blive misbrugt på mange forskellige måder. Meulen (2006) skelner mellem økonomisk og kriminelt misbrug. En tredje form af misbrug af identitetsoplysninger, som Meulen nævnes, kaldes identitetskloning. I sådan en situation overtager gerningspersonen en anden persons identitet totalt, som det skete for Angela Bennett (Sandra Bulllock) i filmen *The Net* (1995). Selv om jeg ikke vil udelukke, at der findes identitetskloning i realiteten, må det i hvert fald regnes for et yderst sjældent fænomen.[8] Der findes imidlertid også eksempler på identitetsmisbrug som ikke sigter efter økonomisk gevinst eller kriminelt misbrug, men som omfatter misbrug af en kendt persons navn i det offentlige rum. Selvom rigsadvokaten påpeger, at det at udgive sig for at være en anden eksisterende person som udgangspunkt ikke i sig selv kan anses for strafbar (JM, 2009, s. 1-2), anser jeg det som misbrug af identitetsoplysninger og kalder det for socialt misbrug.

2.2.1 Økonomisk misbrug af identitetsoplysninger

Meulen beskriver to basisformer for økonomisk misbrug af identitetsoplysninger. Den første form er kendt som 'account take over', hvor gerningspersonen misbruger en eksisterende bankkonto eller et kreditkort. Den anden form for økonomisk misbrug kaldes 'true name fraud' som henvises til situationer hvori gerningspersonen misbruger identitetsoplysninger til at oprette lån, bestille kreditkort eller erhverv formue på en anden måde på bekostning af ofret.

[6] Navn, adresse, bopæl.

[7] Kreditkort- eller kontooplysninger.

[8] "I England har enkelte borgere fået stjålet så mange oplysninger om deres identitet, at de har været nødt til formelt at erklære sig selv for 'afdøde' for at komme ud af problemet. Det kaldes 'pseudocide' (afledt af suicide) skrev Nyheds-avisen i oktober 2006." (Stove & Valeur, 2007, s. 37).

Ifølge Identity Theft Resource Center (ITRC) bliver 97 procent af ofrene for identitetstyveri udsat for berigelseskriminalitet. Misbrug af kreditkort er forbrydernes mest almindelige metode. Rapporten bygger på spørgeskemaer udfyldt af ofre for identitetstyveri (ITRC, 2008).

Tyve stjal Liselottes identitet

På det seneste har fremtidsforsker Liselotte Lyngsø modtaget ting, hun ikke selv har bestilt, for eksempel otte billetter til Roskildefestivalen, en ansøgning om et benzinkort, hvor der manglede en underskrift, og en bankkonto hos Nordea. Jeg har fået stjålet min identitet, siger Liselotte Lyngsø til DR-nyhederne. Hun blev helt tilfældigt klar over tyveriet, da et forsikringsselskab ville sætte hendes præmie op, fordi hun åbenbart var flyttet til et farligere område. Men Liselotte er ikke flyttet. Hun er blevet offer for en flok kriminelle, der uden hendes viden har flyttet hendes adresse til en tom lejlighed i Valby. De har købt en masse ting i hendes navn og med hendes penge. Det skyldes, at de kriminelle har fået fat i hendes cpr-nummer og har oprettet en bankkonto og fire mobiltelefonnumre i hendes navn.

Kilde: www.dr.dk/Nyheder/Indland/kriminalitet/2009/05/22/183407.htm

Ved økonomisk misbrug af identitetsoplysninger er det spørgsmålet, hvordan gerningspersonen tilegner sig penge, varer og/eller ydelser i en andens navn uden at kunne bliver sporet med det samme. Til dette formål bruges såkaldte muldyr: en person, der – bevist eller ubevist – hjælper gerningspersonen med at transportere penge eller varer ud af landet. Muldyret bliver typisk rekrutteret igennem spammail, som sendes ud til mange tusinde modtagere på samme tid. I mailen lokkes der med lette penge og et hurtigt udbytte. Typisk overføres stjålne penge til muldyrets konto, hvor efter pengene hæves i kontanter og sendes ud af landet. Herunder ses et eksempel på sådan en mail, der vil lokke muldyr til hæleri.

ARBEJDSTILBUD

Mine damer og herrer

Søger De en mulighed for at tjene penge? Vi tilbyder Dem at tjene lige så mange penge som De vil hurtigt og uden ekstra indsats. De skal bruge en bankkonto og 2-3 timers fritid om dagen. Vi overfører penge på Deres konto, sædvanligvis udgør det 30.000,00 DKK– 60.000,00 DKK, De hæver pengene og sender dem til os via Western Union. Deres løn udgør 20 procenter af det pengebeløb, der blev overført på Deres konto. For eksempel, vi overfører 30.000,00 DKK til Dem, De tjener 6.000,00 DKK med det samme, lige så snart pengene er ankommet på Deres konto. De kan også overlade os flere konti eller invitere Deres venner til samarbejde. Deres arbejdsløn afhænger kun af Deres behov og arbejdsvilje. Til at begynde samarbejdet bør De meddele os følgende data, som skal bruges til at overføre pengene: bankets navn, reg.nr. (nummeret på den bankafdeling hvor De har Deres konto), kontonummer, navn og efternavn af kontohaveren, Deres adresse: (land, postnr, by, vej, husnr), og et telefonnummer De kan kontaktes på. Vi skal ikke bruge personlig information om Dem undtagen den, der skal bruges til at gennemføre en standart bankoverførsel.

Kilde: Politiken, 21. januar 2009 (http://politiken.dk/incoming/article633230.ece)

2.2.2 Kriminelt misbrug af identitetsoplysninger

Ved kriminelt misbrug af identitetsoplysninger handler det ifølge Meulen (2006) om, at gerningspersonen anvender ofrets identitet, når personen bliver anholdt af politiet for en forbrydelse. Formålet med identitetsmisbrug er i dette tilfælde at undgå strafforfølgelse. Meulen tilfører, at denne form for anvendelse af identitetsoplysninger ikke er i fokus ved myndighederne og at dets omfang er ukendt.

Klerks (2009) beskriver enkelte eksempler på kriminelt misbrug af identitetsoplysninger i Holland. For eksempel blev en mand anholdt for besiddelse af børnepornografi, da hans kreditkortoplysninger var blevet brugt til at skaffe sig adgang til en internetsite med børnepornografi. Et andet eksempel, som Klerks nævner, stammer fra ombudsmanden. En hollandsk mands identitet blev misbrugt af narkoforbrydere og havde 43 forbrydelser stående på 'sit' navn. Ofret havde problemer med at rejse, har været anholdt flere gange og har været udsat for ransagning af sin bolig. Ombudsmanden var overrasket, hvor svært det var at rette op følgerne af dette misbrug, selvom ofret fik hjælp af myndighederne.

2.2.3 Socialt misbrug af identitetsoplysninger

Suzanne Bjerrehuus oplevede ligeledes misbrug af sine personoplysninger, da en person oprettede en profil med billeder af hende i hendes navn på Facebook. I en klumme skriver Bjerrehuus: "Det ubehagelige var alt det, han havde skrevet i mit navn". Hun har politianmeldt sagen, men hun fik meddelt at falske profiler på Facebook ikke er strafbart. (Bjerrehuus, 2008).

Bjerrehuus er ikke den eneste kendte dansker, der har oplevet misbrug af sine oplysninger. Chefredaktøren på Berlingske Tidende, Lisbeth Knutsen, oplever i maj 2007, at der blev sendt en stribe mails til personer i hendes adressekartotek, blandt andet med ordlyden: "Jeg vil gerne frabede mig alle jeres sleske e-mails." Knutsens computer var været genstand for en hacker som har overtaget hendes mail-identitet (Stove & Valeur, 2007, s. 37).

2.3 Følger af misbrug

Man kan læse mange skrækhistorier berettet af identitetstyveriets ofre. Ved misbrug af eksisterende konti eller kort lider ofrene for det meste intet økonomisk tab. Love om visse betalingsmidler "udsteder hæfter i forhold til brugeren for tab som følge af andres uberettigede anvendelse af et betalingsmiddel" (§ 11), medmindre brugere har vist grov uforsvarlig adfærd. I sådan et tilfælde hæfter brugeren med op til 8.000 kr. for tab (stk. 3). Dermed ligger risikoen for misbrug af kreditkort ved kortselskabet.[9]

Sagen er anderledes, når der oprettes lån eller en ny konto i ofrets navn. I sådan en situation er der generelt mere besværligt at bevise, at en anden person har misbrugt ens oplysninger. "En af de værste ting ved identitetstyveri er, at det er dig selv, som har bevisbyrden. Når tyven har brugt din

[9] Pr. 1 november 2009 bliver der indført en selvrisiko på 1.100 kr. ved misbrug af betalingskort.

identitet, er det svært at bevise, at du ikke er den kriminelle. Et offer for identitetstyveri føler sig ofte berøvet, ydmyget og magtesløs, for man kan ikke få hjælp nogen steder", siger Peter Steenstrup, som er administrerende direktør i rådgivningsvirksomheden Affinion International i Danmark, der udvikler programmer og forsikringer i samarbejde med banker, kreditkortudstedere og forsikringsselskaber (www.presswire.dk). Mulige indirekte omkostninger for ofrene af identitetstyveri er således et dårligt omdømme og svækket kreditværdighed.

KAPITEL 3

Omfang, art og udvikling af identitetstyveri

Omfanget af kriminalitet baseres typisk på anmeldelser til politiet eller på offerundersøgelser. Begge måleinstrumenter har sine fordele og ulemper. Offerundersøgelser kræver, at der er en forurettet part, som vil medvirke i et (telefon)interview. Dermed egner offerundersøgelser sig ikke til at måle omfanget af forbrydelser, der ikke har et direkte offer, fx hæleri eller spirituskørsel. Politiets anmeldelsesstatistik er ofte kun toppen af isbjerget. Afhængigt af borgernes anmeldelsestilbøjelighed afspejler politiets kriminalitetsstatistik en større eller en mindre del af kriminalitetens omfang. I tilfælde af identitetstyveri er det ikke kun politiets registre, der kunne være nyttige til at få en fornemmelse af omfang og udvikling, men også data fra de IT-relaterede myndigheder samt private virksomheder (fx finansielle institutioner) kunne være oplysende. Derfor er dette kapitel delt op i tre afsnit: offerundersøgelser, politiets anmeldelsesstatistik og andre kilder.

3.1 Offerundersøgelser

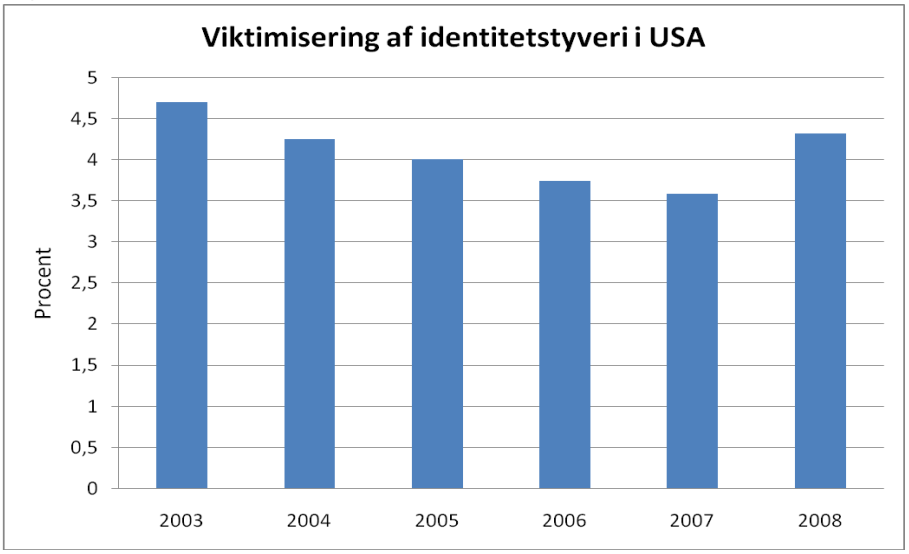
I første omgang ses på internationale offerundersøgelser og undersøgelser i andre vestlige lande. Bagefter præsenteres resultaterne af den første danske offerundersøgelse rettet mod identitetstyveri.

3.1.1 (Inter)nationale offerundersøgelser

Det er ikke mange offerundersøgelser som retter sig mod identitetstyveri. Undtagelsen er en serie undersøgelser af *Javelin Strategy & Research* (JSR) i USA. JSR har for sjette gang i træk foretaget en national repræsentativ stikprøve af næsten 4.800 voksne om dette emne. I perioden 2003-2008 har ca. 4 procent af alle voksne amerikanere, efter eget udsagn, været udsat for identitetstyveri. Figur 3.1 viser, at der er tale af en dalende tendens fra 2003 og til og med 2007. I 2008 er der tale om en stigning. Ifølge James Van Dyke, Javelins direktør, er denne stigning et resultat af den økonomiske krise. "The only thing we can logically attribute to that is the economy. If people need to make money, and decide to do so illicitly, identity fraud is the logical opportunity."
(www.identitytheftassistance.org)

4,32 procent af alle voksne amerikanere svarer til 9,9 million mennesker. JSRs forskere regner sig frem til et tab af 48 mia. dollars i 2008 på grund af identitetsmisbrug. Viktimisering sker oftere for borgere med en indkomst over 75.000 dollars, og aldersklassen '35-44 år' er den mest udsatte gruppe. Kvinder viser sig oftere at være ofre for identitetstyveri. Ifølge JSR er forklaringen kvinders brug af restauranter og butikker: "... increased focus on finding victims in stores and restaurants, where it said woman may spend more frequently."

Figur 3.1



Kilde: JSR 2009 Identity fraud Survey Report

I USA findes et *Identity Theft Assistence Center* (ITAC), og her er de, der henvender sig, blevet spurgt, hvordan deres identitetsoplysninger er blevet stjålet. Af de 1.530 adspurgte, kunne kun 28 procent svarer på dette spørgsmål. Resultaterne er følgende (www.identitytheftassistance.org):

- Venner, familie eller hjemansatte som har adgang til personlig information (27 %);
- Computer relateret (22 %);
- Stjålen eller tabte punge/taske (15 %);
- Korrupte virksomheder/ansatte (12 %);
- Misbrug af konsument data (5 %).

Nu er det svært at tolke overstående resultater, når 72 procent af ofre ikke har kendskab til gerningspersonens metode, men vi må antage, at kategorierne venner, familie eller hjemansatte og stjålen/tabte punge/taske er overrepræsenterede i denne oversigt.

Ifølge det amerikanske Bureau of Justice Statistics (2006) er tre procent af husstandene i USA i 2004 blevet udsat for en form for identitetstyveri. Det svarer til 3,6 millioner husstande. Identitetstyveri går især ud over yngre mennesker (18-24 år) i byer og forstæder. De mest udbredte former er misbrug af kreditkort (48 procent), misbrug af andre former for konti (25 procent) og misbrug af personlige, fortrolige oplysninger (15 procent).

I 2004-2005 ICVS og 2005 EU ICS[10] er der stillet enkelte spørgsmål vedrørende consumer fraud. Et af spørgsmålene retter sig mod creditcard fraud. Forberedelser for 2009 ICVS er i gang, men disse data er ikke tilgængelige på nuværende tidspunkt. Tabel 3.1 viser resultatet af spørgsmål vedrørende kreditkortsvindel. USA har den klart største andel af misbrug af kreditkort jævnfør denne statistik. I Europa gør der sig for de angelsaksiske lande et højere niveau af kreditkortsvindel gældende end for resten af det vestlige Europa. Danmark ligger i bunden sammen med de andre nordiske lande og Vesteuropas fastland.

Tabel 3.1 Misbrug af kreditkort i vestlige lande

Lande	Procent	Lande	Procent
USA	4,0 %	Nederlandene	0,4 %
England & Wales	1,7 %	Belgien	0,4 %
Skotland	1,4 %	Portugal	0,4 %
Grækenland	1,4 %	Frankrig	0,3 %
Nord Irland	1,3 %	Luxembourg	0,3 %
Irland	1,3 %	**Danmark**	**0,3 %**
Spanien	0,9 %	Sverige	0,3 %
Mexico	0,6 %	Italien	0,1 %
Østrig	0,4 %	Finland	0,0 %

Kilde: Van Dijk et al (2008, Table 15, p. 88)

3.1.2 Offerundersøgelse i Danmark

Som beskrevet i kapitel 1 er der gennemført en offerundersøgelse som et led i Danmarks Statistiks omnibusundersøgelser. Der er stillet spørgsmål omkring identitetstyveri (se bilag 1) til 1.007 respondenter i marts 2009 og 846 respondenter i juni 2009, i alt 1.853 respondenter. Af disse 1.853 respondenter angiver 20 personer, eller 1,08 procent, at de har været udsat for identitets-tyveri. Er dette tal repræsentativt for alle voksne borgere i Danmark, skulle der være omkring 47.850 ofre for identitetstyveri her i landet. Da opgørelsen er baseret på en stikprøve medfører dette en vis statistisk usikkerhed. Hvis stikprøven ikke har været selektiv, kan det fastslås, at antallet af ofre for identitetstyveri i Danmark med 95 procent sikkerhed ligger mellem 27.000 og 69.000 personer (se også tabel 3.2).

Tabel 3.2 Omfang af identitetstyveri

Omfang stikprøve	1.853
Antal udsatte for ID-tyveri	20
Procenttal af udsatte	1,08 %
Antal af udsatte i Danmark	47.850
95 % -interval	27.043 – 68.716

[10] ICVS står for International Crime Victims Surveys, og EU ICS står for European Survey on Crime and Safety.

De fleste forurettede har været udsat for misbrug af deres Dankort- eller kreditkortoplysninger. 14 ud af de 20 udsatte respondenter (70 procent) falder i denne kategori. En respondent er franarret sine bankoplysninger, mens to andre har oplevet, at deres personoplysninger (navn, cpr-nummer) er blevet misbrugt. To respondenter svarer 'andet' på dette spørgsmål. En respondent har været udsat for indbrud i sin computer (hacking) og alt mulige inlogkoder er blevet ændret. Den anden respondent svarer, at der er franarret fortrolige oplysninger over mobiltelefonen. Hvilke oplysninger er ikke oplyst (se tabel 3.3).

Når EU ICS resultatet – Danmark 0,3 procent misbrug af kreditkort i 2005 – skal sammenlignes med resultaterne af denne offerundersøgelse fra 2009, skal der regnes ud hvor står en procentdel står for misbrug af kreditkort (inkl. Dankort). 14 ud af 1.853 respondenter svarer til 0,8 procent. Nu er stikprøven begrænset og dermed den statistiske usikkerhed rimelig stor, men den forsigtige konklusion må være, at viktimisering af kreditkortmisbrug af steget i perioden 2005 – 2008.

Tabel 3.3 Kategori af identitetstyveri

	Antal	Procenttal
Dankort	9	45 %
Kreditkort	5	25 %
Bankoplysninger	1	5 %
Personoplysninger	3	15 %
Andet	2	10 %
I alt	**20**	**100 %**

Kort- og bankoplysninger bliver for det meste brugt til at købe på nettet. Oplysningerne bliver desuden anvendt til at hæve eller overføre penge eller til at shoppe i en butik. To respondenter, som angiver, at deres kort- eller bankoplysninger er stjålet, svarer 'andet' på spørgsmålet om, hvad oplysninger er blevet brugt til. I den ene sag er oplysningerne brugt til at betale motorvejafgift, mens respondenten i den anden sag ikke aner hvor oplysninger er brugt til (eller om de er anvendt). Tabel 3.4 giver en detaljeret oversigt.

Tabel 3.4 Misbrug af oplysninger

	At købe noget		Hæve eller overføre penge	Andet	I alt
	på nettet	i en butik			
Kort eller bankoplysninger	7	2	4	2	15
Personoplysninger	1	1	-	1	3
Andet	1	-	-	1	2
I alt	**9**	**3**	**4**	**4**	**20**

Respondenter opdager, at deres identitetsoplysninger er misbrugt enten når de bliver konfronteret med regningen – på en udskrift fra deres netbankkonto eller en opkrævning – eller når udstedere af kreditkort eller indblandede virksomheder tager affære. Tabel 3.5 viser en oversigt over, hvordan misbruget opdages. Ved 14 ud af de 20 respondenter er der lidt økonomisk tab for i alt 64.735 kr. En enkelt sag er atypisk med et tab på 23.000 kr. Når vi ser bort fra denne sag, ligger det

estimerede tab på landsplan på ca. 100 mio. kr. Ifølge PBS ligger det reelle tab ved misbrug af dankort på knap 40 mio. kr. i 2008 (se afsnit 3.3.3). Når vi tager i betragtning, at dankort udgør den største andel af betalingskortene i Danmark, virker et samlet tab på omkring 100 mio. kr. lidt urealistisk. I alt fire ud af de 14 respondenter med økonomisk tab skal selv betale (en del af) beløbet. I alt står borgerne for 5.050 kr. af det samlede tab på 64.735 kr. Det svarer til 8 procent af det samlede tab.

Tabel 3.5 Opdagelse af misbrug

	Udskrifter; netbank	Kort spærret	Opkræv-ning	Opringning; mail	I alt
Kort eller bankoplysninger	7	5	1	2	15
Personoplysninger			1	2	3
Andet				2	2
I alt	**7**	**5**	**2**	**6**	**20**

Respondenterne er også blevet spurgt, hvordan gerningspersonen har fået fat i deres oplysninger. Kun fire ud af de tyve respondenter har ingen anelse om det. Syv respondenter peger på deres computer som kilden til identitetstyveri: tre svarer, at de har været udsat for hacking, to mistænker en nethandel og to har været ofre for phishing (falsk hjemmeside). I tre tilfælde har gerningspersonerne fået fat på oplysningerne ved taske- eller lommetyveri. De resterende seks respondenter svarer 'andet' på spørgsmålet om gerningspersonens metode. Det handler om følgende hændelser: i et tilfælde har offeret tabt sit betalingskort, en respondent har været offer i udlandet, to respondenter er franarret oplysninger via deres telefon, en respondent er udsat for skimming og den sidste respondent peger på fængsel som metode. Det er uklart, hvad der menes med det.

Tabel 3.6 Metode til at få fat i identitetsoplysninger

	Computer	Tyveri	Andet	Ukendt	I alt
Kort eller bankoplysninger	6	3	3	3	15
Personoplysninger			2	1	3
Andet	1		1		2
I alt	**7**	**3**	**6**	**4**	**20**

Til sidst giver offerundersøgelsen et praj om den forurettedes profil. I tabel 3.7 sammenlignes fem karakteristika for respondenter, der har været udsat for identitetstyveri med karakteristika for respondenter, der ikke har været ofre for identitetstyveri. Også her gælder, at det er svært at drage konklusioner på grund af det begrænsede antal af forurettede. Men når det er sagt, ser det ud til, at mænd har en lidt højere risiko for at blive ofre for identitetstyveri end kvinder. Det samme gælder for dem, der er fraskilt. Alders- og indkomstmæssigt er der ingen forskel mellem forurettede og ikke-forurettede. Det viser sig heller ingen betydningsfulde forskelle imellem bopælsregionerne i forhold til risikoen for at blive offer for identitetstyveri.

Tabel 3.7 Karakteristika af forurettede og ikke-forurettede for identitetstyveri

	Forurettede ID-tyveri (n=20)		Ikke-forurettede ID-tyveri (n=1.833)	
Køn	Antal	Procent	Antal	Procent
Mand	12	60 %	870	47 %
Kvinde	8	40 %	963	53 %
Alder				
Gennemsnitligt	44,6 år		45,8 år	
Brutto indkomst (pers.)				
Gennemsnitligt	308.900		296.255	
Civilstand				
Gift	6	30 %	1.066	58 %
Ugift	6	30 %	566	31 %
Fraskilt	6	30 %	144	8 %
Andet	2	10 %	57	3 %
Bopælsregion				
Hovedstaden	7	35 %	531	29 %
Sjælland	2	10 %	250	14 %
Syddanmark	6	30 %	440	24 %
Midtjylland	2	10 %	426	23 %
Nordjylland	3	15 %	186	10 %

3.2 Politiets anmeldelsesstatistik

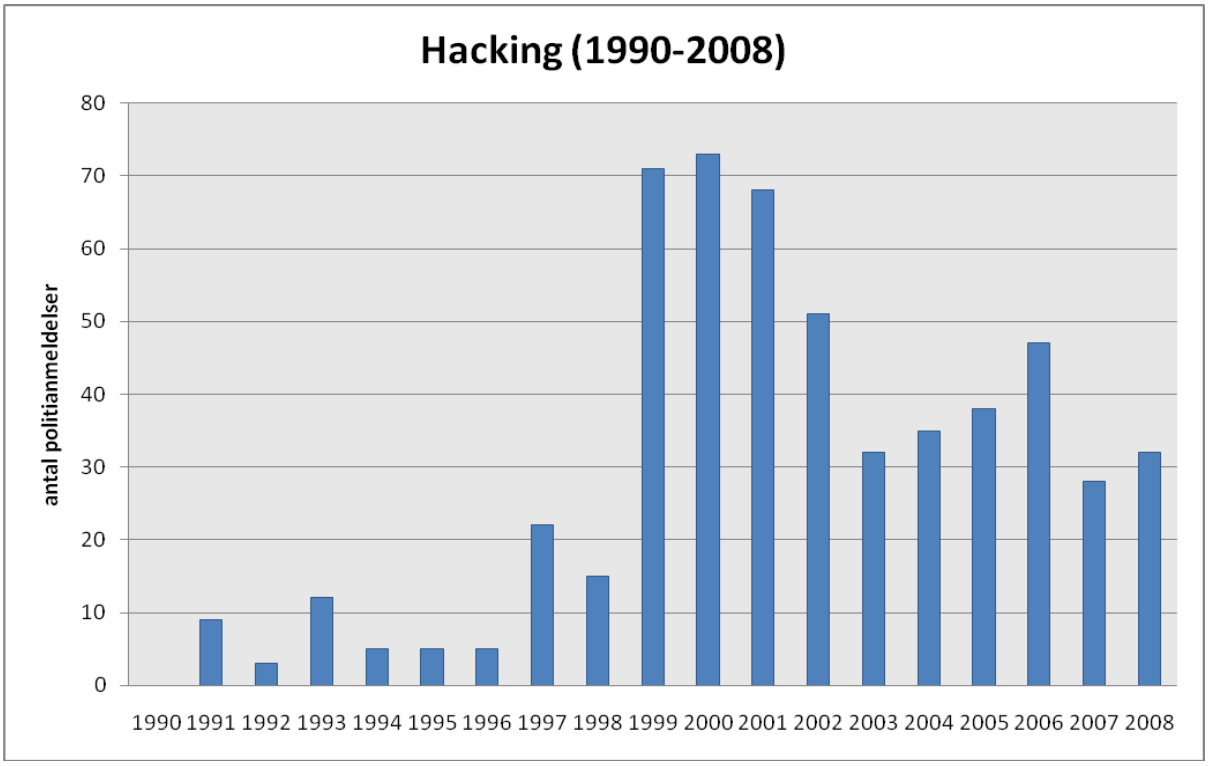
Politiets anmeldelsesstatistik er baseret på lovovertrædelser, og dermed er vi nødt til at finde ud af, hvilke lovbestemmelser der er relateret til identitetstyveri for at kunne sige noget om fænomenet på basis af politiets data. Problemet er, at identitetstyveri ikke er et juridisk begreb i Danmark. Udtrykket i sig selv er problematisk: kan man stjæle en anden persons identitet; med andre ord: kan man eje en identitet (ellers kan den vel ikke bliver stjålet). Problemet med politiets statistik er, at der i princippet ingen grænser er for, hvilke forbrydelser man kan begå ved at give sig ud for en anden. Også strafferetligt skelner jeg mellem tilegnelse af identitetsoplysninger og anvendelse heraf.

3.2.1 Tilegnelse af identitetsoplysninger

Tilegnelse af identitetsoplysninger kan, som beskrevet i kapitel 2, ske på mange måder. Hacking er en af metoderne og er strafbart jf. straffelovens § 263, stk. 2: Den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at blive brugt i et informationssystem, straffes med bøde eller fængsel i indtil 1 år og 6 måneder. Formålet med hacking er ikke altid at tilegne identitetsoplysninger, og dermed er det svært at tolke politi-anmeldelser for hacking i lyset af identitetstyveri. I kapital 2 er beskrevet, at der er sket et skift fra 'hacking for fame' til 'hacking for fortune'. Dermed forventes – men dokumenteres ikke – at de seneste års anmeldelser af hacking oftere er relaterede til tilegnelse af identitetsoplysninger end i starten.

Figur 3.2 viser udviklingen af politianmeldelser for hacking i perioden 1990-2008. Den bratte stigning i 1999 er i øjenfaldende. Ellers ser det – rent talmæssigt – ud at tendensen er lidt faldende i perioden efter 1999.

Figur 3.2



Er det svært at sige noget om tilegnelsen af identitetsoplysninger ved hacking uden at studere hver enkel politirapport, der er umuligt at sige noget om andre tilegnelsesmetoder (fx phishing, skimming eller tyveri) på basis af politiets anmeldelsesstatistik. I en redegørelse fra rigspolitiet for udviklingen i IT-kriminalitet samt den politimæssige indsats på området (uden dato) skrives at "politiet modtager stadig flere henvendelser vedrørende 'phishing', det vil sige forsøg på internettet på at franarre en person bl.a. bankoplysninger med henblik på misbrug af disse oplysninger." (Rigspolitiet, s. 3). I samme redegørelse oplyses, at rigspolitiets IT-efterforskningscentret (NITEC) har modtaget 117 henvendelser og anmeldelser vedrørende phishing i 2005 (i 2004 var antallet af anmeldelser kun 2).

3.2.2 Misbrug af identitetsoplysninger

Misbrug af identitetsoplysninger kan – ligesom tilegnelsesprocessen – berøre en række straffebestemmelser. Rigsadvokaten (2009) peger blandt andet på straffelovens § 264 d (uberettet videregivelse af meddelelser eller billeder vedrørende en andens private forhold), § 267 (ærekrænkelse) og § 279 (bedrageri). Rigsadvokatens svarer på et spørgsmål om falske profiler på

sociale netværkssider som Facebook og My Space og bemærker, at der er tale om et meget begrænset antal anmeldelser af den karakter.

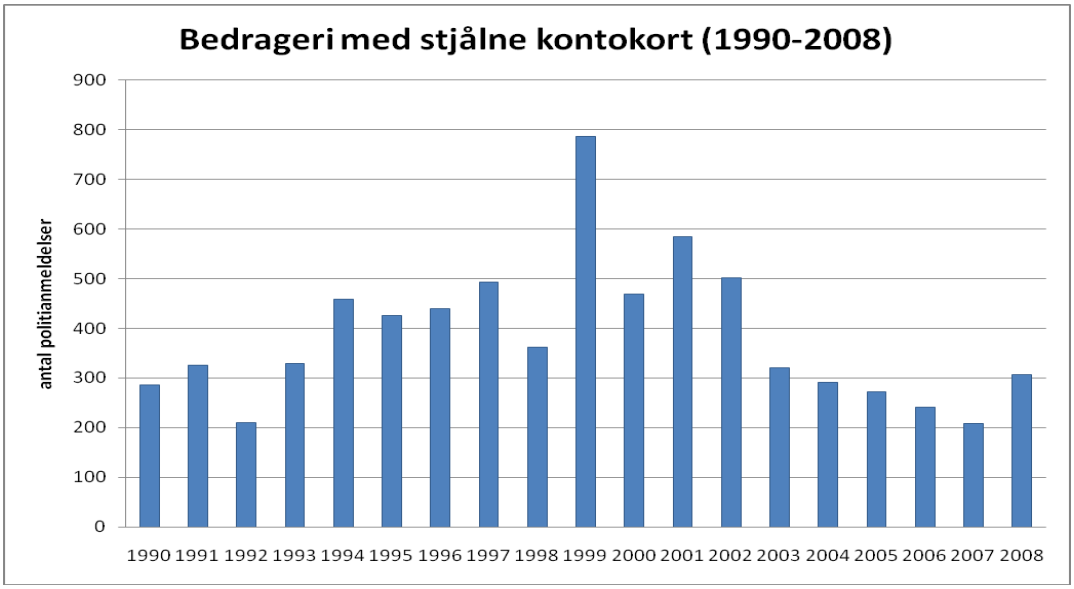
Det gælder ikke bedrageri. I 1985 er straffebestemmelsen om databedrageri (§ 279a) indført. Almindeligt bedrageri kræver, at der er nogen, der lider under en 'vildfarelse', og det kan ifølge lovgiveren ikke være en maskine. Derfor blev § 279a lavet. Der er imidlertid ingen tradition i Danmark for at lave specielle straffebestemmelser for forbrydelser, der er begået ved hjælp af tekniske indretninger. "Hvis man ringer til en anden og under telefonsamtalen narrer ham til at købe en værdiløs samling af rengøringsmidler, er det en overtrædelse af straffelovens § 279, ganske som hvis man havde stået ansigt til ansigt med den anden, medens man fyldte ham med løgn. Det vil heller ikke gøre nogen forskel, om man havde skrevet breve til ham og bundet ham samme historier på ærmet, lige så lidt som det vil gøre forskel, hvis man bruger nye kommunikationsformer som fx e-mails eller Messenger." (Tranberg & Langsted, 2008, s. 504).

I politiets anmeldelsesstatistik er bedrageri delt op i et antal kategorier, navnlig:

- Dankortovertræk, egen konto
- Øvrige kontokort, egen konto
- Øvrige kontokort, stjålne
- Checkbedrageri
- Øvrige bedrageri

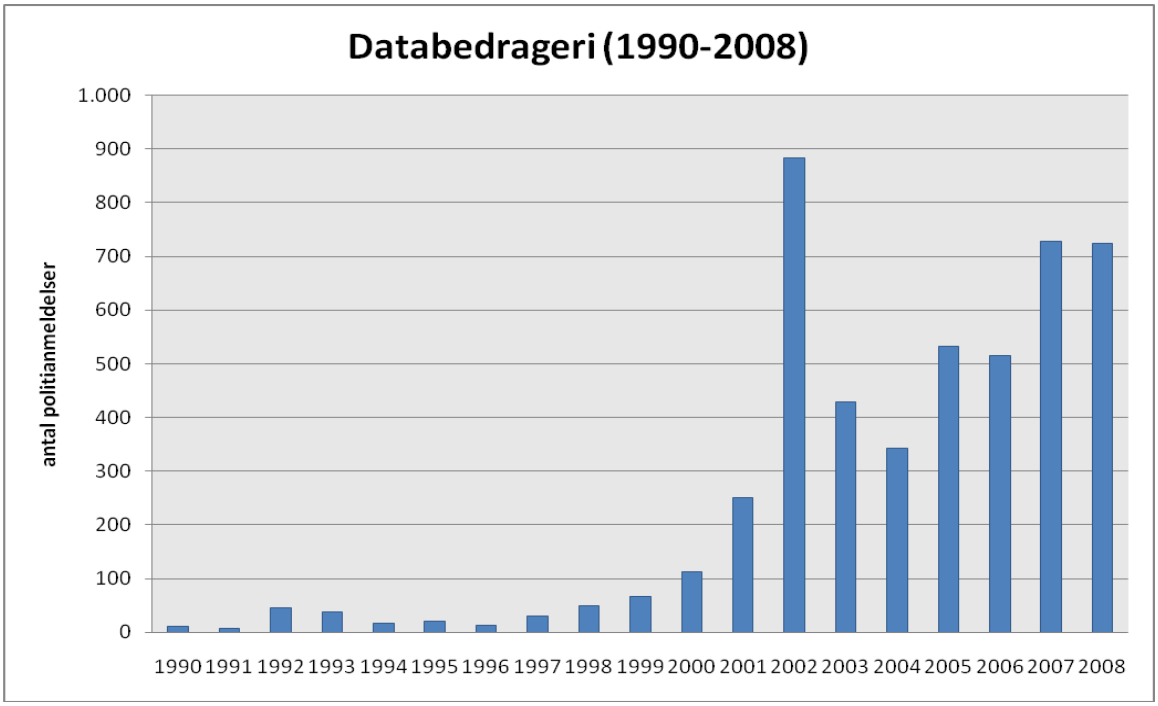
Den meste interessante kategori i forbindelse med identitetstyveri er stjålne kontokort. En persons kontokort er stjålet og gerningspersonen har begået bedrageri ved at anvende kortet. Figur 3.3 viser udviklingen i politianmeldelser for denne kategori. Til og med år 1999 er tendensen stigende, mens tendensen efterfølgende er faldende.

Figur 3.3



Udviklingen i antal politianmeldelser vedrørende databedrageri (§ 279a) er anderledes. Antallet af anmeldelser er ubetydeligt i den forrige århundrede, mens tendensen siden år 2000 er stigende. Figur 3.4 viser udviklingen. Antallet af anmeldelser i 2002 er iøjnefaldende. I den tidligere omtalte redegørelse fra Rigspolitiet vedrørende IT-kriminalitet peges på en forklaring på de afvigende antal af anmeldelser i 2002: "Antallet af anmeldelser for databedrageri efter straffelovens § 279a steg betydeligt i år 2002. Dette skal formentlig ses i lyset af befolkningens generelt øgede tillid til forretningssteder på internettet og den kraftige stigning i anvendelsen af kreditkort til køb af varer og tjenesteydelser på internettet. Den hastige udvikling i antallet af kreditkortbetalinger medførte en øget interesse fra kriminelle, som udnyttede den manglende sikkerhed på området. Med indførslen af kontrolcifre (CVV-kode) på nyudstedte Visa/Dankort fra april 2002 blev sikkerheden i forbindelse med brugen af betalingskort ved køb af varer og tjenesteydelser på internettet væsentligt forbedret. Pr. 1. februar 2005 var samtlige Dankort og Visa/Dankort udskiftet og bar således kontrolcifre." (Rigspolitiet, s. 2).

Figur 3.4



3.3 Øvrige datakilder

Der er søgt i tre retninger for at finde yderligere oplysninger, der muligvis kan kaste lys over omfang og udvikling af identitetstyveri, navnlig:

1. Myndigheder eller virksomheder med fokus på IT-sikkerhed
2. Myndigheder eller virksomheder med fokus på persondatabeskyttelse
3. Myndigheder eller virksomheder med fokus på finanser

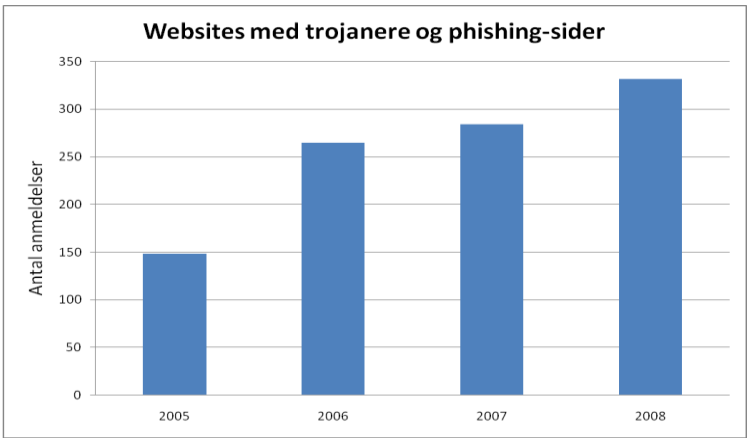
3.3.1 IT-sikkerhed

Der findes adskillige instanser inden for IT-sikkerhed som rådet for IT- og Persondatasikkerhed (www.it-sikkerhedsraadet.dk), IT- og Telestyrelsen (www.itst.dk) samt et hav af private virksomheder, som lever af salg af sikkerhedsprogrammer som F-secure og McAfee. I forhold til oplysningen i relation til omfang og udvikling af identitetstyveri er DK•CERT imidlertid det mest interessante.

DK•CERT, Computer Emergency Response Team i Danmark (www.cert.dk), er oprettet i 1991 som følge af en af Danmarks første hackersager. DK•CERT er en afdeling af UNI•C, Danmarks IT-center for uddannelse og forskning under Undervisningsministeriet. Missionen af DK•CERT er at skabe øget fokus på IT-sikkerhed gennem aktuel, relevant og brugbar viden. Dermed er DK-CERT i stand til at udsende advarsler om (potentielle) risici og sikkerhedsproblemer.[11] DK•CERT håndterer på årsbasis ca. 50.000 IT-sikkerhedshændelser. Langt de fleste anmeldelser handler om såkaldte portscanninger.[12]

DK•CERT modtager også anmeldelser angående danske websider med trojanere[13] og phishing-sider. I 2008 modtog DK•CERT 332 anmeldelser vedrørende inficerede danske websider. Figur 3.5 viser, at der er en stigende tendens i antallet af anmeldelser til DK•CERT.

Figur 3.5



Kilde: DK•CERTs Trendrappport 2008, s. 14.

[11] DK•CERT var blandt pionererne, der først i 90'erne tog initiativ til etablering af et internationalt samarbejde med grundidé i den amerikanske CERT Coordination Center (CERT/CC). Som led i det internationale samarbejde overvåger DK•CERT it-sikkerheden i Danmark (www.cert.org). DK•CERT er desuden medlem af Forum of Incident Response and Security Teams (FIRST), en international organisation med over 180 medlemmer fra hele verden (www.first.org).

[12] Portscanning har til formål at identificere sårbare services knyttet til åbne porte på internettet. En firewall lukker som udgangspunkt for adgangen til computernes åbne porte.

[13] Den trojanske hest er et program der har andre funktioner end dem som det foregiver at have, og indeholder enten spyware eller benyttes til at installere virus eller botter. Et botnet er et netværk af computere, som en angriber kan fjernstyre fra centralt hold. Ejerne af computerne ved ikke, at deres PC er inficeret med en bot og indgår i botnettet. Et botnet bliver bl.a. brugt til at udsende phishing-mails.

Ikke alle danske websider inficiret med trojanske heste eller phishing-sider bliver anmeldt til DK•CERT. PhishTank (www.phishtank.com) er startet den 28. oktober 2006. Indtil den 26. august 2009 er der registreret 458.291 phishing-websites på verdensplan. USA står for mere en en tredjedel af disse websider (175.182; 38,2%) efterfulgt af Korea, Canada, Rusland og Tyskland. Danmark står på nr. 25 på verdensranglisten med 2.728 phishingwebsider (0,6%). I forhold til de andre nordiske lande har Danmark førerpositionen. Sverige står som nr. 30 med 1.832 phishingwebsider og Norge på nr. 49 med 662 sider. (http://support.clean-mx.de/clean-mx/phishstats). Finland og Island forekommer ikke i top-50.

På den 26. august 2009 var 4.170 af disse sider ikke lukkede endnu. Også her ligger USA i spidsen med 2.443 websider (58,6%). Danmark indtager plads nr. 17 på verdensplan denne dag med 15 ikke-lukkede phishingsider (0,4%). I DK•CERTs trendrapport 2008 oplyses, at "danske webhosting-udbydere er langsomme til at reagere og lukke phishing-sites på deres servere. Median-levetiden for et phishing-site på danske servere er over 16 dage. Det vil sige, at halvdelen af alle phishing-sider i Danmark når at være aktive over 16 dage, inden de lukkes." (s. 14).

Når PhishTank har registreret 2.728 danske phishing-websider på knap tre år (fra den 28. oktober 2006 til og med den 26. august 2009), og DK•CERT har modtaget 881 anmeldelser i en periode på tre år (2006-2008), må konklusionen være, at ca. en tredjedel af de danske phishing-websider bliver anmeldt ved DK•CERT.

Ifølge sikkerhedsfirmaet PandaLabs er mængden af software, der forsøger at stjæle ofrenes identitetsoplysninger, vokset 600 procent på et år. Firmaet modtager næsten 37.000 nye stykker skadelige programmer hver dag. 71 procent af dem er trojanske heste, der forsøger at opsnuse folks kontooplysninger eller kreditkortnumre. Andre trusler består af virus, orme, spyware og phishing. PandaLabs anslår, at tre procent af brugerne bliver ofre for truslerne. Ofte er de skadelige programmer ikke til at se medmindre man foretager en sikkerhedsscanning af pc'en.
Kilde: www.cert.dk; 25. august 2009.

3.3.2 Persondatabeskyttelse

Datatilsynet er den centrale uafhængige myndighed, der fører tilsyn med, at reglerne i persondataloven overholdes. På hjemmeside (www.datatilsynet.dk) kan læses om anmeldelser til Datatilsynet. Mange af anmeldelser har overskrift 'sikkerhedsbrist'. For eksempel blev "Datatilsynet den 24. februar 2009 gjort opmærksom på, at Holstebro Tekniske Skole havde offentliggjort oplysninger om studerendes personnumre på universitetets hjemmeside" og "Datatilsynet blev i april måned 2009 bekendt med, at der var en sikkerhedsbrist på www.pengesparet.dk." Det fremgår imidlertid ikke klart i årsberetningerne, hvor mange af denne typer sager, der er kommet til kendskab af Datatilsynet.

3.3.3 Finanser

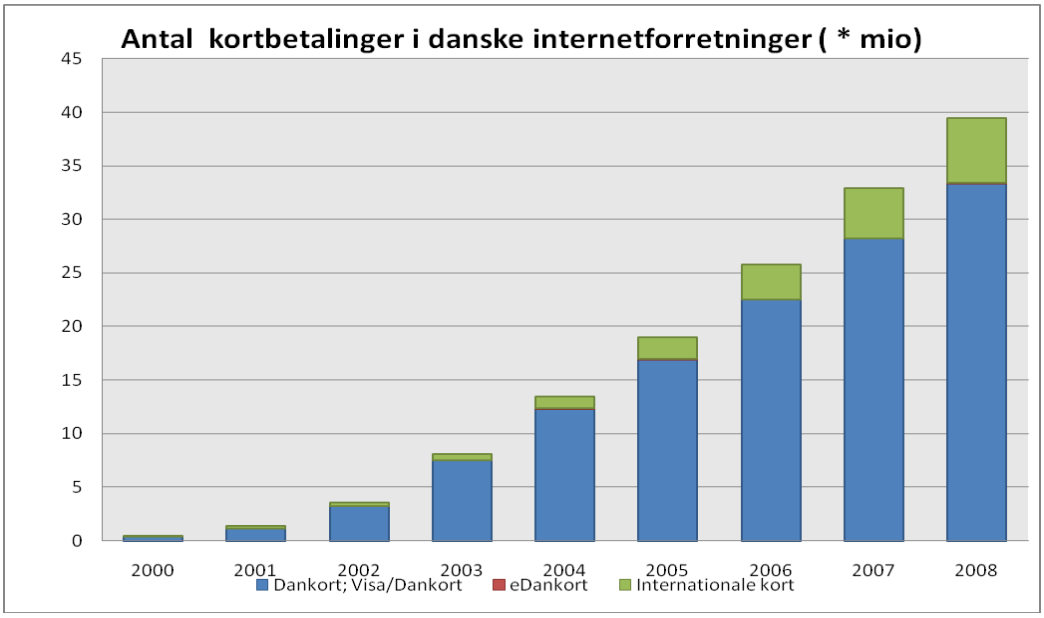
Både offerundersøgelser og politiets oplysninger indikerer at identitetsmisbrug i stor stil rettet sig mod kreditkort. Eller for at sige det rigtigt: debit- og kreditkort.[14] Dankort er vel den mest kendte og anvendte variant som administreres af PBS. Figur 3.6 viser udviklingen i antallet af kortbetalinger i danske internetforretninger. I 2008 nærmer antallet sig 40 mio.

Visa/Dankort

Det nye Dankort, indført i løbet af sommeren 2004, har inkorporeret en synlig chip til venstre på kortets forside. På **forsiden** finder man som på stort set alle slags betalingskort - oppe fra og ned - navnet på banken, de 4x4 - fysisk fremhævede - cifre som udgør Dankortets kortnummer, bank-koden (som er identisk med de første fire cifre i kortnummeret), udløbsdatoen, kortholders navn (kortets ejer) og endelig et VISA-mærke og VISAs hologram med en due, hvis VISA/Dankort-løsningen er valgt. På **bagsiden** af Dankortet finder man Dankortsymbolet, den tilknyttede kontos registreringsnummer og kontonummer. Neden under dette finder man et felt, hvor kortholderen skal placere sin underskrift, dette felt indeholder desuden nogle cifre, hvoraf de sidste tre er dét, der kaldes 'kontrolnummeret' (dette bruges fx til visse internetbetalinger). Derefter følger den bevarede sorte magnetstribe og producentens fabrikationsnummer i små typer.

Kilde: http://da.wikipedia.org/wiki/Dankort

Figur 3.6

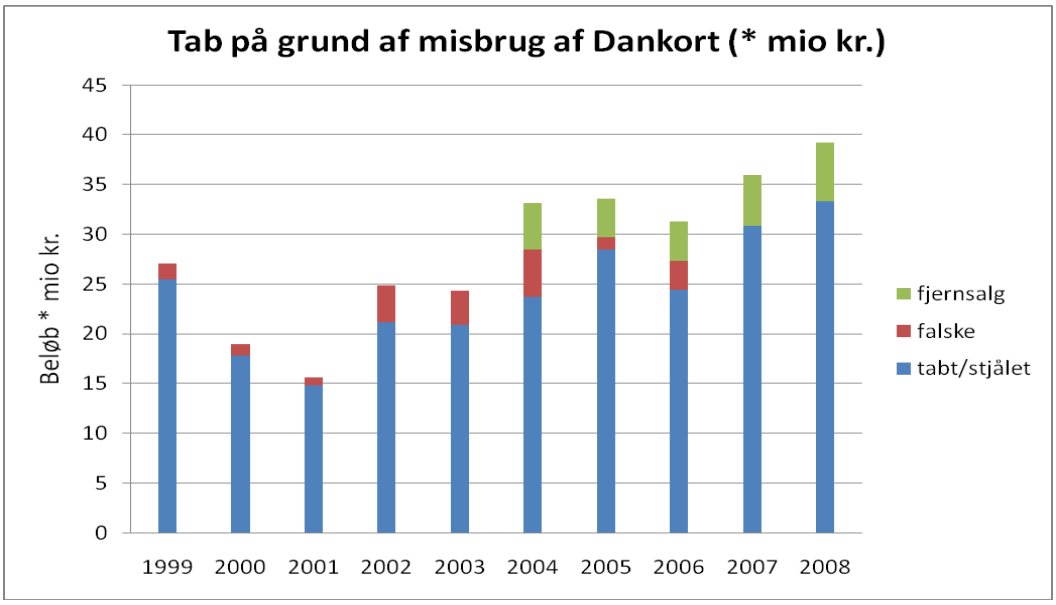


Kilde: www.pbs.dk

[14] "Ordet *kreditkort* anvendes af mange også fejlagtigt om *debetkort* (betalingskort) som de rettere bør kaldes, eksempelvis *Visa* og dets derivater så som *Visa-Elektron*. Debetkort stiller ikke et kreditbeløb til rådighed for kortindehaveren (i modsætning til eksempelvis Eurocard, Masters Card eller Diners Club kort), men forudsætter dækning på den konto, der hører til kortet for at en betaling kan anses for retsgyldig." (http://da.wikipedia.org/wiki/Kreditkortbetaling).

På jagt efter oplysninger om misbrug af betalingskort fandt jeg på en exceloversigt om misbrug af Dankort. Figur 3.7 viser omvang og udvikling af misbrug af Dankort.[15]

Figur 3.7



Figuren viser, at der er tale om en stigende tendens. I 2006 er der tale om et mindre fald i den samlede tab, men i 2007 og 2008 stiger omfanget igen. Dette er i strid med meldinger fra PBS. I et interview med Samdata (IT-fagets fagforening) siger PBSs pressechef at "mængden af misbrug med betalingskort stort set lig nul i 2006 og 2007 og første halvår af 2008. Grunden er, at forretningerne i vid udstrækning har lagt om til chipkort. Derfor ses væksten primært på internet, men også her er det tale om en moderat vækst." Tallene for det første halvår 2008 som pressechef ellers refererer til i interviewet stemmer overens med figur 3.7, men tolkning virker misvisende.

Figur 3.7 viser at den traditionelle metode til misbrug – tabt eller stjålet – stadig udgør langt den største del af det samlede tab. I 2008 står tabt/stjålet for lidt over 33 mio. kr., mens fjernsalg tegner for knap 6 mio. kr.[16] Den nye Dankort (med chip) har imidlertid sat en stopper for falske Dankort (skimming).

Finansrådet melder i årsberetning fra 2006: "De såkaldte afluringssager fortsatte i 2005/2006 frem til påsken 2006, hvor sektoren – i lyset af den kraftige stigning i angrebene i vintermånederne – stoppede den såkaldte fall back løsning i landets pengeautomater. Fall back-løsningen indebar, at pengeautomaten læste kortets magnetstribe, hvis chippen ikke kunne læses. Nedlukningen af fall back-muligheden opfattedes positivt af Dankort-indehaverne, idet der blandt disse var en bred forståelse for, at denne svindelmulighed måtte ophøre. Ved at ophøre med at foretage udbetaling i pengeautomater på grundlag af magnetstriben på kortene og kun foretage udbetaling i de

[15] Der findes ingen datagrundlag for fjernsalg i perioden 1999-2003.

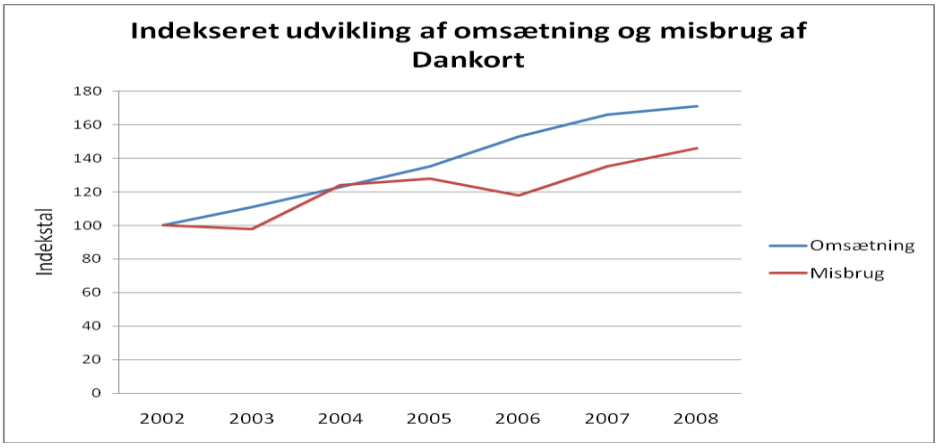
[16] Fjernsalg omfatter Internet, Postordre, Telefonordre og betalingsautomater uden PIN-kode. Før 2008 foreligger der kun datagrundlag for Internet.

situationer, hvor chippen i kortene kun læses af pengeautomaten, stoppede denne svindelform – udført af bander med tilknytning til Rumænien – stort set fra den ene dag til den anden."

Figur 3.7 viser også et markant fald i misbruget af Dankort i 2000 og 2001. Forklaringen findes formentlig igen i et teknisk modtræk af finanssektoren mod svindeler. I Finansrådets årsberetning fra 1999 læser vi: "Pengeinstitutterne har på baggrund af det passerede besluttet at sikre penge-automaterne yderligere. Langt de fleste udendørs pengeautomater vil inden udgangen af 1999 blive forsynet med en afskærmning omkring PIN-tastaturet. Ligeledes er der foran kortindførings-stedet påmonteret en enhed, som gør det stort set umuligt for forbrydere at påmontere en falsk kortlæserenhed. Finansrådet mener, at disse to tiltag vil hindre en gentagelse af det svindel-nummer, som vi så i Vimmelskaftet i København i marts. For så vidt angår øvrige automater, det være sig på benzinstationer eller andre steder, har PBS kontaktet de pågældende benzinselskaber m.fl. og disses leverandører af de pågældende automater. Det sker for at sikre, at der ikke på disse automater kan påsættes falske fronter, som gør det muligt at aflæse magnetstriben og registrere eventuel tilhørende PIN-kode. Den samme vurdering vil blive gennemført over for øvrige leverandører af pengeautomater på det danske marked med henblik på, at også sådanne penge-automater om nødvendigt vil blive sikret yderligere."

I den kriminologiske litteratur peges ofte på den begrænsede levetid af præventive tiltag (se fx Graham, 1990). Det ligner et kapløb, hvor kriminelles opgave er at uskadeliggøre præventive tiltag og samfundets/virksomhedens opgave at finde frem til nye forhindringer. Et andet kendt kriminologisk fænomen er forskydning (se fx Reppetto, 1976). Ideen bag denne teori er, at præventive forhindringer til et bestemt slags kriminalitet gør, at kriminelle søger deres lykke i andre retninger. Begge fænomener – uskadeliggørelse og forskydning – gør sig gældende inden for kortsvindel, men i det lange løb holder finanssektoren og kortsvindlere hinanden mere eller mindre i skak, når forholdet i udvikling mellem omsætning og misbrug af Dankort betragtes som målestok (figur 3.8).[17]

Figur 3.8



[17] Figur 3.8 er indekseret fra 2002 af, og ikke fra 1999 (jf. figur 3.7) for årene 1999-2001 er atypisk i forhold til den efterfølgende periode (fra 2002-2008).

Svindel med betalingskort er en metode, hvorved identitetsoplysninger kan blive misbrugt i forhold til finanssektoren. Den anden metode er misbrug af netbanker. I efteråret 2006 melder Finansrådet om de første angreb mod danske netbanker. Via spammail lokkes netbankkunder til at åbne vedhæftede malware som kan få fat i nøglefilen til netbanken og aflure passwordet. Ifølge Finansrådets årsberetning 2006 var det samlede tab 1,7 mio. kr.

Finansrådet har ikke publiceret årsberetninger efter 2006. Tallene for antal af netbankindbrud for 2007 og 2008 stammer fra en avisartikel i dagbladet Politiken i starten af 2009. Tallene viser, at antal af indbrud er fordoblet in 2008 i forhold til 2006. Størrelsen af tabet i 2007 og 2008 har jeg ikke kendskab til.[18]

Tabel 3.8: Indbrud i danske netbanker

	Antal	Indeks
2006	78	100
2007	85	109
2008	156	200

Skaffede hackere sig i 2006 adgang til netbank via spammail, udnytter hackere i 2009 små huller i ikke-opdaterede programmer, som iTunes, PDF-reader eller Java til at sende et spionprogram (malware) ind i brugerens computer. "Derfor skal danskere lære at opdatere deres programmer og sikre deres computere, ligesom de sikrer deres hjem ved at låse døren, når de går hjemmefra", siger lederen af sektionen for økonomisk kriminalitet ved Københavns Politi til Politiken.

[18] Henvendelse til Finansrådet om disse oplysninger gav ingen resultat

KAPITEL 4

Striden mod identitetstyveri

I dette kapitel sættes fokus på, hvordan samfundet prøver at forebygge og bekæmpe identitetstyveri. Striden belyses fra fire vinkler, navnlig:

- Lovgivning
- Information og registrering
- Tekniske forhindringer
- Overvågning og efterforskning

Situationen i Danmark er udgangspunktet, men erfaringer og initiativer i andre vestlige lande tages også i betragtning. Dette forskningsprojekt er imidlertid relativt begrænset i sit omfang og dermed er tilstanden i andre lande i forhold til identitetstyveri ikke undersøgt systematisk.

4.1 Lovgivning

Ifølge OECD har ikke ret mange lande specifik lovgivning vedrørende identitetstyveri. USA må betragtes som forgangsland på dette område. I USA er identitetstyveri en selvstændig forbrydelse. Identitetstyveri (ID Theft) er defineret som følgende: "knowingly transfers, possesses, uses, without lawful authority, a means of identification of another person with the intent to commit, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." (OECD, 2009, p. 47).

I Frankrig er et lovforslag vedrørende identitetstyveri i 2005 ikke blevet til noget for den franske justitsminister trak lovforslaget tilbage i 2006 med den begrundelse at identitetstyveri tilstrækkeligt kan straffes efter den eksisterende lovgivning (OECD, 2009, p. 50). Ellers har der ifølge OECD ikke været initiativer i EU-medlemsstaterne til at betragte identitetstyveri som en selvstændig forbrydelse.

I Norge er identitetstyveri blevet en selvstændig forbrydelse i den nye straffelov. Den nye bestemmelse om identitetskrænkelse vil give straf for den som tager en andens identitet, optræder med en andens identitets eller optræder med en identitet som er let at forveksle med en andens. I tillæg omfattes det at sætte sig i besiddelse af en andens identitetsbevis. Identitet kan omfatte

navn, fødselsnummer, organisationsnummer, e-postadresse eller andre oplysninger som alene eller sammen med anden information kan identificere en fysisk eller juridisk person. (Justits- og Politidepartementet, 2009).

I den norske pressemeddelelse påpeges, at mange handlinger som vil kunne omfattes af den nye bestemmelse allerede var strafbare under den gamle straffelov blandt andet efter bedrageri-bestemmelser. Men det er en forudsætning, at stjålet identiteten bruges til at udføre en strafbar handling. Den nye straffebestemmelse gør det enklere at strafforfølge identitetstyveri, for det er lettere at bevise en identitetskrænkelse end et forsøg på fuldbyrdet bedrageri.

Mads Bryde Andersen peger på, at strafbarheden af identitetstyveri ifølge dansk ret beror på, hvilket forsæt gerningsmanden har, dvs. hvilken forbrydelsen han havde i tankerne at udføre, da han foretog sine forskellige tilegnelsesaktiviteter. Mange IT-gerningsmænd (hackere) siger ofte, at de kun gjorde, hvad de gjorde for at se, om det kunne lade sig gøre, og slet ikke for at begå yderligere kriminalitet (personlig kommunikation d. 25. august 2009).

4.2 Information og registrering

Information er et vigtigt instrument i striden om identitetstyveri. Der er mange internetsider, hvor borgere og virksomheder kan få gode råd til at minimere risikoen til at blive udsat for identitets-tyveri. Opskriften er mere eller mindre den samme. Det gælder de danske sider, men også de ikke-danske sider. Herunder et eksempel hentet fra www.it-borger.dk.

Sådan undgår du phishing

- Oplys kun fortrolige og personlige oplysninger, herunder cpr-numre, på et netsted, du har tillid til og som anvender kryptering (se efter hængelås nederst i browseren).
- Oplys ikke fortrolige og personlige oplysninger i e-mails, medmindre du benytter kryptering.
- Oplys ikke fortrolige og personlige oplysninger, når du er på debatsider, i chatrum osv.
- Undlad at oplyse nummeret på dit betalingskort eller din bankkonto, med mindre du skal købe en vare på nettet - og du har tillid til netstedet.
- Oplys ikke pin-kode til dit betalingskort, hverken via nettet eller telefon.
- Tænk dig altid om en ekstra gang, når du afgiver personlige oplysninger.

I Danmark findes der ikke en internetside, hvor borgere kan melde, at de har været udsat for identitetstyveri, og hvor de kan få hjælp og vejledning. I mange lande omkring Danmark har myndighederne tager hånd om det. Den 17. juni 2009 lancerede den norske justitsminister internetsiden www.idtyveri.no. Internetsiden tilhører det nationale identitetstyveriprojekt. I Holland har Indenrigsministeriet oprettet en Centraal Meldpunt Identiteitsfraude. Her kan borgere melde, at de har været udsat for identitetsmisbrug og de kan melde, at der findes registreringsfejl i offentlige registre. På den måde burde det være nemmere at 'rydde op' efter man har været offer for identitetstyveri, fx ved at rense en plettet straffeattest efter gerningspersonens anvendelse af

ofrets navn overfor politiet eller ved at blive fjernet som dårlig betaler på grund af identitets-misbrug.

4.3 Tekniske forhindringer

Betalingskort
For det meste er sikring og brugervenlighed i konflikt med hinanden. Jo mere sikkert systemet er, jo mindre brugervenligt og omvendt. Dette gælder også for internethandel. Det er naturligt meget nemt og enkelt at kunne betale med et kreditkort ved nethandel, men det åbner også op for misbrug. Det første forhindring til at dæmme op for misbrug var at indføre CVV-koden (på bagsiden af kreditkort). Flere – ofte udenlandske netbutikker har lagt en anden forhindring til misbrug af kreditkort, navnlig en ekstra kode (verified by).

Verified by Visa; MasterCard Secure Code
Bruger du Visakort eller MasterCard, når du handler på internettet, kan du blive bedt om at oprette en ny type sikkerhedskode. Koden kaldes Verified by Visa og MasterCard Secure Code og vil fremover blive benyttet af flere og flere netbutikker. Ved at bruge koden bekræfter du, at det er dig, der bruger dit kort til betaling. På den måde giver koden ekstra sikkerhed mod misbrug af dine kortoplysninger. Det er op til de enkelte netbutikker, om de vil bruge Verified by Visa og MasterCard SecureCode.
Når du første gang skal betale i en netbutik, der bruger Verified by Visa eller MasterCard Secure Code, skal du oprette en personlig kode. Når du først har oprettet koden, kan du genbruge den samme kode i andre netbutikker, som bruger sikkerhedsløsningen. Du kan også vælge at oprette et kodeord nu, så du slipper for at gøre det midt i en nethandel. Vær opmærksom på, at du skal lave et kodeord for hvert enkelt kortnummer, men kodeordet kan godt være det samme.
Kilde: www.danskebank.dk

Sikring af betalingskort i den 'fysiske' verden er indførelsen af en chip på kortet. Dermed er der sat et stopper for skimming – kopiering af kortets magnetstribe – for betalinger kræver aflæsning af chip.

Det ser ud til at mobiltelefonen mere og mere kan blive brugt som betalingsmiddel. I dag kan man betale for parkering eller købe en busbillet med mobilen. Beløbsloftet til betalinger gennem mobiltelefon er på nuværende tidspunkt 225 kr., men det ser ud til at loftet fjernes snart. "Det er en interessant mulighed, men den kræver, at sikkerheden for betaling med mobiltelefonen bliver meget højere, end den er i dag. Det bør være sådan, at hvis mobiltelefonen bliver tabt eller stjålet, så kan en anden ikke gå ind og betale for varer med penge fra ejerens konto", siger Forbrugerrådets direktør Rasmus Kjeldahl (Politiken, 12 oktober 2009).

Netbank
Netbanker i Danmark er som regel sikrede mod misbrug ved bruger-id, personlig kode og en fil på computeren til at kunne log in på netbanken. Misbrug kan kun ske, når gerningspersonen får fat i alle tre nøgler til netbanken. Spyware er i princippet i stand til at opsnappe alle tre ingredienser til at skaffe adgang til en anden persons netbank. En anden metode til at sikre adgang til netbanken er – i stedet for en fil på computeren – en liste med unikke koder (typisk 6 cifre). For at kunne gennemføre en betaling skal der indtastes sådan en unik kode. Når listen med unikke koder er brugt op, fås kunden en ny liste. For nyligt er det også muligt at modtage disse koder pr. sms.

Net ID
Netbankens adgangskode bliver også brugt som net-ID. Finansrådet skriver om net-ID: "Når en bruger ønsker at få adgang til egne oplysninger hos en virksomhed, klikker brugeren på net-ID-logo'et på virksomhedens hjemmeside. Kan pengeinstituttets sikkerhedssystem godkende adgangskoden, sendes en bekræftelse på brugerens identitet til virksomheden." Det er fx muligt at få adgang til e-post gennem net-ID. Virksomheder som vil benytte net-ID skal indgå en aftale med PBS, som stiller krav til sikkerhed. Det kræver imidlertid ikke ret meget fantasi for at indse, at udbredelse af netbank-adgangskoder til at komme ind på andre systemer forøger risikoen for misbrug.

Biometri
Traditionelt er danskernes cpr-nummer måden, hvorpå man identificeres. I mange sammenhænge spørges efter ens cpr-nummer. Om det nu er at låne bøger på biblioteket, at afslutte et abonnement til sin mobiltelefon eller at oprette en konto i banken, bliver man spurgt om sit cpr-nummer. Dermed er det unikke nummer blevet langt fra sikkert og har tabt sin værdi til et troværdigt identifikations-middel.

Biometri bliver ofte betegnet som den bedste forhindring mod identitetstyveri. Biometri er den samlede betegnelse for en række teknologiske metoder til identifikation og genkendelse af personer ved hjælp af unikke biologiske kendetegn hos personerne; fx elektronisk genkendelse af ansigt, øjne (iris), fingre (fingeraftryk), stemme, hænder, vener og gangart.

Indenfor det offentlige anvendes biometri traditionelt af politiet. Brug af fingeraftryk til at bevise gerningsmandens tilstedeværelse på gerningsstedet stammer fra slutningen af 18. hundredtallet. Først hundrede år senere er der kommet et nyt biometrisk register til gavn for politiets opklarings-arbejde, navnlig dna-registret.

Men det er ikke kun politiet som bruger biometri som identifikationsmiddel. Pas-myndighederne anvender digitale billeder, ligesom det overvejes at integrere biometriske sikkerhedsløsninger i et fremtidigt borgerkort. Faktisk er alle danske pas, udstedt efter 1. august 2006, såkaldte biometriske pas, da de indeholder et digitalt billede lagret på en indbygget chip. I EU-regi er det besluttet, at alle nyudstedte pas skal indeholde både et digitalt foto og to sæt fingeraftryk. Planerne for et biometrisk borgerkort, hvor en række funktioner (bl.a. sygesikringsbevis, kørekort, dankort og mobil digital

signatur) er samlet i ét, er indtil videre blevet udskudt med den begrundelse, at det på nuværende tidspunkt er for dyrt. Det antages dog, at teknologien i fremtiden vil blive så billig, at et biometrisk borgerkort ud fra et økonomisk perspektiv vil blive den foretrukne løsning.

Den private sektor har taget biometri til sig på flere områder. I stigende omfang bliver biometriske data brugt til at sikre identifikation af kunden, fx ved betaling eller adgangskontrol. Datatilsynet har givet Crazy Daisy tilladelse til at registrere gæsternes fingeraftryk (med deres samtykke) for at lette adgangskontrol til diskoteket. I april 2007 indførte SAS mulighed for check in på indenrigsruter fra Aalborg lufthavn gennem fingeraftryk identifikation. Computerfabrikanter har skabt muligheden for at logge på computeren med fingeraftryk som adgangskode.

Datatilsynet har haft en række principielle afgørelser vedrørende brug af biometriske teknologier. Det blev afvist at anvende fingeraftryksscanning i forbindelse med adgang til fitnesscentre, mens et vagtfirma og Københavns Lufthavn begge har fået godkendelse til at bruge fingeraftryk til at identificere personer. Datatilsynet lægger vægt på proportionalitetsprincippet.

Teknologirådet kommer i slutningen af 2009 med en rapport om anvendelse af biometri. Projektets formål er at se bredt på fordele og ulemper ved nuværende anvendelsesmuligheder og komme med anbefalinger vedrørende fremtidig brug af biometri i Danmark. Forud publicering af rapporten har teknologirådet lavet en oversigt over argumenter for og imod brug af biometri som identifikations-middel (www.tekno.dk):

Ifølge teknologirådet peger kritikere på:

- At risikoen for og konsekvenserne ved identitetstyveri er stigende.
- At registrering af personoplysninger, der er knyttet til den biometriske identifikation risikerer at blive for omfattende.
- At personoplysningerne bliver for let tilgængelige, hvis ikke sikkerheden sættes i højsædet.
- At der er risiko for øget overvågning.
- At biometriske teknologier kan virke ekskluderende.
- At flere af de nuværende biometriske teknologier er for lette at snyde.

Modsat peger fortalerne på:

- At data allerede indsamles og kædes sammen.
- At biometri netop udgør en mulighed for at øge kvaliteten af data og for, at disse data beskyttes bedre.
- At der kan opnås et meget højt sikkerhedsniveau ved at kombinere forskellige biometriske teknologier.
- At biometriske løsninger kan være udgiftsbesparende.
- At biometri kan medvirke til at lette brugeren i forskellige dagligdagssituationer, fx ved at kunne anvende fingeraftryk til økonomiske transaktioner eller ved undgå at skulle huske et stort antal pinkoder.

Stephan Engberg fra firmaet Priway advarer i et interview med IT-avisen ComOn om, at biometri kan medføre permanent identitetstab. "Den største fejl er, at nogle tror, at biometri giver sikre nøgler. Biometriske data eller væv i form af fingeraftryk eller dna kan opsamles mange steder, uden at ofret har en chance for at beskytte sig. Udover selve den kriminelle handling kan de uskyldige ofre for identitetstyveri komme i en vanskelig situation, hvor de reelt står med omvendt bevisbyrde." (Pedersen, 2005)

4.4 Overvågning og efterforskning

DK•CERT overvåger it-sikkerheden i Danmark som en del af et internationalt samarbejde. Anmeldelser fra personer, der har været udsat for en sikkerhedshændelse analyseres og på baggrund af disse analyser gives forslag til en løsning af problemerne og advarsel til andre, der kunne risikere at blive udsat for en tilsvarende hændelse. Anmeldelser bliver behandlet fortroligt. DK•CERT har en rådgivende rolle og har ikke myndighed til at pålægge andre at foretage bestemte handlinger (www.cert.dk).

PBS har et Risk Management System til overvågning af misbrug og misbrugsmønstre vedrørende betalingskort. Eksperter følger og overvågner døgnet rundt samtlige korttransaktioner; i gennemsnit over to mio. i døgnet. Risk Management-systemet er sat op til at fange usædvanlige hændelser; fx et kort, der bliver brugt mange gange efter hinanden, hvilket tyder på, at kortet er stjålet. Systemet advarer også, hvis det samme kort – inden for samme tidsrum – bliver brugt både på Storebæltsbroen og i Thailand. Det betyder, at kortet er kopieret og bliver lukket det med det samme (www.pbs.dk).

På politiets hjemmeside kan læses, at man kan henvende sig til rigspolitiets IT-Efterforskningscenter (NITEC) vedrørende mistanke om børnepornografi eller hacking. Alle andre henvendelser og generelle forespørgsler på IT-området skal rettes til den lokale politikreds. Ved henvendelse til NITEC vil centeret, hvis nødvendigt, sikre beviser og starte en indledende efterforskning. Derefter vil sagen blive overdraget til den lokale politikreds (www.politi.dk).

NITEC er en hastigt voksende enhed. I en tiårig periode er antallet af medarbejdere steget fra tre til omkring 70. De fleste medarbejdere er politifolk, men for et par år siden er der åbnet op for civilansatte, blandt andet softwareudviklere. I Magasinet for politi og anklagemyndighed siger NITEC's leder Søren Thomassen, at "politiet tidligere er blevet kritiseret for at give hackere for let spil og ikke være ordentligt klædt på til opgaven med at bekæmpe IT-kriminalitet, men det er fortid." (Broksø, 2008, s. 18).

Om dette billede af NITEC og politiet holder stik har ikke været genstand for forskning, men i Computerworld påpeges, at virksomheder undlader at anmelde hacker-angreb. "Risikoen for at blive eksponeret i medierne er mange gange højere end sandsynligheden for, at politiet fanger en gerningsmand. Vores kunder som Alm. Brand, KMD, Tryg, Danske Spil, TDC, DONG og Arla

Foods er store nok til at rydde op efter sig selv, men det er ærgerligt, at gerningsmændene går fri", ifølge direktør Ulf Munkedal fra sikkerhedsfirmaet Fort-Consult (Hansen, 2006).

NITEC og politikredsene efterforsker ny bølge af databedrageri

I den aktuelle sag misbruges danske borgeres netbank-konti ved at udenlandske gerningsmænd sender e-mails ud til danske borgere indeholdende en vedhæftet fil med navnet 'regning.zip', 'regning.ex' eller tilsvarende. Åbner man den vedhæftede fil, downloades et program til computeren, som opsamler både tastetryk og nøglekoder. Ved hjælp af danske mellemmænd kan gerningsmændene efterfølgende overføre penge fra computerejernes netbank-konti til egne konti i udlandet. Der er allerede anholdt fem danske mellemmænd, som har hjulpet de udenlandske gerningsmænd i forbindelse med overførsel af stjålne penge. NITEC har desuden iværksat et internationalt samarbejde for at komme yderligere til bunds i sagen. Ofre for denne form for databedrageri kan henvende sig hos det lokale politi.

Kilde: www.politi.dk (3 november 2006)

KAPITEL 5

Konklusioner og diskussion

I dette afsluttende kapitel bliver resultaterne fra kapitler 2-4 anvendt til at søge svar på problemstillinger formuleret i afsnit 1.2.

Hvordan foregår identitetstyveri?
Identitetstyveri strækker sig ud over to faser: tilegnelse og misbrug af oplysninger. Der kan skelnes mellem online- og offline-tilegnelse af personoplysninger. Når tilegnelsen sker online kaldes det phishing. Phishing kan forekomme på forskellige måder. Det (naive) offer kan blive spurgt direkte gennem e-mail om at oplyse bestemte informationer. Det kan også ske ved at dirigere forurettede til en falsk hjemmeside eller via spyware. Til at kunne sende mange e-mails ud, bliver ofte brugt et botnet. På den måde er der ofte en forbindelse mellem phishing og hacking. Også mobiltelefoner er blevet inddraget i phishing. Når tilegnelsen af en andens identitetsoplysninger sker offline peger de fleste kilder på tre metoder: 'gammeldags' tyveri (taske/pungtyveri eller indbrud), affald (dumpster diving) og postvæsen. Skimming (kopiering af betalingskort) ser ud til at være forsvundet i Danmark ved introduktion af chip på betalingskort.

Der skelnes mellem tre former for misbrug af personoplysninger. For det første økonomisk misbrug af oplysninger. Det kan ske ved at misbruge ofrets eksisterende (net)bankkonto eller betalingskort. Men det kan også ske ved at oprette lån, bestille betalingskort eller lignende i ofrets navn. I den internationale litteratur betegnes disse to former for økonomisk misbrug som: 'account take over' og 'true name fraud'. Ved økonomisk misbrug af personoplysninger bliver der ofte inddraget et såkaldt muldyr (en person, der lægger bevist eller ubevist navn til transaktioner) til at transportere penge eller varer ud af landet. Den anden form for misbrug er det såkaldte kriminelle misbrug. Gerningsmænd bruger ofrets personoplysninger til at vildlede myndighederne for at undgå strafforfølgelse. Den sidste form for misbrug er socialt betonet. Folk misbruger en kendt persons navn, billeder eller andre personoplysninger til en profil på nettet eller lignende. I princippet er denne form af misbrug ikke strafbart i Danmark.

I hvilket omfang er danskere udsat for former af identitetstyveri?
Offerundersøgelsen, der omfatter 1.853 danskere, viser, at lidt over en procent (20 personer) har været udsat for en form for identitetstyveri de sidste 12 måneder. Når denne oplysning generaliseres til Danmarks befolkning skulle der være mellem 27-69 tusinde danskere er blevet

offer for identitetstyveri. Misbrug af betalingskort udgør klart hovedparten af identitetstyveri i Danmark. Ca. 70 procent af respondenterne peger på denne form af identitetsmisbrug. Uden tvivl er økonomisk misbrug den dominerende form af identitetstyveri i Danmark.

Offerundersøgelsen giver ikke et indtryk af udviklingen i identitetstyveri i Danmark. Når misbrug af betalingskort sammenlignes med resultatet for Danmark i EU ICS er den forsigtige konklusion, at kortmisbrug er steget i perioden 2005-2008 fra at ramme 0,3 til 0,8 procent af Danmarks befolkning. Denne konklusion bekræftes af tal fra PBS. I 2005 lå det samlede tab på grund af misbrug af Dankort på 19 mio. kr., dette beløb er steget til knap 40 mio. kr. i 2008. Også politiets anmeldelsesstatistik for databedrageri viser en stigning i perioden 2005-2008 fra 533 anmeldelser i 2005 til 724 i 2008. Politiets statistik vedrørende stjålne kontokort viser imidlertid ingen betydningsfulde stigning; fra 273 anmeldelser i 2005 til 307 i 2008.

Når disse tre kilder – offerundersøgelser, PBS-statistik og politiets anmeldelsesstatistik – tages i betragtning, er konklusionerne, at der er en stigende tendens i misbrug af betalingskort, og at denne stigning skyldes hovedsagelig online tilegnelse og misbrug af kortoplysninger.

Respondenter i offerundersøgelsen mener i lidt under halvdelen af tilfældene, at de har mistet deres oplysninger online. Politiets anmeldelsesstatistik vedrørende hacking viser imidlertid en faldende tendens i perioden 1999-2008. De sidste par år (2005-2008) er der ikke tale om en klar tendens i politiets anmeldelsesstatistik for hacking. Antal anmeldelser er i sig selv imidlertid lavt. I 2008 blev der anmeldt 32 sager. Dermed bekræftes formodning, at virksomheder og borgere ikke hyppigt anmelder denne slags sager til politiet. Tal fra DK•CERT peger i retning af en klart stigende tendens af websites med trojanere og phishingsider. Fra 148 anmeldelser in 2005 til 332 i 2008.

Hvordan foreholder Danmark sig internationalt?
Internationale offerundersøgelser viser, at misbrug af betalingskortoplysninger står for en stor del af identitetstyverierne. USA er et kapitel for sig selv. Mellem 4 og 4,5 procent af den amerikanske befolkning har været udsat for identitetstyveri. I Europa er niveauet betydelige lavere. De angelsaksiske lande (England & Wales, Skotland, Irland og Nord Irland) ligger i toppen i Europa, mens de skandinaviske lande ligger i bunden, hvad angår identitetstyveri.

I europæisk perspektiv er niveauet af identitetstyveri i Danmark således lavt, men i et nordisk perspektiv ligger Danmark i toppen. Ifølge Phish Tank ligger Danmark på nr. 25 på verdensranglisten i forbindelse med phishing websider, efterfulgt af Sverige (nr. 30) og Norge (nr. 49). Finland og Island forekommer ikke i top-50.

Hvilke forebyggende tiltag er indført i Danmark?
Information er et vigtigt våben til forebyggelse af identitetstyveri. På den ene side er der almene oplysninger om, hvordan man færdes sikkert på internettet, på den anden side er der information om konkrete trusler (specifikke phishing mails osv.). Det er både offentlige myndigheder og

private virksomheder, som bidrager med information til at undgå identitetstyveri. For at kunne informere borgere og virksomheder er det vigtigt til at overvåge, hvad der foregår på nettet. DK•CERT overvåger it-sikkerheden i Danmark som en del af et internationalt samarbejde. Der er flere private virksomheder, som overvågner internettet med henblik på til at sælge deres vare (anti-virus programmer osv.).

Derudover er der tekniske tiltag til at forebygge identitetstyveri. De fleste computerbrugere har installeret anti-virus software, en firewall osv. Sikre dele af websiderne er krypteret og kan kun besøges ved brug af adgangskoder. Kortselskaber har indført en chip på betalingskort til at undgå kopiering af kortet (skimming). Biometri ser ud til at være vejen frem inden for identitetssikring. Kritikere advarer imidlertid om, at konsekvenserne for ofre kan være meget omfattende, og spørgsmålet er, om 'medicinen ikke er værre end problemet'. Ved siden af tekniske tiltag til at forebygge misbrug, overvågner PBS korttransaktioner til at stoppe misbrug så hurtigt som muligt ved hjælp af et Risk Management System.

Hvad er forventningerne for de kommende år?
Det ser ud til, at identificering ved hjælp af cpr-numret har haft sin længste tid. Rådet for IT- og Persondatasikkerhed spurgte sig selv i årsberetning 2007, hvordan vi identificerer os mest sikkert over for de digitale systemer og om der er behov for andre systemer end de, der baserer sig på cpr-numret. Efter min vurdering vil biometri vinde i betydning de kommende år. For ofre af identitetstyveri er det en dårlig nyhed. Forhåbentligt bliver antallet af ofre begrænset, men dem der bliver udsat herfor får mere og mere svært ved at bevise deres uskyld. På baggrund af det, ville det antageligt være en god idé, om der i Danmark – lige som i mange andre vestlige lande – oprettedes et center, hvor ofre for identitetstyveri kan få hjælp at komme ude af situationen ved at rydde op efter tyveriet.

Jeg kan ikke forestille mig, at systemet med betalingskort holder i længden. Misbrug udgør på nuværende tidspunkt åbenbart så lille en del af omsætningen, at kortselskaberne stadig tjener penge på det, men vi må forvente, at der på sigt findes bedre løsninger. Mobiltelefonen er en mulig kandidat, men det kan også godt være, at der findes løsninger i andre retninger.

Politiets rolle i forbindelse med denne form for kriminalitet er og har været begrænset. Virksomheder tager affæren i egen hånd, og håbet er, at bagmænd kan strafforfølges er ikke særligt stort. Initiativer som i Norge til at kriminalisere tilegnelsesprocessen af personoplysninger yderligere forekommer mere som symbollovgivning end at det nu virkelig rykker noget i kampen mod identitetstyveri.

Om identitetskloning som Angela Bennett bliver udsæt for i filmen *The Net* bliver en del af fremtiden er svært at vurdere, men at vi bliver mere afhængige af vores systemidentitet frem for vores fysiske identitet i en digitaliseret og globaliseret verden er efter min mening sandsynligt. Og dermed bliver konsekvenserne af identitetstyveri mere alvorlige. Det er i sig selv en vigtig grund

til at gennemtænke, hvordan vores identitetsoplysninger skal sikres, og dårlig sikkerhed er måske værre end ingen sikkerhed.

Litteratur

Balvig, Flemming & Britta Kyvsgaard (2009) *Udsathed for vold og andre former for kriminalitet: offerundersøgelserne 2005-2008*. Københavns Universitet, Justitsministeriet, Det Kriminalpræventive Råd, Rigspolitichefen. www.jm.dk

Binder, R. & M. Gill (2005) *Identity theft and fraud: learning from the USA*. Perpetuity Research and Consultancy International.
www.perpetuitygroup.com/prci/pdfs/identitytheftandfraudreport.pdf

Bjerrehuus, Suzanne (2008) Falske profiler er helt lovlige!
ekstrabladet.dk/nationen/article1057528.ece

Broksø, Keld (2008) Jagten på it-kriminelle er for alvor gået ind. I: *Magasinet til politi og anklage-myndighed*, nr. 10.

DK-Cert (2009) Trendrapport 2008: It-kriminalitet og sikkerhed i året der gik.
www.cert.dk/trendrapport2008/trendrapport2008.pdf

Cheney, J.S. (2005) *Do definitions still matter?*
phil.frb.org/pcc/discussion/identity-theft-definitions.pdf

Dijk, J.J.M. van, Kesteren, J.N. van & Smit, P. (2008). *Criminal Victimisation in International Perspective*, Key findings from the 2004-2005 ICVS and EU ICS. The Hague, Boom Legal Publishers.

Ertman, Berit (2008) *Der svindles for milliarder på nettet.*
epn.dk/teknologi2/computer/sikkerhed/article1523316.ece

Europol (2006) Organised Crime Threat Assessment (OCTA).
europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_(OCTA)/OCTA2006.pdf

Fellowes Benelux, Bescherm uw identiteit: een praktische handleiding.
stop-identiteitsfraude.com

Finansrådet. Årsberetninger (1999-2006)
finansraadet.dk/

Graham, John (1990) *Crime Prevention Strategies in Europe and North America*, HEUNI report nr. 18, Helsinki.

Identity Theft Resource Center (ITRC) (2008) Identity Theft: The Aftermath 2007. idtheftcenter.org/artman2/uploads/1/Aftermath_2007_20080529v2_1.pdf

Hansen, Kristian (2006) Dansk politi giver hackerne frit spil. I: *Computerworld*, 15 september 2006. computerworld.dk/art/35655?op=print

Justitsministeriet (2009) *Besvarelse af spørgsmål nr. S 1907* (strafbare forhold i relation til såkaldt identitetstyveri og identitetsmisbrug på internettet).

Javelin Strategy & Research, *Identity Fraud Survey Report* (years 2003-2008) javelinstrategy.com

Klerks, P. (2009) Identiteitsfraude: Je weet niet wat je overkomt. In: *Tijdschrift voor de Politie*, 71:3, p. 34-36.

Korsgaard, Ole (2005) Drenges svindel med kreditkort på internettet. I: *Nordisk Kriminalreportage 2005*. Nordisk Politi Idrætsforbund, s. 9-12.

Koszyczarek, Henrik Hindby (2009a) *It-angrebene bliver værre*. epn.dk/teknologi2/computer/sikkerhed/article1691752.ece

Koszyczarek, Henrik Hindby (2009b) *PDF er hackernes foretrukne våben*. epn.dk/teknologi2/computer/sikkerhed/article1686600.ece

Meulen, N.S. van der (2006) Achter de schermen: De ervaringen van slachtoffers van identiteits-roof. In: *Justitiële Verkenningen*, 32:7, p. 23-36.

Nationaal Dreigingsbeeld 2008, Korps Landelijke Politiediensten, Dienst IPOL. justitie.nl

McNally, Megan M. (2008) Charting the Conceptual Landscape of Identity Theft. In: McNally & Newman (eds.) *Perspectives on Identity Theft*. Crime Prevention Studies Vol. 23, Monsey: Criminal Justice Press; Devon: Willan Publishing Cullompton, pp. 33-55.

McNally, Megan M. & Graeme R. Newman (2008) Editors' introduction. In: McNally & Newman (eds.) *Perspectives on Identity Theft*. Crime Prevention Studies Vol. 23, Monsey: Criminal Justice Press; Devon: Willan Publishing Cullompton, pp. 1-8.

OECD (2009) Online Identity Theft. sourceoecd.org/governance/9789264056589

Pedersen, Karim (2005) Biometri kan medføre permanent identitetstab. I: ComOn, 25 august 2005. comon.dk

Prins, J.E.J & N.S. van der Meulen (2006) Identiteitsdiefstal: lessen uit het buitenland. In: *Justitiële Verkenningen*, 32:7, p. 8-35.

Repetto, T.A. (1976) Crime Prevention and the Displacement Phenomenon. In: *Crime and Delinquency*, p. 166-177.

Rigspolitiet, *Redegørelse for udviklingen I IT-kriminalitet samt den politimæssige indsats på området*. København.

Stove, Marie & Erik Valeur (2007) Det store identitetstyveri. I: *Tænk*, september 2007, s. 32-37.

Tranberg, Charlotte Bagger & Lars Bo Langsted (2008) Internet-kriminalitet. I: Trzaskowski, Jan (red.) *Internetretten*. København: Ex Tuto Publishing, s. 503-538.

Besøgte websider

www.cert.dk
www.cert.org
www.comon.dk
www.danskebank.dk
www.da.wikipedia.org
www.datatilsynet.dk
www.dr.dk
www.epn.dk
www.ekstrabladet.dk
www.europol.europa.eu
www.finansraadet.dk
www.first.org
www.identitytheftassistance.org
www.idtheftcenter.org
www.idtyveri.info
www.id-tyveri.no
www.it-borger.dk
www.itst.dk
www.javelinstrategy.com
www.justitie.nl
www.krak.dk
www.pbs.dk
www.pengesparet.dk
www.phishtank.com
www.politi.dk
www.politiken.dk
www.preswire.dk
www.sikkerhedsraadet.dk
www.stop-identiteitsfraude.com
www.support.clean-mx.de
www.tekno.dk

Bilag 1: Spørgsmålene offerundersøgelse vedr. identitetstyveri

1. Har du inden for de seneste 12 måneder været udsat for misbrug af personoplysninger eller identitetsbeviser?
    O Nej
    O Ja, jeg har selv været udsat for misbrug af mine personoplysninger

2. Er der tale om et enkeltstående misbrug, eller er det sket flere gange inden for de sidste 12 måneder?
    > antal gange <

3. Hvilke personoplysninger/identitetsbeviser er misbrugt? (flere svarmuligheder)
    O Navn og/eller adresse
    O Cpr-nummer
    O Dankort
    O Kreditkort
    O Bankoplysninger
    O Sygesikringsbevis
    O Pas/ID kort
    O Kørekort
    O Andet (-> navnlig:)

4. Til hvilket formål misbrugte gerningspersonen personoplysningerne eller identitetsbeviser? (flere svarmuligheder)
    O At købe noget på nettet
    O At købe noget i en butik
    O At hæve penge fra min konto (hæveautomat)
    O At overføre penge fra min konto til en anden konto
    O At leje noget (fx en bil) i mit navn
    O At afslutte et abonnement (fx mobiltelefon) i mit navn
    O At oplyse mit navn til myndighederne
    O At publicere (fx på nettet) noget i mit navn
    O Andet (-> navnlig:)

5. Hvordan har du opdaget, at dine personoplysninger/ identitetsbeviser blev misbrugt?
    O Konto- eller kortudskrifter
    O Netbank
    O Kort spærret af kortselskab
    O Opkrævning fra selskab/firma for en ydelse/abonnement/produkt
    O Bøde
    O Andet (-> navnlig:)

6. Hvordan, tror du, at gerningspersonen har fået fat i dine personoplysninger/ identitetsbeviser?
    O Falsk e-mail
    O Falsk hjemmeside
    O Hacking
    O Profiloplysninger (fx på Facebook)
    O Skimming (kopiering af magnetstrip ved fx hæveautomat)
    O Tvivlsom handel på nettet
    O Tvivlsom handel i butik/restaurant el.
    O Udlandet
    O Telefon
    O Taske/lommetyveri
    O Boligindbrud
    O Gade/hjemmerøveri
    O Affald
    O Andet (-> navnlig:)
    O Ukendt

7. Hvor stor et beløb er der trukket fra din konto eller opkrævet på grund af misbrug af personoplysninger/ identitetsbeviser?
    > Indtast beløb i kroner <

8. Hvor stor en del af dette beløb, måtte du betale selv?
    > Indtast beløb i kroner <

9. Har du meldt episoden til politiet?
    O Ja, og politiet optog anmeldelsen
    O Ja, men politiet afviste anmeldelsen
    O Nej, men politiet har fået kendskab om det på anden vis
    O Nej (-> hvorfor ikke?)

10. Er der blevet opklaret, hvem der står bag misbrug af dine personoplysninger/ identitetsbeviser?
    O Nej
    O Ja
    O Ved jeg ikke

11. Kendte du den person der har misbrugt dine personoplysninger/ identitetsbeviser i forvejen?
    O Nej
    O Ja, familie
    O Ja, venner
    O Ja, fra arbejde
    O Ja, fra uddannelsessted
    O Ja, fra naboskab
    O Ja, andet kendskab

Baggrundsvariabler:

- Køn
- Alder

- Civilstand
- Statsborgerskab
- Region
- Uddannelse
- Hovedbeskæftigelse
- Bruttoindkomst